reboot

– omstart för den digitala förvaltningen

Slutbetänkande av Utredningen om effektiv styrning av nationella digitala tjänster

Stockholm 2017

STATENS OFFENTLIGA UTREDNINGAR

SOU 2017:114

SOU och Ds kan köpas från Norstedts Juridiks kundservice.
Beställningsadress: Norstedts Juridik, Kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Norstedts Juridik AB
på uppdrag av Regeringskanslietsförvaltningsavdelning
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2018

ISBN 978-91-38-24745-7
ISSN 0375-250X

Till statsrådet Ardalan Shekarabi

Regeringen beslutade vid regeringssammanträde den 19 maj 2016 att uppdra åt en särskild utredare att analysera och ge förslag till effektiv styrning av utveckling, införande och förvaltning av nationella digitala tjänster (dir. 2016:39). Tidigare generaldirektören Hans-Eric Holmqvist utsågs samma dag till utredare. Den 24 november 2016 beslutade regeringen i tilläggsdirektiv (dir. 2016:97) om att utredaren skulle analysera hur digitaliseringen i den offentliga sektorn kan stärkas genom att, inom ramen för den befintliga myndighetsstrukturen, samla ansvaret för dessa frågor till en myndighet. Uppdraget redovisades i denna del den 15 mars 2017 i delbetänkandet digitalforvaltning.nu (SOU 2017:23).

Till experter i utredningen förordnades den 24 oktober 2016 kanslirådet Karina Aldén, Finansdepartementet, verksamhetsutvecklaren Emma Bohman, Transportstyrelsen, chefsstrategen digitalisering Lena Carlsson, Tillväxtverket, juristen Lena Carlsson, Datainspektionen, numera departementssekreteraren Veronica Eckerby, Finansdepartementet, tidigare kanslichefen vid E-legitimationsnämnden Eva Ekenberg, verksamhetsutvecklaren Anna Fors, Försäkringskassan, systemvetaren Ulrika Gani, Myndigheten för delaktighet, samordnaren digital samverkan Anders Granström, Arbetsförmedlingen, senior adviser Peter Göransson, Bankföreningen, filosofie doktorn Anneli Hagdahl, Finansdepartementet, utredaren Gabriella Jansson, Statskontoret, chefsjuristen Gustaf Johnssén, Statens servicecenter, experten offentlig digitalisering Anna Kelly, avdelningschefen Eva Lindblom, Ekonomistyrningsverket, kanslirådet Eva Lundbäck, Finansdepartementet, chefsarkitekten Peter Mannerhagen, Västerås stad, direktören Per Mosseby, Sveriges Kommuner och Landsting, CTO Valter Nordh, SUNET, CIO & avdelningschefen it Peder Sjölander, Pensionsmyndigheten, styrelseledamoten Åke Strandberg, Vårdföretagarna, verksamhets-

utvecklaren Magnus Wallström, Skatteverket, kanslirådet Lena Warstrand, Justitiedepartementet, handläggaren Carl Önne, Myndigheten för samhällsskydd och beredskap, arkitekten Mikael Österlund, eSam.

Anna Fors entledigades från uppdraget som expert från och med den 10 februari 2017 och från och med samma dag förordnades verksamhetsutvecklaren Markus Bill, Försäkringskassan och handläggaren Björn Scharin, Post- och telestyrelsen att vara experter i utredningen. Per Mosseby entledigades med verkan från den 1 maj 2017 från uppdraget som expert och från och med samma dag förordnades sektionschefen Åsa Zetterberg, Sveriges Kommuner och Landsting att vara expert i utredningen. Den 27 november 2017 entledigades Lena Warstrand från uppdraget att vara expert.

Experterna har bidragit med värdefulla synpunkter på textutkast och på förslagen i betänkandet. Utredningen vill rikta ett särskilt tack till Eva Sartorius, Anna Månsson Nyhlén och Ulf Palmgren för betydelsefulla bidrag till utredningens arbete.

Som huvudsekreterare i utredningen förordnades Christine Annemalm den 22 juni 2016, som sekreterare i utredningen förordnades Hanna Nilo den 19 augusti 2016, Michiko Muto den 12 september 2016 och Sofia Larsdotter Carlsson den 8 maj 2017. Michiko Mutos anställning upphörde från och med den 31 augusti 2017.

Utredningen som antagit namnet Utredningen om effektiv styrning av nationella digitala tjänster, får härmed överlämna sitt slutbetänkande.

Stockholm i december 2017

Hans-Eric Holmqvist

/Christine Annemalm
Hanna Nilo
Sofia Larsdotter Carlsson

Innehåll

Bilagor

Sammanfattning

Utredningen bedömer att regeringen det senaste året genom en serie olika initiativ har markerat en tydlig förändring av inriktningen av politiken för den digitala förvaltningen. I flera avseenden innebär initiativen en tydlig omprövning av tidigare ställningstaganden. Det som pågår kan därför beskrivas som en omstart – reboot – av politiken för digitalisering inom den offentliga sektorn. De förslag som återges i detta slutbetänkande, liksom förslagen i utredningens delbetänkande, bygger vidare på dessa åtgärder och är avsedda att komplettera dem.

Effektiv styrning

Om styrningen ska vara effektiv måste den riktas direkt till den eller de offentliga myndigheter som ska styras. Styrningen behöver anpassas både till den eller de som ska styras och till den typ av verksamhet eller de förvaltningsgemensamma digitala funktioner som avses. För detta behöver riksdagen och regeringen använda och utforma en väl balanserad kombination av flera olika styrmedel, både bindande och icke-bindande, liksom finansiella och legala. En effektiv finansiell styrning och finansiering av förvaltningsgemensamma digitala funktioner innebär att riksdagen och regeringen måste styra resurserna utifrån ett förvaltningsövergripande perspektiv och att kraven på kvalitet och effektivitet i dessa funktioner måste tillgodoses och bedömas på en förvaltningsövergripande nivå. Det måste finnas formella beslut om vad som ska vara det offentliga åtagandet i den nationella digitala infrastrukturen.

Av det skälet bör riksdagen lägga fast ett mål för den offentliga förvaltningens digitalisering. Detta ska ligga till grund för regeringens redovisning till riksdagen och styrningen av de offentliga myndigheterna. Det bör också finnas ett digitaliseringsmål för alla statliga myndigheter.

Regeringen behöver fastställa en särskild intern process för att bereda initiativ till samt utvärdera förvaltningsgemensamma digitala funktioner. Regeringen bör vidare besluta om en tidsbestämd övergripande plan – en strategi – för digitalisering och it i den offentliga förvaltningen samt förnya avsiktsförklaringen om digitalisering med Sveriges Kommuner och Landsting.

Statlig elektronisk identitetshandling

Utredningen bedömer att det bör vara ett statligt åtagande att det finns en tillförlitlig process för grundidentifiering, det vill säga att säkerställa individers identitet. Staten ska också utfärda en elektronisk identitetshandling för att på det viset säkerställa att medborgare och folkbokförda kan få en sådan. Den statliga elektroniska identitetshandlingen ska utfärdas samtidigt med en statlig fysisk identitetshandling. Den statliga elektroniska identitetshandlingen ska kunna användas för identifiering hos myndigheter men också kunna växlas till en mobil elektronisk identitetshandling. Därmed kan den statliga elektroniska identitetshandlingen fungera som en backup om t.ex. mobiltelefonen blir obrukbar.

Gränsöverskridande användning av elektroniska identitetshandlingar

Utredningen bedömer att det finns ett behov av att staten säkerställer att Sverige kan anmäla en elektronisk identitetshandling för användning i Europa enligt eIDAS-förordningen.[1] Sverige bör delta aktivt i det europeiska arbetet med att möjliggöra gränsöverskridande användning av elektroniska identitetshandlingar. När det gäller att öppna upp elektroniska tjänster anser utredningen att Sverige bör samverka med länder som har identitetsbeteckningar som liknar det svenska personnumret och som har anmält eller avser att anmäla en nationell elektronisk identitetshandling. Samarbetet bör präglas av ömsesidighet och tjänster som används frekvent bör prioriteras.

[1] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Det redan påbörjade nordiska samarbetet är en lämplig början. Regeringen bör ge uppdrag till myndigheter som har särskilt ofta förekommande ärenden rörande nordiska medborgare att delta i och stödja samarbetsprojekt med motsvarande myndigheter i de nordiska och baltiska länderna.

Som ett stöd för arbetet bör Skatteverket få i uppdrag att inrätta ett svenskt register över säkerställda kopplingar mellan europeiska elektroniska identitetshandlingar och svenska personnummer.

Mina meddelanden

Utredningen föreslår att Mina meddelanden ska regleras i en lag om infrastruktur för digital post. Av flera skäl anser utredningen att infrastrukturen Mina meddelanden behöver ännu tydligare reglering än vad som föreslogs i delbetänkandet.[2]

Anpassningar till dataskyddsförordningen[3] och fördelning av personuppgiftsansvaret behöver stöd i lag. Dessutom bör infrastrukturen öppnas upp för privata aktörer som avsändare, vilket också bör regleras i lag.

[2] SOU 2017:23, digitalforvaltning.nu, s. 33 ff.

[3] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

1 Författningsförslag

1.1 Förslag till lag om statlig elektronisk identitetshandling

Härigenom föreskrivs följande.

1 § I denna lag finns bestämmelser om statliga elektroniska identitetshandlingar.

2 § En statlig elektronisk identitetshandling kan utfärdas till den som är svensk medborgare eller folkbokförd i Sverige enligt folkbokföringslagen (1991:481).

3 § En statlig elektronisk identitetshandling innehåller följande uppgifter om en individ:

– nuvarande efternamn
– nuvarande förnamn
– födelsedatum
– personnummer

Regeringen eller den myndighet som regeringen bestämmer får besluta om att lägga till andra uppgifter om en individ i den elektroniska identitetshandlingen.

4 § En statlig elektronisk identitetshandling ska utfärdas på den högsta svenska tillitsnivån enligt tillitsramverket i lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

En statlig elektronisk identitetshandling ska utformas enligt de tekniska specifikationerna i lagen om infrastruktur för elektronisk

identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

5 § En statlig elektronisk identitetshandling ska finnas på de fysiska identitetshandlingar som regeringen bestämmer.

En statlig elektronisk identitetshandling har samma giltighetstid som den fysiska identitetshandling som den finns på.

6 § Ansökan om en statlig elektronisk identitetshandling ska göras hos de myndigheter (utfärdande myndigheter) som regeringen bestämmer.

7 § Ansökan om en statlig elektronisk identitetshandling ska göras i samband med ansökan om en fysisk identitetshandling. Uppgifterna i ansökan ska avges på heder och samvete eller under annan sådan försäkran. Sökanden är skyldig att inställa sig personligen.

8 § Sökanden är skyldig att i samband med ansökan om en statlig elektronisk identitetshandling styrka sin identitet och övriga personuppgifter.

9 § En ansökan om en statlig elektronisk identitetshandling ska avslås om förutsättningarna i 8 § inte är uppfyllda eller det som har föreskrivits av regeringen i fråga om ansökan inte har iakttagits och sökanden inte har följt en uppmaning att avhjälpa bristen.

10 § Regeringen eller de myndigheter som regeringen bestämmer får meddela ytterligare föreskrifter om ansökan och utfärdande av statliga elektroniska identitetshandlingar.

11 § Statliga myndigheter, kommuner och landsting ska erkänna identifiering med den statliga elektroniska identitetshandlingen i de e-tjänster där den statliga myndigheten, kommunen eller landstinget kräver elektronisk identifiering.

12 § Användare får använda den statliga elektroniska identitetshandlingen som underlag vid ansökan om en annan elektronisk identitetshandling.

13 § Regeringen eller de myndigheter som regeringen bestämmer får uppställa villkor för när en statlig elektronisk identitetshandling får användas som underlag för ansökan om en annan elektronisk identitetshandling.

14 § När en statlig elektronisk identitetshandling används som underlag vid ansökan om en elektronisk identitetshandling hos en annan utfärdare av elektroniska identitetshandlingar ska denne informera den utfärdande myndigheten.

15 § Den utfärdande myndigheten ska registrera vilka andra elektroniska identitetshandlingar som har skapats med den statliga elektroniska identitetshandlingen som underlag.

16 § En statlig elektronisk identitetshandling ska spärras om

– det fanns hinder mot att utfärda den statliga elektroniska identitetshandlingen vid tiden för utfärdandet och hindret fortfarande består,

– någon väsentlig uppgift som framgår av den statliga elektroniska identitetshandlingen är felaktig och inte längre gäller, eller

– någon annan än den som den statliga elektroniska identitetshandlingen är utställd till förfogar över den statliga elektroniska identitetshandlingen.

17 § Om en statlig elektronisk identitetshandling spärras ska den utfärdande myndigheten informera de utfärdare av elektroniska identitetshandlingar, som har använt den statliga elektroniska identitetshandlingen som underlag om detta.

18 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om förfarandet vid spärr av statliga elektroniska identitetshandlingar.

19 § Beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätt.

20 § Beslut enligt denna lag gäller omedelbart, om inte något annat anges i beslutet.

Denna lag träder i kraft den 1 januari 2020.

1.2 Förslag till lag om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling

Härigenom föreskrivs följande.

1 § I denna lag finns bestämmelser om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

I infrastrukturen för elektronisk identifiering ingår:

1. tillitsramverk,
2. tekniska specifikationer för elektronisk identifiering,
3. register med utfärdare och förlitande aktörer samt
4. modell för dialogruta med valbara elektroniska identitetshandlingar.

Svensk elektronisk identitetshandling är ett kvalitetsmärke för elektroniska identitetshandlingar som har granskats och godkänts mot tillitsramverket och de tekniska specifikationerna.

2 § I lagen avses med

1. *användare:* den som har en elektronisk identitetshandling,
2. *elektronisk identitetshandling:* en värdehandling som en användare kan använda för att identifiera sig elektroniskt,
3. *fysisk bärare:* en fysisk identitetshandling, en koddosa eller liknande,
4. *mobil bärare:* exempelvis en smarttelefon eller en surfplatta,
5. *förlitande aktör:* den som behöver verifiera en användares uppgifter vid identifiering mot en e-tjänst,
6. *utfärdare:* den som utfärdar en elektronisk identitetshandling till en användare,
7. *tillitsramverk:* ett graderat ramverk för tillförlitlighet i utfärdade elektroniska identitetshandlingar,
8. *tillitsnivå:* en nivå inom tillitsramverket,
9. *tekniska specifikationer:* tekniska krav som ställs på elektronisk identifiering,

10. *modell för dialogruta med valbara elektroniska identitetshandlingar:* gruppering av elektroniska identitetshandlingar som har kvalitetsmärket Svensk elektronisk identitetshandling och som presenterar dessa för användaren när denne ska identifiera sig elektroniskt.

Tillitsramverk

3 § Det ska finnas ett tillitsramverk för elektroniska identitetshandlingar, som löpande ska anpassas till väletablerade standarder och utvecklingen i övrigt samt de hot och risker som kan uppkomma på området.

4 § Den myndighet som regeringen bestämmer ska förvalta och utveckla tillitsramverket enligt 3 §.

Tekniska specifikationer

5 § Det ska finnas tekniska specifikationer för elektronisk identifiering, som löpande ska anpassas till väletablerade standarder, utvecklingen i övrigt, samt de hot och risker som kan uppkomma på området.

6 § Den myndighet som regeringen bestämmer ska förvalta och utveckla de tekniska specifikationerna enligt 5 §.

Kvalitetsmärket Svensk elektronisk identitetshandling

7 § Utfärdare av elektroniska identitetshandlingar kan ansöka om att granskas mot tillitsramverket enligt 3 § och de tekniska specifikationerna enligt 5 §. Den som uppfyller kraven på tillitsnivåerna och de tekniska specifikationerna ska godkännas.

8 § Godkända elektroniska identitetshandlingar får som ett tillägg till egen benämning även använda kvalitetsbenämningen Svensk elektronisk identitetshandling.

9 § Ansökan om att granskas mot tillitsramverket och de tekniska specifikationerna ska göras hos den myndighet som regeringen bestämmer. Samma myndighet ska godkänna att en elektronisk identitetshandling får använda kvalitetsbenämningen Svensk elektronisk identitetshandling.

Register med utfärdare av elektroniska identitetshandlingar och förlitande aktörer

10 § Det ska finnas ett register över utfärdare av elektroniska identitetshandlingar med kvalitetsmärket Svensk elektronisk identitetshandling och förlitande aktörer som är anslutna till valfrihetssystem enligt lagen om valfrihetssystem i fråga om funktioner för elektronisk identitetskontroll.

11 § Den myndighet som regeringen bestämmer ska förvalta och utveckla registret enligt 10 §.

12 § Förlitande aktörer som är anslutna till valfrihetssystem enligt lagen om valfrihetssystem i fråga om funktioner för elektronisk identitetskontroll ska registreras i registret med utfärdare och förlitande aktörer.

Modell för dialogruta med valbara elektroniska identitetshandlingar

13 § Det ska finnas en modell för dialogruta med valbara elektroniska identitetshandlingar. En dialogruta med valbara elektroniska identitetshandlingar ska visa de elektroniska identitetshandlingar som ingår i valfrihetssystem som tillhandahålls enligt lagen om valfrihetssystem i fråga om funktioner för elektronisk identitetskontroll samt den statliga elektroniska identitetshandlingen.

14 § Den myndighet som regeringen bestämmer ska förvalta och utveckla modellen enligt 13 §.

15 § Statliga myndigheter, kommuner och landsting ska använda modellen för dialogruta med valbara elektroniska identitetshandlingar i de e-tjänster där den statliga myndigheten, kommunen eller landstinget kräver att individen ska identifiera sig elektroniskt.

16 § Regeringen får besluta om undantag till skyldigheten i 15 § om det finns särskilda skäl.

Denna lag träder i kraft den 1 januari 2020.

1.3 Förslag till lag om infrastruktur för digital post

Härigenom föreskrivs följande.

Allmänna bestämmelser

1 § Den myndighet som regeringen bestämmer (myndigheten) ska tillhandahålla en infrastruktur för digital post.

2 § Denna lag gäller vid behandling av personuppgifter inom infrastrukturen. Vid sådan behandling gäller lagen endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

3 § I denna lag avses med

1. *ankomstkontroll:* att leverantören av brevlådetjänster för digital post utför kontroll mot förmedlingsadressregistret att avsändaren är ansluten.
2. a*vsändare:* offentlig myndighet eller juridisk person som skickar digital post till en mottagare inom infrastrukturen.
3. a*vsändningskontroll:* att avsändaren utför kontroll mot förmedlingsadressregistret att mottagaren är ansluten till infrastrukturen, i så fall hos vilken leverantör mottagarens brevlådetjänst för digital post finns samt att avsändaren får sända digital post till mottagaren.
4. *brevlådetjänster för digital post:* den del inom infrastrukturen som lagrar digital post efter att den har gjorts tillgänglig för mottagaren.
5. *digital post:* meddelanden genom digitala kanaler mellan olika aktörer i infrastrukturen.
6. *förmedlare:* en juridisk person eller en individ som utför uppdrag åt en avsändare genom att vidarebefordra digital post.
7. *förmedlingsadressregister:* det register som innehåller uppgifter, däribland personuppgifter, om de anslutna i infrastrukturen.

8. *leverantör av brevlådetjänster för digital pos*t: en juridisk person eller en individ som tillhandahåller brevlådetjänster för digital post.

9. *mottagare:* individer och företag som anslutit sig till förmedlingsadressregistret och i sin brevlådetjänst för digital post tar emot digital post inom infrastrukturen.

10. *privat utförare:* en juridisk person eller en individ som har hand om en kommunal angelägenhet.

I övrigt gäller definitioner i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

4 § Infrastrukturen består av förmedlingsadressregister, brevlådor för digital post, valfrihetssystem enligt lagen om valfrihet om elektroniska brevlådor samt vad regeringen, eller den myndighet regeringen bestämmer, har beslutat i form av föreskrifter.

5 § Myndigheten får tillhandahålla brevlådetjänster för digital post till mottagare som enbart tar emot digital post från avsändare enligt 11 §.

6 § Till stöd för förmedling av digital post får myndigheten föra ett förmedlingsadressregister över anslutna enligt 11–15 §§. Syftet med registret är att ge de som är anslutna till infrastrukturen möjlighet att behandla personuppgifter i sin digitala postverksamhet på ett ändamålsenligt sätt och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Om rätten att få meddelande från myndighet via infrastrukturen

7 § Om en ansluten mottagare begärt att en statlig myndighet ska sända digital post genom infrastrukturen får detta underlåtas endast om särskilda skäl finns.

Förhållandet till annan lagstiftning

8 § Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Vid behandling av personuppgifter enligt denna lag gäller lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av denna lag eller föreskrifter som har meddelats med anslutning till den.

Ändamål

9 § Personuppgifter får bara behandlas om det behövs för att

1. hantera digital post i syfte att kunna utföra en arbetsuppgift inom en författningsreglerad verksamhet hos någon av de som anslutit sig till infrastrukturen, eller
2. lagra och bearbeta digital post som avses i 1 p. i syfte att erbjuda tilläggstjänster för brevlådeinnehavarna.

10 § Personuppgifter som behandlas eller har behandlats enligt 9 § får även behandlas om det behövs för att fullgöra uppgiftslämnande i överensstämmelse med lag eller förordning.

I ett enskilt fall får personuppgifter som behandlas eller har behandlats enligt 9 § även behandlas för att tillhandahålla information för något annat ändamål än det som anges, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in.

Anslutning

11 § Till infrastrukturen ska som avsändare anslutas myndigheter under regeringen om inte regeringen har beslutat annat. Till infrastrukturen får kommuner och landsting ansluta sig som avsändare. Vidare får privata utförare av kommunala angelägenheter ansluta sig som avsändare enligt vad som föreskrivs i denna lag.

Regeringen får besluta att som avsändare får företag och organisationer som utför en uppgift av allmänt intresse ansluta sig. Regeringen får besluta om att denna anslutning ska villkoras med att företaget eller organisationen ska ha avtal med leverantör av brevlådetjänster för digital post.

12 § Till infrastrukturen får individer och företag ansluta sig som mottagare om de anmält att de vill ta emot digital post från anslutna avsändare. Varje mottagare har genom sin anmälan tillgång till en brevlådetjänst för digital post.

13 § Till infrastrukturen får leverantör av brevlådetjänster för digital post ansluta sig.

14 § Den som ansluter sig till infrastrukturen ska registreras i förmedlingsadressregistret.

Avsändnings- och ankomstkontroll

15 § Avsändare ska före sändning av digital post kontrollera i förmedlingsadressregistret om mottagaren är ansluten till infrastrukturen och i så fall hos vilken leverantör mottagarens brevlådetjänst för digital post finns samt att avsändaren får sända digital post till mottagaren. Om mottagaren inte är ansluten till infrastrukturen eller inte tar emot meddelanden från den aktuella avsändaren får den digitala posten inte sändas via infrastrukturen.

16 § Förmedlare ska före sändning av digital post kontrollera i förmedlingsadressregistret om mottagaren fortfarande är ansluten till infrastrukturen och om avsändaren får sända digital post till mottagaren. Om mottagaren inte är ansluten till infrastrukturen eller inte tar emot meddelanden från den aktuella avsändaren får den digitala posten inte sändas via infrastrukturen.

17 § Leverantör av brevlådetjänster för digital post ska vid ankomst av digital post kontrollera i förmedlingsadressregistret att avsändaren fortfarande är ansluten till infrastrukturen. Om avsändaren inte är ansluten eller har något civilrättsligt avtal med mottagaren om digital brevlådetjänst ska meddelandet inte mottas.

Personuppgiftsansvar

18 § Myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför när den tillhandahåller förmedlingsadressregistret.

19 § Avsändaren är personuppgiftsansvarig för behandling av personuppgifter till dess att leverantör av brevlådetjänster för digital post genom ankomstkontroll godkänt mottagandet enligt 17 §.

Avsändaren är vidare personuppgiftsansvarig för behandling av uppgifter som leverantören utför på avsändarens begäran efter att meddelandet gjorts tillgängligt för mottagaren.

20 § Leverantör av brevlådetjänster för digital post är personuppgiftsansvarig för behandling av uppgifter efter att ankomstkontroll genomförts med undantag för förhållanden enligt 19 § andra stycket.

Leverantören är vidare personuppgiftsansvarig för behandling av uppgift som denne erbjuder mottagaren.

Anslutning av privata utförare av kommunala angelägenheter

21 § Privata utförare av kommunala angelägenheter får ansluta sig på begäran av kommun eller landsting som är ansluten till infrastrukturen. När utförarens uppdrag har upphört ska kommunen anmäla detta till den myndighet som regeringen beslutar för att ta bort registreringen på den privata utföraren som avsändare i förmedlingsadressregistret.

En förutsättning för anmälan ska vara att kommunen eller landstinget är ansluten samt har kommit överens med utföraren att denne ska använda infrastrukturen.

Kommunen eller landstinget ska kontrollera att utföraren använder infrastrukturen på avsett sätt. Om kommunen eller lands-

tinget finner att utföraren brister härvidlag eller då uppdraget upphör ska anmälan återkallas.

Föreskrifter

22 § Regeringen eller den myndighet som regeringen bestämmer får med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. inrättande och drift av infrastrukturen,
2. den längsta tid under vilken personuppgifter får behandlas,
3. säkerhetsåtgärder till skydd för personuppgifter,
4. behörighets- och sökbegränsningar, och
5. vilka verksamheter som regeringen vill ge möjlighet att ansluta som avsändare i infrastrukturen samt villkor för dem.

Ersättning till leverantör av brevlådetjänster för digital post

23 § När myndigheten tillämpar lagen om valfrihet om digitala brevlådor ska regeringen eller den myndighet regeringen bestämmer fastställa ersättning till leverantör av brevlådetjänster för digital post anslutna enligt 13 §. Vad som där fastställs ska inte tillämpas för den som anslutits enligt 11 § andra stycket.

Denna lag träder i kraft den 1 juli 2019.

1.4 Förslag till lag om valfrihet om digitala brevlådor

Härigenom föreskrivs följande.

1 § Skatteverket får besluta att tillhandahålla valfrihetssystem för digitala brevlådor enligt lagen om infrastruktur för digital post. Med valfrihetssystem menas ett förfarande där mottagaren har rätt att välja den leverantör som ska utföra tjänsten och som Skatteverket har godkänt och tecknat avtal med.

2 § När Skatteverket tillhandahåller valfrihetssystem enligt denna lag ska myndigheten tillämpa lagen (2008:962) om valfrihetssystem. I stället för det som sägs i 2 kap. 3 § första meningen, 6 och 7 §§ lagen om valfrihetssystem ska med

1. leverantör avses den som på marknaden tillhandahåller tjänster som nämns i 1 §,
2. tjänst avses sådan tjänst som nämns i 1 §, och
3. upphandlande myndighet avses Skatteverket.

Denna lag träder i kraft den 1 juli 2019.

1.5 Förslag till lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Härigenom föreskrivs i fråga om lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering att det i lagen ska införas nio nya paragrafer, tre nya rubriker samt en ny rubriknivå med följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	Tillsynsmyndigheten
	5 §
	Tillsynsmyndigheten har rätt att på begäran få de upplysningar och handlingar som behövs för tillsynen.
	Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som står under tillsyn bedrivs.
	Tillsynsmyndigheten har rätt att få biträde av Kronofogdemyndigheten för tillsyn enligt första och andra styckena.
Avgifter	*Avgifter*
	7 §
	Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om skyldighet för tillhandahållare av betrodda tjänster att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.
Överklagande	*Överklagande*
	8 §
	Tillsynsmyndighetens beslut enligt EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen, samt enligt denna lag och föreskrifter som har

meddelats med stöd av lagen, får överklagas till allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Noden

9 §

Den myndighet som regeringen utser (nodmyndigheten) ska ansvara för att tillhandahålla en offentlig förbindelsepunkt (nod) för gränsöverskridande elektronisk identifiering och att den fungerar i enlighet med EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen.

Regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om noden.

10 §

För att användare ska kunna identifieras får nodmyndigheten behandla de personuppgifter som kommer till noden. Vilka personuppgifter som kommer till noden regleras i bilagan till Kommissionens genomförandeförordning (EU) 2015/1501.

Nodmyndigheten är personuppgiftsansvarig för de behandlingar av personuppgifter som utförs i noden.

11 §

Nodmyndigheten får behandla (tekniska) uppgifter för de aktörer vars uppgifter ska behandlas av noden. Myndigheten får även behandla de personuppgifter som är nödvändiga för att säkerställa behörigheter för aktörernas ombud.

12 §

Alla myndigheter som, för att ge åtkomst till sina nättjänster, omfattas av kraven på elektronisk identifiering enligt EU:s förordning om elektronisk identifiering, ska ansluta till den svenska offentliga noden.

Myndigheter som inte omfattas av förordningens krav får ansluta till den svenska offentliga noden.

13 §

Privata aktörer får ansluta till den svenska offentliga noden.

Regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om skyldighet för privata aktörer att betala avgift för att ansluta till noden enligt denna lag.

14 §

Alla som är anslutna till noden ska utan otillbörligt dröjsmål underrätta nodmyndigheten om alla händelser som påverkat funktionalitet eller säkerhet i noden.

Anmälan av svenska medel för elektronisk identifiering

15 §

Den myndighet som regeringen utser ansvarar för anmälan av svenska medel för elektronisk identifiering för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering. (anmälande myndighet)

Regeringen eller den myndighet som regeringen bemyndigar får meddela föreskrifter om hur anmälan ska gå till.

16 §

För att kunna anmälas för gränsöverskridande elektronisk identifiering ska ett svenskt medel för elektronisk identifiering

1. vara kvalitetsgranskat av digitaliseringsmyndigheten,

2. endast utfärdas till medborgare eller folkbokförda i Sverige,

3. ingå i valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering, och

4. vara utfärdat av en aktör som har tecknat försäkring som täcker ersättning för skada som åsamkats fysiska eller juridiska personer avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla de skyldigheter som avses i artikel 7 i EU:s förordning om elektronisk identifiering.

17 §

Anmälande myndighet ansvarar även för att tillfälligt upphäva, återkalla, återinföra och dra tillbaka elektroniska identitetshandlingar vid säkerhetsincidenter enligt artikel 10 i EU:s förordning om elektronisk identifiering.

Denna lag träder i kraft den 29 september 2018.

1.6 Förslag till lag om ändring i lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering

Härigenom föreskrivs att rubriken till lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering samt 1, 2, 4, 11, 16, 19 och 22 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Lag om valfrihetssystem i fråga om *tjänster* för elektronisk *identifiering*	**Lag om valfrihetssystem i fråga om *funktioner* för elektronisk *identitetskontroll***
1 §[4]	
I denna lag finns bestämmelser om tillämpning av valfrihetssystem i fråga om *tjänster* för elektronisk *identifiering*.	I denna lag finns bestämmelser om tillämpning av valfrihetssystem i fråga om *funktioner* för elektronisk *identitetskontroll.*
Lagen gäller när en upphandlande myndighet har	*Den myndighet som regeringen bestämmer (den upphandlade myndigheten) ska tillhandahålla valfrihetssystem för funktioner för elektronisk identitetskontroll.*
1. beslutat att tillämpa valfrihetssystem i fråga om tjänster för elektronisk identifiering av enskilda i myndighetens elektroniska tjänster,	*Statliga myndigheter, kommuner och landsting med behov av funktioner för elektronisk identitetskontroll ska ansluta sig till valfrihetssystem som den upphandlande myndigheten tillhandahåller.*
2. anslutit sig till ett system för säker elektronisk identifiering som tillhandahålls av den myndighet som regeringen bestämmer, och	*Regeringen får besluta om undantag från skyldigheten i andra stycket om det finns särskilda skäl.*
3. uppdragit åt den myndighet som avses i 2 att i den upphandlande myndighetens namn administrera valfrihetssystemet enligt 3–14 §§, föra dess talan i	

[4] Senaste lydelse 2013:311.

samband med mål om rättelse enligt 16 § och i förekommande fall vidta rättelse enligt 17 §.

2 §[5]

Med valfrihetssystem avses i denna lag ett förfarande där den enskilde har rätt att välja den leverantör som ska utföra *tjänsten* och som *en upphandlande myndighet* har godkänt och tecknat kontrakt med.

Termerna upphandlingsdokument, kontrakt och upphandlande myndighet har i denna lag samma betydelse som i lagen (2016:1145) om offentlig upphandling.

Med valfrihetssystem avses i denna lag ett förfarande där den enskilde har rätt att välja den leverantör som ska utföra *identitetskontrollen* och som *den upphandlande myndigheten* har godkänt och tecknat kontrakt med.

Termerna upphandlingsdokument, kontrakt och upphandlande myndighet har i denna lag samma betydelse som i lagen (2016:1145) om offentlig upphandling.

4 §[6]

En upphandlande myndighet som har beslutat att inrätta eller förändra ett valfrihetssystem ska *annonsera* på en nationell webbplats som har upprättats för ändamålet. Ansökningar ska löpande begäras in genom sådan annonsering.

Upphandlingsdokumenten ska finnas tillgängliga på webbplatsen tillsammans med annonsen.

När den upphandlande myndigheten har beslutat att inrätta eller förändra ett valfrihetssystem ska *det annonseras* på en nationell webbplats som har upprättats för ändamålet. Ansökningar ska löpande begäras in genom sådan annonsering.

Upphandlingsdokumenten ska finnas tillgängliga på webbplatsen tillsammans med annonsen.

[5] Senaste lydelse 2016:1161.
[6] Senaste lydelse 2016:1161.

11 §[7]

Den upphandlande myndigheten får begära att sökanden visar att det inte finns någon grund för att utesluta denne med stöd av 10 § första stycket 1, 2 eller 5.

Den upphandlande myndigheten ska som bevis för att det inte finns grund för att utesluta en sökande godta utdrag ur ett officiellt register eller annan likvärdig handling när det gäller ett förhållande som avses i 10 § första stycket 1 eller 2 och intyg från en behörig myndighet när det gäller ett förhållande som avses i 10 § första stycket 5.

Om, i fråga om en sökande som inte är medborgare i eller bosatt i Sverige, sådana handlingar eller intyg som avses i andra stycket inte utfärdas i sökandens hemland eller ursprungsland, eller inte omfattar samtliga de fall som avses i 10 § första stycket 1, 2 och 5, får de ersättas med en utsaga som har avgetts på heder och samvete eller av en liknande försäkran. En sådan sökande får också föreläggas att visa att det inte finns grund för att utesluta denne med stöd av 10 § första stycket 3 eller andra stycket.

Om en sökande är registrerad i en officiell förteckning över godkända *tjänstetillhanda-*

Den upphandlande myndigheten får begära att sökanden visar att det inte finns någon grund för att utesluta denne med stöd av 10 § första stycket 1, 2 eller 5.

Den upphandlande myndigheten ska som bevis för att det inte finns grund för att utesluta en sökande godta utdrag ur ett officiellt register eller annan likvärdig handling när det gäller ett förhållande som avses i 10 § första stycket 1 eller 2 och intyg från en behörig myndighet när det gäller ett förhållande som avses i 10 § första stycket 5.

Om, i fråga om en sökande som inte är medborgare i eller bosatt i Sverige, sådana handlingar eller intyg som avses i andra stycket inte utfärdas i sökandens hemland eller ursprungsland, eller inte omfattar samtliga de fall som avses i 10 § första stycket 1, 2 och 5, får de ersättas med en utsaga som har avgetts på heder och samvete eller av en liknande försäkran. En sådan sökande får också föreläggas att visa att det inte finns grund för att utesluta denne med stöd av 10 § första stycket 3 eller andra stycket.

Om en sökande är registrerad i en officiell förteckning över godkända *tillhandahållare*

[7] Senaste lydelse 2013:311.

hållare i ett land inom Europeiska ekonomiska samarbetsområdet, ska den upphandlande myndigheten utgå från att sökanden inte kan uteslutas som leverantör enligt 10 § första stycket 1–5.	*av identitetskontroll* i ett land inom Europeiska ekonomiska samarbetsområdet, ska den upphandlande myndigheten utgå från att sökanden inte kan uteslutas som leverantör enligt 10 § första stycket 1–5.
16 §[8]	
En leverantör som gör gällande att *en upphandlande myndighet* har brutit mot en bestämmelse i denna lag, får ansöka om rättelse hos allmän förvaltningsdomstol. Endast den sökande som inte har godkänts får ansöka om rättelse av beslut enligt 12 §. En ansökan om rättelse ska vara skriftlig.	En leverantör som gör gällande att *den upphandlande myndigheten* har brutit mot en bestämmelse i denna lag, får ansöka om rättelse hos allmän förvaltningsdomstol. Endast den sökande som inte har godkänts får ansöka om rättelse av beslut enligt 12 §. En ansökan om rättelse ska vara skriftlig.
19 §[9]	
En upphandlande myndighet som inte har följt bestämmelserna i denna lag ska ersätta sökanden för därigenom uppkommen skada. Talan om skadestånd ska väckas vid allmän domstol. En skadeståndstalan som grundar sig på ett beslut att inte godkänna en sökande ska väckas inom ett år från dagen för beslutet. Väcks inte talan i tid, är rätten till skadestånd förlorad.	*Om den upphandlande myndigheten* inte har följt bestämmelserna i denna lag ska *myndigheten* ersätta sökanden för därigenom uppkommen skada. Talan om skadestånd ska väckas vid allmän domstol. En skadeståndstalan som grundar sig på ett beslut att inte godkänna en sökande ska väckas inom ett år från dagen för beslutet. Väcks inte talan i tid, är rätten till skadestånd förlorad.

[8] Senaste lydelse 2013:311.
[9] Senaste lydelse 2013:311.

22 §[10]

Den myndighet som regeringen bestämmer utövar tillsyn över att denna lag följs.	Den myndighet som regeringen bestämmer utövar tillsyn över att denna lag följs.
Tillsynsmyndigheten får inhämta sådana upplysningar som är nödvändiga för tillsynen från *en upphandlande myndighet och från den myndighet som avses i 1 § andra stycket 2.* Upplysningarna ska i första hand inhämtas genom ett skriftligt förfarande. Om det på grund av materialets omfång, brådska eller något annat förhållande är lämpligare, får upplysningarna i stället inhämtas genom besök hos den upphandlande myndigheten eller den myndighet som avses i 1 § *andra stycket 2*.	Tillsynsmyndigheten får inhämta sådana upplysningar som är nödvändiga för tillsynen från *den upphandlande myndigheten och från den myndighet som avses i 1 § tredje stycket.* Upplysningarna ska i första hand inhämtas genom ett skriftligt förfarande. Om det på grund av materialets omfång, brådska eller något annat förhållande är lämpligare, får upplysningarna i stället inhämtas genom besök hos den upphandlande myndigheten eller den myndighet som avses i 1 § *tredje stycket*.
En upphandlande myndighet och den myndighet som avses i 1 § andra stycket 2 är skyldig att tillhandahålla de upplysningar som tillsynsmyndigheten begär för sin tillsyn.	*Den upphandlande myndigheten och den myndighet som avses i 1 § tredje stycket* är skyldig att tillhandahålla de upplysningar som tillsynsmyndigheten begär för sin tillsyn.

Denna lag träder i kraft den 1 januari 2020.

[10] Senaste lydelse 2013:311.

1.7 Förslag till förordning med mål för de statliga myndigheternas digitaliseringsarbete

Härigenom föreskrivs följande

Förordningens tillämpningsområde

1 § Denna förordning gäller för myndigheterna under regeringen.

Mål för de statliga myndigheternas digitaliseringsarbete

2 § Målet för de statliga myndigheternas digitaliseringsarbete är att den statliga förvaltningens användning av digitala medel ska leda till att det blir så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av den statliga förvaltningens service. De statliga myndigheternas användning av digitala medel ska vara säker samt öka kvaliteten och effektiviteten i den offentliga förvaltningen som helhet.

Redovisning

3 § Myndigheterna ska i sin årsredovisning redovisa sina resultat i förhållande till regeringens mål i 2 § i denna förordning för de statliga myndigheternas digitaliseringsarbete. Resultatredovisningen ska lämnas enligt 3 kap. 1 § förordningen (2000:605) om årsredovisning och budgetunderlag.

Denna förordning träder i kraft den 1 januari 2019.

1.8 Förslag till förordning om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling

Härigenom föreskrivs följande

1 § Digitaliseringsmyndigheten ska förvalta och utveckla tillitsramverket enligt 3 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

2 § Digitaliseringsmyndigheten ska förvalta och utveckla de tekniska specifikationerna enligt 5 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

3 § Digitaliseringsmyndigheten ska granska elektroniska identitetshandlingar enligt 9 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling elektroniska identitetshandlingar samt godkänna att en elektronisk identitetshandling får använda benämningen Svensk elektronisk identitetshandling.

4 § Digitaliseringsmyndigheten ska förvalta och utveckla registret med utfärdare av elektroniska identitetshandlingar och förlitande aktörer enligt 10 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

5 § Digitaliseringsmyndigheten ska förvalta och utveckla modellen för dialogruta med valbara elektroniska identitetshandlingar enligt 13 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

Denna förordning träder i kraft den 1 januari 2020.

1.9 Förslag till förordning om infrastruktur för digital post

Härigenom föreskrivs följande.

1 § Skatteverket ska tillhandahålla en infrastruktur för digital post och vara myndigheten enligt lagen om infrastruktur för digital post.

2 § Skatteverket får meddela föreskrifter enligt 23 § lagen om infrastruktur för digital post.

3 § Som avsändare i infrastrukturen för digital post får enligt 24 § 4 p. lagen om infrastruktur för digital post friskolor, banker, försäkringsföretag, pensionsförvaltare, kreditupplysningsföretag, apotek, bilbesiktningsföretag och bostadsföretag ansluta sig.

4 § De avsändare som ansluts enligt 3 § denna förordning ska ha avtalat om att skicka digital post med leverantörerna av brevlådetjänster för digital post som är anslutna till infrastrukturen.

Denna förordning träder i kraft den 1 juli 2019.

1.10 Förslag till förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Härigenom föreskrivs i fråga om förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering att det i förordningen ska införas fyra nya paragrafer med följande lydelse.

6 § Digitaliseringsmyndigheten ska vara nodmyndighet enligt 9 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Digitaliseringsmyndigheten ska vara kontaktpunkt för Europeiska kommissionen i frågor som rör gränsöverskridande elektronisk identifiering.

7 § Digitaliseringsmyndigheten får meddela föreskrifter om

1. hur aktörer ska ansluta till noden, och
2. rapportering av händelser som påverkat funktionaliteten eller säkerheten i noden.

8 § Digitaliseringsmyndigheten ska ansvara för anmälningar till kommissionen av svenska medel för elektronisk identifiering för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering.

9 § Digitaliseringsmyndigheten ska vid större förändringar av det system som den svenska noden omfattar, begära en teknisk säkerhetsgranskning av Försvarets radioanstalt. Granskningsförfarandet får ta max tre månader från det att digitaliseringsmyndigheten ansökt om granskning.

Denna förordning träder i kraft den 29 september 2018.

1.11 Förslag till förordning om ändring i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte (I)

Härigenom föreskrivs att det i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte ska införas en ny paragraf, 2 a, med följande lydelse.

2 a § Myndigheter får samverka utanför sina verksamhetsområden i frågor om digitalisering av den offentliga förvaltningen.

Denna förordning träder i kraft den 1 januari 2019.

1.12 Förslag till förordning om ändring i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte (II)

Härigenom föreskrivs att 5 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte ska upphöra att gälla den 1 juli 2019.

Denna förordning träder i kraft den 1 juli 2019.

2 Utredningens uppdrag och arbete

2.1 Uppdraget

Regeringen beslutade vid regeringssammanträde den 19 maj 2016 att tillkalla en särskild utredare för att analysera och lämna förslag till effektiv styrning av utveckling, införande och förvaltning av nationella digitala tjänster. I uppdraget har ingått att, med utgångspunkt i de nationella digitala tjänsterna Mina meddelanden och Svensk e-legitimation, analysera och lämna förslag till utformning av organisering och ansvarsfördelning för de nationella digitala tjänsterna, åtgärder och incitament för att uppnå en ökad användning av de nationella digitala tjänsterna, och samverkan mellan offentlig och privat sektor i tillhandahållandet av de nationella digitala tjänsterna. Utredaren skulle även analysera och lämna förslag om vissa specifika frågor som rör Svensk e-legitimation och Mina meddelanden, samt återstående frågor om den nationella tillämpningen av EU-förordningen om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen[1]) m.m.

I uppdraget har ingått att, i ett delbetänkande senast den 15 mars 2017, redovisa hur privata utförare av offentligfinansierad verksamhet ska kunna ansluta som avsändare inom Mina meddelanden, hur en övergång för privatpersoner och företag till digital myndighetspost kan genomföras i praktiken och förslag till utformning av en ersättningsmodell för de brevlådeoperatörer som tillhandahåller brevlådor inom ramen för Mina meddelanden.

[1] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Regeringen beslutade vid regeringssammanträde den 24 november 2016 att utvidga uppdraget. I tilläggsdirektivet fick utredaren i uppdrag att analysera hur digitaliseringen i den offentliga sektorn kan stärkas genom att, inom ramen för den befintliga myndighetsstrukturen, samla ansvaret för dessa frågor till en myndighet. Enligt uppdraget skulle utredaren med utgångspunkt i analysen lämna förslag till nödvändiga författningsändringar och övriga åtgärder som krävs för att en myndighet så snart som möjligt ska kunna ges denna uppgift. Utredaren fick dessutom i uppdrag att lämna förslag till en reglering som innebär en skyldighet för lämpliga statliga och kommunala myndigheter att ansluta sig till tjänsten Mina meddelanden. Den del av uppdraget som avsåg att samla ansvaret för digitaliseringen i den offentliga sektorn skulle redovisas senast den 15 mars 2017. Samtidigt förlängdes utredningstiden med två månader till senast den 31 december 2017.

2.2 Utredningsarbetet

I arbetet med slutbetänkandet har utredningen genomfört sex möten med expertgruppen. Utredningen har vidare samrått och diskuterat utredningsfrågorna med ett stort antal offentliga myndigheter och organisationer. Utredningen har deltagit vid flera möten med Sveriges Kommuner och Landstings (SKL) beredning för digitalisering och med SKL:s styrgrupp Center för eSamhället. Utredningen har även samrått med Integritetskommittén, Utredningen om rättsliga förutsättningar för en digitalt samverkande förvaltning, Servicekontorsutredningen och 2017 års ID-kortsutredning.

Utredningen har genomfört två workshops, en om elektronisk identifiering enligt eIDAS-förordningen och en om betrodda tjänster enligt eIDAS-förordningen.

Utredningen har deltagit i två workshops anordnade av EU-kommissionen, den ena om en marknadsföringsplan för att stimulera användningen av elektroniska identitetshandlingar och betrodda tjänster, och den andra om elektronisk identifiering inom banksektorn.

Utredningen har under hösten 2017 skickat ut en enkät till ett tjugotal offentliga myndigheter som har påbörjat anpassningsarbetet till eIDAS-förordningen för att få veta vilka konsekvenser de ser av eIDAS-förordningens krav. Utredningen har under samma period

även skickat en enkät till ett tiotal medlemsstater i EU för att få en uppfattning om hur de ser på anpassningar och krav med anledning av eIDAS-förordningen. Under hösten 2017 genomfördes ett möte med representanter för de leverantörer av digitala brevlådetjänster som anslutit sig till Mina meddelanden.

2.3 Utredningens utgångspunkter och inriktning

Tilläggsdirektivet har påverkat utredningens arbete även i de delar som det inte direkt berörde. Utredningen har under arbetets gång erfarit att regeringen avsett genomföra utredningens förslag om ett samlat myndighetsansvar för digitalisering av offentlig verksamhet. Vidare har regeringen beslutat om en ny organisation för statliga lokalkontor från och med den 1 januari 2019 och om att låta utreda frågan om vilka identitetshandlingar staten ska utfärda och vilka myndigheter som ska svara för denna uppgift. Tillsammans har detta varit en viktig inriktning för arbetet med de frågor som behandlas i detta betänkande.

Det bör framhållas att Sverige och den Europeiska Unionen befinner sig i en omfattande förändringsprocess när det gäller digitalisering. Den digitala mognaden hos unionens medlemsstater skiljer sig betydligt. Tillsammans medför detta svårigheter att göra precisa bedömningar om utvecklingen. Det gäller särskilt den europeiska marknadens vilja att utnyttja olika former av digitala tjänster. Utredningen utgår från att den myndighet som ska inleda sitt arbete den 1 september 2018 följer denna utveckling, vägleder myndigheterna och ger strategiskt stöd till regeringen.

Utredningens uppdrag och avgränsning är att lämna förslag till effektiv styrning av nationella digitala tjänster i en samverkande förvaltning, inte att lämna förslag till nya eller fler digitala tjänster. Utredningen har en förvaltningspolitisk utgångspunkt vilket innebär att det är individer och företag som står i fokus för den digitala förvaltningsutvecklingen samtidigt som förvaltningen ska effektivisera och hushålla väl med skattebetalarnas pengar.

Utredningen instämmer i det perspektiv som lyftes av E-delegationen och som betonade e-förvaltningens betydelse för samhällets samlade utvecklingsförmåga och innovationskraft. Med detta perspektiv blir digitaliseringen av förvaltningen inte en förvaltnings-

intern angelägenhet utan en vital del av arbetet med att utveckla den nationella digitala infrastrukturen. Digitaliseringen har därför inte bara som syfte att underlätta för individer och företag. Den syftar också till att främja konkurrenskraften.

Med detta breda perspektiv finns det också skäl att uppmärksamma de risker som följer av en alltmer utvecklad användning och spridning av individrelaterad information. Utredningen har därför valt att integrera frågor om informationssäkerhet, integritetsskydd och personuppgiftsansvar i utvecklingen och genomförandet av den digitala förvaltningen. Dessa frågor har därför kommit att ta en större plats i utredningsarbetet än direktiven gett uttryck för och utredningen lämnar även flera förslag som rör frågor om informationssäkerhet.

2.4 Betänkandets disposition

Betänkandet kan delas in i fyra delar, effektiv styrning och informationssäkerhet (kap. 3–9), elektroniska identitetshandlingar (kap. 10–15), eIDAS-förordningen (kap. 16–20) och Mina meddelanden (kap. 21).

Dessutom bifogar utredningen eIDAS-förordningen i sin helhet.

2.5 Användning av några begrepp

2.5.1 digitaliseringsmyndigheten

Regeringen har beslutat att inrätta en myndighet för digitalisering av den offentliga sektorn.[2] I skrivande stund är det inte klart vad myndigheten kommer att ha för namn. I betänkandet benämns myndigheten digitaliseringsmyndigheten.

[2] Dir. 2017:117.

2.5.2 eIDAS-förordningen och terminologin

Med eIDAS-förordningen följer en begreppsflora som inte alltid stämmer överens med den svenska. Utredningen har försökt anpassa skrivningarna så mycket som möjligt men det finns exempel på begrepp i eIDAS-förordningen som inte alltid är naturliga att använda i svenska texter. I eIDAS-förordningen används t.ex. begreppet nättjänst i stället för e-tjänst.

Artikel 3 i eIDAS-förordningen innehåller definitioner av 41 begrepp som används i förordningen. Utredningen hänvisar till dessa definitioner när det gäller förklaringar av begrepp som används i sammanhang med eIDAS-förordningen.

2.5.3 Medel för att genomföra kärnverksamhet och kommunala angelägenheter

Förvaltningsgemensamma digitala funktioner är, enligt utredningens definition, *medel* dvs. redskap, verktyg, metoder m.m. för offentliga myndigheter att genomföra sin kärnverksamhet och angelägenheter. På samma sätt används begreppet *medel* för elektronisk identifiering i eIDAS-förordningen som ett redskap eller verktyg för elektronisk identifiering.

Kärnverksamhet och angelägenheter är en offentlig myndighets huvudsakliga uppgifter enligt instruktionen eller andra styrande dokument. Det kan beskrivas som myndighetens unika verksamhet eller den verksamhet som myndigheten är inrättad för att uträtta. Vad som är att beakta som kärnverksamhet kan variera över tid, med uppgifterna, och utifrån prioriteringar i verksamheterna. Verksamhet som inte är kärnverksamhet kan betraktas som stödverksamhet.[3]

Det begrepp i kommunallagen som utredningen tolkat som beskrivning av kommunernas och landstingens kärnverksamhet, eller huvudsakliga uppgifter är kommunala angelägenheter.

[3] ESV 2014:49, Effektivisering av kärnverksamheter: Exempel från statliga myndigheter, Statskontoret 2015, Att göra eller köpa? Om outsourcing av statlig kärnverksamhet, Statskontoret 2016:19, Mer tid till kärnverksamheten.

2.5.4 Offentliga myndigheter

Regeringsformen skiljer mellan två typer av offentliga organ: *beslutande politiska församlingar*, till exempel riksdagen och regeringen och *myndigheter*. Samtliga statliga och kommunala organ, dvs. statliga myndigheter, kommuner och landsting med undantag för de beslutande församlingarna är myndigheter.

För att inte tynga texterna i onödan använder utredningen begreppet offentliga myndigheter som ett samlingsbegrepp för statliga myndigheter, kommuner och landsting. Begreppet offentliga myndigheter används dock inte konsekvent. I bland väljer utredningen att i stället skriva statliga myndigheter, kommuner och landsting.

I de fall utredningen har använt begreppet myndighet utan närmare precisering, såsom statlig myndighet, framgår det av kontexten vilken typ av myndighet som avses, t.ex. upphandlande myndighet.

3 Individ och myndighet i det digitala samhället

3.1 Den digitala världen är – global!

Regeringen konstaterade i skrivelsen om nationell strategi för informations- och cybersäkerhet[1] att digitaliseringen är ett globalt fenomen och påverkar i stort sett alla delar av vårt samhälle. Det medför stora möjligheter, men också risker. Hur vi hanterar riskerna som följer av digitaliseringen har stor betydelse för vår förmåga att upprätthålla och stärka både vårt välstånd och vår säkerhet. I skrivelsen presenterade regeringen strategiska prioriteringar inom sex olika områden med syfte att motverka hot i form av avsiktliga angrepp från främmande makt, terrorgrupper och kriminell verksamhet.

Brottsförebyggande rådet (BRÅ) har konstaterat att den it-relaterade brottsligheten har ökat markant under senare år.[2] Internationellt har även uppmärksammats hur digitala hjälpmedel använts för att påverka allmänna val.[3]

Digitaliseringen sätter gränser och formulerar villkor för såväl privata som offentliga aktörer. Ett begränsat antal företag dominerar de flesta marknader. Det gäller både hårdvara och mjukvara. E-tjänster riktade till allmänheten, såsom söktjänster och sociala medier, är i hög grad präglade av monopol. Tidskriften the Economist[4] har jämfört de moderna globala informationsföretagen med oljeindustrin. I bägge fallen handlar det om att utvinna råvara och förädla den. Råvaran i informationsindustrin är de data individerna själva delar med sig av.

[1] Skr. 2016/17:213.
[2] https://www.bra.se/brott-och-statistik/kriminalstatistik/anmalda-brott.html.
[3] Assessing Russian Activities and Intentions in Recent US Elections, The Central Intelligence Agency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA), CA 2017-01D 6 January 2017.
[4] The Economist Fuel of the future Data is giving rise to a new economy, 2017-05-06.

Förädlingen innebär att bearbeta dessa uppgifter och generera information om vanor, beteenden och värderingar. Dessa datamängder har ett mycket högt ekonomiskt värde för internetföretagen vilket är förklaringen till varför e-tjänster riktade till allmänheten ofta är gratis.

Offentliga myndigheter är i hög grad beroende av externa leverantörer av tjänster för it-drift. Inom vissa områden finns det få eller kanske endast en leverantör att tillgå.

Enligt Internetstiftelsen i Sverige har 82 procent av befolkningen över 12 år tillgång till en smartphone. I hälften av fallen handlar det om en Iphone.[5] Det betyder att en stor majoritet av befolkningen har möjlighet att använda e-tjänster mobilt. När individer utnyttjar privata eller offentliga e-tjänster använder de verktyg som tillhandahålls av ett begränsat antal multinationella företag.

Digitaliseringen av förvaltningen innebär att myndighetsutövningen kommer att äga rum i en miljö där många faktorer endast i begränsad utsträckning är påverkbara av den nationella lagstiftaren. Även om motåtgärder kan vara möjliga på EU-nivå[6] så gäller att de offentliga myndigheterna i hög grad får anpassa sig till vad marknadens globala aktörer erbjuder.

3.2 Elektronisk identifiering får ökad betydelse

Användningen av kontanter som betalningsmedel minskar drastiskt. År 2016 använde endast 15 procent av befolkningen kontanter vid sin senaste betalning. Motsvarande andel 2010 var 39 procent. Av befolkningen har 97 procent tillgång till bankkort, 85 procent har tillgång till internetbank och 61 procent har tillgång till betaltjänsten Swish.[7] År 2015 hade alla landsting utom ett, två tredjedelar av kommunerna och en tredjedel av de statliga myndigheternas e-tjänster som

[5] IIS, Svenskarna och internet 2016, s. 21, www.iis.se/docs/Svenskarna_och_inter-net_2016.pdf
[6] Se t.ex. Europaparlamentets och Rådets förordning om åtgärder rörande en öppen internetanslutning, (EU) 2015/2120 av den 25 november 2015. Syftet med förordningen är bl.a. att skydda slutanvändare genom att fastställa gemensamma regler för att säkerställa att icke-diskriminerande behandling av trafik vid tillhandahållandet av internetanslutningstjänster.
[7] Riksbanken, Betalningsvanor hos det svenska folket, 2016.

krävde s.k. tvåfaktorsautentisering, dvs. när lösenord kombineras med ett särskilt medel för identifiering, t.ex. en mobiltelefon.[8]

I Sverige är vi starkt beroende av e-tjänster för att utföra grundläggande uppgifter som att betala räkningar och lämna deklarationer. Antalet tillfällen då den enskilda individen måste identifiera sig elektroniskt ökar därmed. I åldern 16–45 år utnyttjar mer än 80 procent av internetanvändarna mobilt BankID.[9]

Användandet av elektroniska identitetshandlingar skapar beroenden och sårbarheter. En elektronisk identitetshandling har begränsad giltighet och kan, på ett mobilt medium, lätt förloras. Den kan raderas av misstag eller i samband med en uppdatering av operativsystemet. Utsätts en mobiltelefon för väta eller annan skada kan all information på den gå förlorad. Återskapandet av en mobil identitetshandling från BankID kräver att individen loggar in hos sin bank, vilket kräver en reservmöjlighet att legitimera sig elektroniskt. Individen tvingas därför att skapa strategier för att minska risken att stå utan möjlighet att identifiera sig elektroniskt. Det kan handla om att ha elektroniska identitetshandlingar från samma utfärdare på flera enheter, vilket kan betyda flera mobila enheter. Det kan också handla om att sprida risken genom att ha elektroniska identitetshandlingar från flera utfärdare. För utfärdare gäller att man behöver tillhandahålla en alternativ möjlighet till säker inloggning, i bankernas fall att man måste fortsätta att tillhandahålla tekniker som används av få och som egentligen varit tänkt att fasas ut.

För individen kan det vara önskvärt att ha tillgång till en elektronisk identitetshandling som kan användas i alla sammanhang. Vardagstryggheten i det digitala samhället kan paradoxalt nog vara den motsatta, nämligen vikten av att ha tillgång till flera alternativa sätt att identifiera sig elektroniskt. Vidare väcks frågan om det inte behövs någon form av basidentitetshandling som är elektronisk, som alla kan få och som är mindre utsatt för de risker som finns med information lagrade på datorer och telefoner och som skulle kunna användas för att återskapa en förlorad elektronisk identitetshandling som lagrats på ett sådant medium.

[8] RiR 2016:14, Riksrevisionen, Den offentliga förvaltningens digitalisering – En enklare, öppnare och effektivare förvaltning, s. 73.
[9] IIS, Svenskarna och internet 2016, s. 75. www.iis.se/docs/Svenskarna_och_inter-net_2016.pdf

3.3 Med användaren i fokus

Den gemensamma strategin för företag och offentliga myndigheter är att presentera sina e-tjänster för användaren i ett gränssnitt av typen ”mina sidor”. Efter elektronisk identifiering kan användaren förutom att använda olika tjänster, ta del av vilka uppgifter tjänsten har och följa utvecklingen i pågående ärenden. Upplägget är självklart eftersom informationen kan individualiseras, det skapar överblick och det är användaren som bestämmer vem som ska ta del av informationen. Med allt fler tjänster från allt fler aktörer kan antalet ”mina sidor” som individen behöver bevaka bli en nära nog övermäktig uppgift.

För individen blir det därför viktigt att någonstans kunna samla sin information eller åtminstone ha en samlad kanal för notiser och påminnelser.[10] Det kan handla om påminnelser via SMS och e-post. I Sverige finns i dag inget samlat stöd för offentliga myndigheter att skicka påminnelser via SMS och e-post utöver den som tillhandahålls inom ramen för Mina meddelanden. De individer som vill ha påminnelser får lämna kontaktinformationen till varje offentlig myndighet separat.

Fortfarande är det många som föredrar att spara viktiga papper i pärmar. Den enkät som utredningen lät genomföra för ett år sedan visade att det fortfarande är många (32 procent) som vill ha information från myndigheter via vanlig post. En stor grupp (28 procent) ville dessutom ha informationen både digitalt och på papper.[11] Den som går över till digital arkivering vill troligen kunna spara kopior i en lättillgänglig form, dvs. lokalt i datorn eller i någon typ av molntjänst. För företag och offentliga myndigheter räcker det därför inte att enbart presentera information i ett gränssnitt lämpligt för bildskärm, mobiltelefon etc. Informationen måste också kunna presenteras på ett beständigt sätt som kan vara tillgänglig för individen även utan teknisk utrustning.

Med de elektroniska sökhjälpmedel som i dag finns tillgängliga brukar man säga att all världens kunskap ligger bara ett knapptryck bort. Om de offentliga myndigheterna har en webbsida så kommer individen att hitta den förr eller senare. I många länder finns dock

[10] Mina sidor för privatpersoner. Slutrapport – Behovsanalys, rapport E-delegationen, 2010.
[11] SOU 2017:23, s. 331.

någon form av myndighetsportal. I Danmark finns bruger.dk och i Norge finns norge.no. I Sverige lades motsvarande portal ned i mars 2008 på grund av att den inte var tillräckligt känd och använd.[12] På förslag från EU-kommissionen väntas under hösten 2018 beslutas om ett förslag till en gemensam europeisk myndighetsportal. Portalen riktar sig till individer och företag och ska innehålla länkar till nationella myndigheter.[13] Detta kan medföra att frågan om en nationell portal i Sverige får en ny aktualitet.

Regeringens mål för digitaliseringen av den offentliga förvaltningen är en enklare vardag för medborgare, en öppnare förvaltning som stödjer innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten.[14] Den förra regeringen hade en liknande formulering[15] vilket påverkade E-delegationen att ta fram riktlinjer för verksamhetsutveckling utifrån ett medborgarperspektiv, så kallad behovsdriven verksamhetsutveckling. Detta bygger på att individens behov av myndighetskontakter analyseras utifrån livshändelser. En bärande tanke är att offentliga myndigheters e-tjänster ska utformas och presenteras så att individen snabbt ska kunna hitta de tjänster man behöver kopplade till den situation man befinner sig i. eSam[16] som bildades efter E-delegationen har fortsatt utveckla vägledningar, riktlinjer och stöd för behovsdriven utveckling.[17]

Att tillhandahålla e-tjänster utifrån ett livshändelsebaserat perspektiv innebär åtskilliga utmaningar för de offentliga myndigheterna. Det väcker bl.a. frågor om standardisering av information och gemensamma informationslösningar. Det ställer krav på förmågan att beakta förhållanden utanför det egna ansvarsområdet och på myndigheternas förmåga att samverka.

[12] Computer Sweden, Myndighetsportalen blev ett praktfiasko, 2007-05-24.
[13] KOM (2017) 256 Förslag till Europaparlamentets och rådets förordning om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012.
[14] Prop. 2017/18:1, utgiftsområde 2, s. 93.
[15] Med medborgaren i centrum, Regeringens strategi för en digitalt samverkande statsförvaltning, Näringsdepartementet, N2012.37.
[16] eSam är ett medlemsdrivet program för samverkan mellan 21 myndigheter och SKL för att underlätta och påskynda digitaliseringen av det offentliga Sverige.
[17] Vägledning för behovsdriven utveckling 1.0, eSam april 2016.

3.4 Utanförskap

Som framgår ovan är individer i Sverige starkt beroende av e-tjänster för att utföra grundläggande uppgifter som t.ex. att betala räkningar eller lämna deklarationer. För varje år ökar andelen individer som använder internet. Samtidigt är det viktigt att uppmärksamma att en stor del av allmänheten av olika skäl antingen inte vill eller har möjlighet att använda de tjänster som det digitala samhället och de offentliga myndigheterna erbjuder.

Regeringen bedömde i budgetpropositionen för 2018 att digitalt ska vara förstahandsval i den offentliga förvaltningens verksamhet och i den offentliga förvaltningens kontakter med individer och företag. Digitalt som förstahandsval innebär alltså att den offentliga förvaltningen, när det är lämpligt, ska välja digitala lösningar. Digitalt först innebär enligt utredningens bedömning inte att de offentliga myndigheterna utan stöd i författning kan kräva att individer och företag ska vara digitala i sina kontakter med de offentliga myndigheterna. Däremot ska myndigheter erbjuda e-tjänster när det är lämpligt. Att erbjuda e-tjänster innebär dock inte att myndigheterna får utesluta andra kommunikationsvägar. Kravet på likvärdig service till dem som inte använder e-tjänster ska beaktas. Såvida inte något annat är föreskrivet i lag ska de offentliga myndigheterna i enlighet med den nya förvaltningslagens teknikneutrala krav på myndigheternas service och tillgänglighet se till att kontakterna med individer blir smidiga och enkla. Myndigheten ska lämna individen sådan hjälp att hon eller han kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, individens behov av hjälp och myndighetens verksamhet. Den ska ges utan onödigt dröjsmål. En myndighet ska vara tillgänglig för kontakter och informera allmänheten om hur och när sådana kan tas, både med digitala medel och via fysiska kontaktpunkter.[18]

Det är viktigt att lägga fast vissa principiella åtaganden för att inte i onödan stänga ute individer från de offentliga myndigheternas e-tjänster. Ett principiellt exempel är att eftersom allt fler av de statliga myndigheternas, kommunernas och landstingens e-tjänster kräver inloggning med elektronisk identitetshandling innebär det i dagsläget att individer riskerar att stängas ute från e-tjänster eftersom de

[18] Förvaltningslagen (2017:900).

inte har eller kan få en elektronisk identitetshandling. Orsaken till detta skiftar. Möjligheten att bruka elektroniska identitetshandlingar påverkas av vilken modell på utrustning och operativsystem som individen har. En individ kan förlora möjligheten att använda elektronisk identitetshandling därför att utrustningens tillverkare inte längre uppdaterar operativsystemet.

Det står dock klart att den digitala förvaltningen innebär att individernas tillgång till elektroniska identitetshandlingar måste säkerställas. Det måste därmed vara ett statligt åtagande att alla som behöver en elektronisk identitetshandling kan få det.

Sammantaget innebär digitaliseringen att vissa centrala värden, som t.ex. principen om likabehandling, aktivt måste värnas samtidigt som statsmakterna måste vara bredda att ompröva hittills gällande lösningar och uppsatta gränser för vad som ska anses vara det offentliga åtagandet.

4 En omstart för den offentliga förvaltningens digitalisering

Utredningen bedömer:
att regeringen genom en serie olika initiativ har markerat en tydlig förändring av inriktningen av politiken för den digitala förvaltningen. Utredningen bedömer att det finns goda möjligheter att ta till vara de möjligheter digitaliseringen innebär samtidigt som utmaningarna kan hanteras.

I flera avseenden innebär initiativen en tydlig omprövning av tidigare ställningstaganden. Det som pågår kan därför beskrivas som en omstart av politiken för digitalisering inom den offentliga sektorn. De förslag som återges i detta betänkande, bygger vidare på dessa åtgärder och är avsedda att komplettera dem.

I budgetpropositionen för år 2015 aviserade den nuvarande regeringen sin satsning på att förstärka styrningen och samordningen av den övergripande it-användningen i statsförvaltningen. Digitaliseringen av den svenska offentliga förvaltningen skulle stimuleras. Satsningen skulle bidra till att nå målen för den digitala förvaltningen samt främja utvecklingen och användningen av gemensamma lösningar.[1]

4.1 En myndighet med samlat ansvar

I budgetpropositionen för år 2018 föreslog regeringen att en ny myndighet med uppgift att samordna och stödja den förvaltningsövergripande digitaliseringen ska inrättas. Förslaget överensstämmer med utredningens förslag i delbetänkandet digitalforvaltning.nu. Reger-

[1] Prop. 2014/15:1, utgiftsområde 2, s. 67.

ingen anför i uppdraget till organisationskommittén att den nya myndigheten medför förbättrade förutsättningar för en säker, effektiv och innovativ verksamhetsutveckling som utgår från användarnas behov. Den nya myndigheten som placeras i Sundsvall, ska inleda sin verksamhet den 1 september 2018 och övertar uppgifter från E-legitimationsnämnden, Ekonomistyrningsverket, Skatteverket, Post- och telestyrelsen, Riksarkivet och Tillväxtverket.

Myndigheten ska bistå regeringen med underlag för utvecklingen av politiken för digitalisering och it inom den offentliga sektorn och verka för en ökad digitalisering av den. Myndigheten ska bl.a. analysera och följa upp utvecklingen av den offentliga sektorns digitalisering utifrån riksdagens och regeringens övergripande mål på området. Vidare ska myndigheten ansvara för att samordna, utveckla, förvalta och tillhandahålla en nationell digital infrastruktur för den offentliga sektorn, samt främja dess användning. Myndigheten ska kunna meddela föreskrifter om nationell digital infrastruktur, såsom tillämpning av standarder, format och specifikationer för informationsutbyte, it-system och grunddata. Myndigheten ska samordna och stödja den offentliga sektorns arbete med användardriven verksamhetsutveckling. I detta ingår bl.a. stöd i samband med digitala investeringar.[2]

4.2 Samordnad organisation för statliga lokalkontor

Från och med den 1 januari 2019 ska Statens servicecenter ansvara för en samlad organisation för lokal statlig service. Uppdraget bygger på den rapport myndigheten lämnade till regeringen i mars 2017.[3]

Regeringen har gett en särskild utredare i uppdrag[4] att analysera och föreslå hur vissa statliga myndigheters lokala serviceverksamheter kan organiseras på ett mer sammanhållet sätt för att säkerställa tillgången till grundläggande statlig service i hela landet. Serviceorganisationen ska bestå av en nationell ledningsfunktion och lokala kontor.

I uppdraget ligger också att ta ställning till bl.a. vilket serviceutbud som bör finnas vid de lokala kontoren. Utredaren skulle pre-

[2] Dir 2017:117, Inrättande av en myndighet för digitalisering av den offentliga sektorn.
[3] Statens servicecenter, En sammanhållen organisation för statlig lokal service, delrapport i regeringsuppdraget om samordning och omlokalisering av myndighetsfunktioner, R:006.
[4] Dir. 2017:95.

sentera en plan för när de lokala kontoren ska kunna tillhandahålla service som avser Försäkringskassans, Pensionsmyndighetens och Skatteverkets verksamhet. Utredaren skulle även föreslå hur serviceorganisationen inledningsvis ska vara organiserad, dimensionerad och finansierad. Denna del av uppdraget redovisades i december 2017.[5]

Vidare ska ytredaren presentera en plan för när tillhandahållande av service som avser Arbetsförmedlingen, Migrationsverket och förarprovsverksamheten vid Trafikverket kan tillhandahållas vid de lokala kontoren samt vid behov föreslå ändringar i uppbyggnaden, dimensioneringen och finansieringen av den utökade serviceorganisationen. Vidare ska utredaren föreslå nödvändiga ändringar av Statens servicecenters instruktion och regleringsbrev. Uppdraget ska slutredovisas senast den 31 maj 2018.

Regeringen anser att lokal statlig service och digitala lösningar ska komplettera och understödja varandra. Om möjligt och lämpligt ska digitala lösningar vara förstahandsvalet i myndigheternas kontakter med individer och företag. Kontakterna mellan myndigheter och individer eller företag tas emellertid inte enbart via digitala lösningar, utan även genom personliga möten.

Statliga myndigheter kan – var och en för sig – inte upprätthålla en kostnadseffektiv kontorsnärvaro för att ge lokal service i hela landet. De servicekontor som Försäkringskassan, Pensionsmyndigheten och Skatteverket gemensamt driver har bidragit till att en lokal närvaro har kunnat upprätthållas på många platser. Vid de mindre kontoren är det dock svårt att ge service på ett kostnadseffektivt sätt. Regeringen bedömer att varken frivillig myndighetssamverkan eller en ny reglering om obligatorisk myndighetssamverkan är tillräckligt för att långsiktigt säkra en statlig service med förstärkt lokal närvaro i hela landet. Enligt regeringen krävs det i stället att en statlig myndighet ges i uppdrag att ansvara för en sammanhållen organisation för lokal statlig service.[6]

Enligt Statens servicecenters förslag ska lokalkontoren bygga på och komplettera, de samverkade myndigheternas e-tjänster. Kontoren ska tillhandahålla digital självservice av berörda myndigheters e-tjänster och e-guidning som syftar till hjälp till självhjälp. Kontoren ska även tillhandahålla muntlig direktservice av enklare karaktär

[5] SOU 2017:109, Servicekontor i ny regim.
[6] Dir. 2017:95 s. 7.

samt digitala och fysiska möten med handläggare från berörda myndigheter.[7]

4.3 Översyn av rättsliga förutsättningar för en digitalt samverkande förvaltning

En särskild utredare har regeringens uppdrag[8] att kartlägga och analysera i vilken utsträckning det finns lagstiftning som i onödan försvårar digital utveckling och samverkan inom den offentliga förvaltningen. Utredaren ska lämna förslag till de författningsändringar som sammantaget bedöms ha störst potential att stödja den fortsatta digitaliseringen av den offentliga förvaltningen. Skyddet av den personliga integriteten och andra sekretesskäl samt informationssäkerhet och rättssäkerhet ska vägas in i förslagen.

Utredaren ska vidare analysera den pågående digitala utvecklingen utifrån ett rättsligt perspektiv. Detta för att skapa en förståelse för vilka områden och företeelser som i förlängningen kommer att kräva lagstiftningsåtgärder för att de möjligheter som digitaliseringen och den tekniska utvecklingen skapar för den offentliga förvaltningen ska kunna tas till vara.

Utredaren ska också analysera och lämna förslag till hur den offentliga förvaltningen som helhet kan samverka om behovet av ny eller ändrad lagstiftning för att främja digitaliseringen av förvaltningen, och lämna förslag till andra åtgärder som syftar till att skapa bättre förutsättningar för hantering av rättsliga utmaningar inom detta område. Uppdraget ska redovisas senast den 31 mars 2018.

[7] Statens servicecenter, En sammanhållen organisation för statlig lokal service, delrapport i regeringsuppdraget om samordning och omlokalisering av myndighetsfunktioner, R:006, s. 43 f.
[8] Dir. 2016:98.

4.4 En expertgrupp för digitala investeringar

Regeringen har inrättat en särskild expertgrupp med uppdrag[9] att stödja myndigheter som avser att göra större strategiska verksamhetsinvesteringar i immateriella anläggningstillgångar med väsentliga inslag av it och digitalisering. Uppdraget omfattar ett urval investeringar hos ett tjugotal myndigheter.

Syftet med expertgruppen är att statliga myndigheter ska bli bättre på att genomföra verksamhetsutveckling och snabbare uppnå önskade resultat av politiska reformer eller förändrade uppgifter.

Expertgruppen ska verka för att statliga myndigheter dels utvecklar den interna styrningen och kontrollen av sin it-verksamhet, dels förbättrar hanteringen av risker vid större investeringar med väsentliga inslag av it och digitalisering. Expertgruppen ska bidra till kunskapsbyggande, erfarenhetsutbyte och lärande inom den offentliga sektorn så att statens samlade kompetens tas tillvara.

Expertgruppens uppdrag kommer att tas över av digitaliseringsmyndigheten.[10]

4.5 Skärpta krav och rutiner för svenska identitetshandlingar

För att minska det ökande antalet bedrägerier som begås med hjälp av förfalskade identitetshandlingar har regeringen tillsatt en särskild utredare[11] med uppdraget att föreslå hur antalet identitetshandlingar ska begränsas och särskilt överväga om det bör regleras i författning vilka handlingar som ska vara giltiga identitetshandlingar, och vilka krav som ska ställas på en giltig identitetshandling. Vidare ska utredaren föreslå hur antalet utfärdare av identitetshandlingar ska begränsas samt lämna förslag på utfärdare.

Utredaren ska analysera behovet av en enhetlig reglering av giltiga identitetshandlingar när det gäller processen för ansökan, bakgrundskontroll av den sökande, tillverkning av den fysiska handlingen och utlämnande av handlingen. Utredaren ska kartlägga hur verifieringen

[9] Dir. 2017:62.
[10] Dir. 2017:117.
[11] Dir. 2017:90.

av identitetshandlingars äkthet och giltighet görs i dag och lämna förslag på förbättringar.

Slutligen ska utredaren analysera och ta ställning till om fysiska identitetshandlingar bör innehålla en e-legitimation på högsta tillitsnivå. Uppdraget ska redovisas senast den 29 mars 2019.

4.6 Nationell strategi för informations- och cybersäkerhet

Regeringen har presenterat en nationell strategi för hur informations- och cybersäkerheten i Sverige ska utvecklas och stärkas.[12] I strategin sätter regeringen upp målsättningar inom sex prioriterade områden:

- Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet.
- Öka säkerheten i nätverk, produkter och system.
- Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter.
- Öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet.
- Öka kunskapen och främja kompetensutvecklingen.
- Stärka det internationella samarbetet.

Målsättningarna ska bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet, samt höja medvetenheten och kunskapen i hela samhället.

I anslutning till strategin beslutade regeringen om ett antal myndighetsuppdrag.

Regeringen har uppdragit åt Myndigheten för samhällsskydd och beredskap (MSB) att, i samverkan med Sveriges kommuner och landsting (SKL), E-hälsomyndigheten och Socialstyrelsen, kartlägga och

[12] Skr. 2016/17:213, Nationell strategi för samhällets informations- och cybersäkerhet.

analysera informationssäkerhetsarbetet inom landstingens hälso- och sjukvårdsverksamhet. Uppdraget ska redovisas senast 1 oktober 2018.[13]

Regeringen har vidare uppdragit åt MSB att verka för att de privat-offentliga samarbetsformerna stärks. I uppdraget ingår att bedöma vilka branscher och sektorer som bör prioriteras. Uppdraget ska redovisas senast den 1 mars 2018 och av redovisningen ska det framgå vilka åtgärder MSB har vidtagit, och vilken effekt dessa har haft samt, vilka ytterligare åtgärder MSB planerar att vidta.[14]

Länsstyrelserna och vissa andra myndigheter har, enligt förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, ett särskilt ansvar för att planera och vidta förberedelser för att skapa förmåga att hantera en kris, förebygga sårbarheter och motstå hot och risker.[15] Dessa myndigheter ska senast den 1 mars 2018 till regeringen och MSB redovisa en analys och bedömning av informationssäkerheten i de delar av den egna verksamheten som är nödvändiga för att myndigheten ska kunna utföra sitt arbete. I sammanhanget ska krisberedskapsperspektivet samt planeringen för det civila försvaret beaktas.[16]

Av redovisningen av uppdraget ska det framgå hur myndigheten bedömer informationssäkerheten, vilka hot, sårbarheter och risker som har identifierats samt vilka åtgärder som har vidtagits, respektive kommer att vidtas, i syfte att reducera dessa.[17]

MSB ska, i samverkan med Försvarsmakten och Säkerhetspolisen, senast den 1 oktober 2018 redovisa en sammanvägd rapport utifrån dessa rapporter.[18]

4.7 En ny säkerhetsskyddslag

Regeringen lämnat ett förslag till lagrådet om en ny säkerhetsskyddslag. Den nya lagen ska gälla för alla som bedriver verksamhet som gäller Sveriges säkerhet, vare sig det är i offentlig eller privat regi. Den nya lagen förtydligar kraven på skydd av verksamheter som

[13] Ju2017/05789/SSK.
[14] Ju2017/05789/SSK.
[15] Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.
[16] Ju2017/05644/SSK.
[17] Ju2017/05787/SSK.
[18] Ju2017/05788/SSK.

har betydelse för Sveriges säkerhet och ökar skyddet mot bland annat spionerі och sabotage. Den omfattar bland annat krav på skydd av it-system som har betydelse för Sveriges säkerhet och den innebär tydligare krav på att skydda utländska intressen som Sverige har åtagit sig.

Kraven på verksamheterna som berörs av lagen förtydligas. Verksamhetsutövarna ska göra en säkerhetsskyddsanalys och utifrån den vidta de åtgärder som behövs – det kan gälla informationssäkerhet, skydd av lokaler och anläggningar samt kontroll av personal. Såväl offentliga som privata aktörer kan söka stöd och råd från tillsynsmyndigheterna Säkerhetspolisen och Försvarsmakten.

Lagen och följdändringarna föreslås träda i kraft den 1 januari 2019.[19]

4.8 Utkontraktering och samordning av it-drift

Regeringen har remitterat en promemoria[20] med förslag till begränsningar i de statliga myndigheternas möjligheter att utkontraktera och överlåta säkerhetskänslig verksamhet. Enligt förslaget ska en statlig myndighet, som avser att genomföra en sådan utkontraktering av den egna verksamheten som innebär krav på säkerhetsskyddsavtal enligt säkerhetsskyddslagen, utföra en särskild säkerhetsanalys av uppdraget och samråda med den tillsynsmyndighet (Säkerhetspolisen eller Försvarsmakten) som är berörd innan ett förfarande för utkontraktering inleds.

Vidare har regeringen tillsatt en särskild utredare[21] för att kartlägga behovet av att förebygga att säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet utsätts för risker i samband med utkontraktering, upplåtelse och överlåtelse av sådan verksamhet, och föreslå olika förebyggande åtgärder, t.ex. tillståndsprövning.

Utredaren ska vidare föreslå ett system med sanktioner i säkerhetsskyddslagstiftningen samt hur en ändamålsenlig tillsyn enligt säkerhetsskyddslagstiftningen ska vara utformad.

---

[19] Lagrådsremiss, Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag, november 2017.
[20] Skärpt kontroll av statliga myndigheters utkontraktering och överlåtelse av säkerhetskänslig verksamhet, Ju 2017/07544/L4.
[21] Dir. 2017:32, Utkontraktering av säkerhetskänslig verksamhet, sanktioner och tillsyn – tre frågor om säkerhetsskydd.

Regeringen har gett Försäkringskassan i uppdrag[22] att åren 2017–2020 erbjuda vissa myndigheter en samordnad och säker it-drift. Det övergripande syftet är att pröva och utvärdera former för samordnad och säker it-drift för lämpliga myndigheter. En delredovisning av hur uppdraget ska genomföras ska lämnas till regeringen senast den 30 november 2017. Delredovisningen ska innefatta en verksamhetsplan för 2018–2020. Dessutom ska de myndigheter som beslutat att inleda ett samarbete med Försäkringskassan redovisas. Ytterligare delredovisningar av hur arbetet fortlöper ska lämnas efter samråd med Finansdepartementet.

Försäkringskassan ska lämna en slutredovisning till regeringen senast den 18 december 2020. Slutredovisningen ska innehålla en beskrivning av vilka åtgärder som genomförts inom ramen för uppdraget, uppnådda effekter samt risker och eventuella hinder som identifierats.

4.9 Offentlig samverkan

Den 29 oktober 2015 beslöt regeringen att skriva under en avsiktsförklaring mellan staten och SKL för en digital förnyelse av det offentliga Sverige.[23] Avsiktsförklaringen anknyter till regeringens inriktning om digitalt först. Den 19 januari 2017 godkände regeringen en med SKL gemensam handlingsplan för utveckling av e-hälsoområdet.[24] Regeringen har gett ett antal myndigheter tidsbegränsade utvecklingsuppdrag inom områdena samhällsbyggnad, jordbruksproduktion, miljöskydd och företagande. Livsmedelsverket har fått ett särskilt uppdrag att verka för digitalisering inom ramen för regeringens livsmedelsstrategi. Skolverket har fått i uppdrag att utveckla en digital lösning för de nationella proven. Sammantaget pågår det åtskilliga statliga utvecklingsprojekt som berör kommunernas uppgifter i olika grad.

SKL har vidtagit åtskilliga åtgärder för att stödja kommunernas digitalisering. Företaget Inera AB som tidigare levererat e-tjänster främst inom landstingens ansvarsområde, Vårdguiden t.ex., har fått ett vidgat ägande och kommer att erbjuda tjänster också för kommunerna.

[22] Uppdrag att erbjuda samordnad och säker statlig it-drift Fi2017/03257/DF.
[23] Dnr N2015/07455/EF.
[24] Dnr S2017/00379/FS.

Kommunutredningen har i ett delbetänkande föreslagit att en kommun eller ett landsting får träffa avtal om att dess uppgifter helt eller delvis ska utföras av en annan kommun eller ett annat landsting. Genom ett sådant avtal får en kommun eller ett landsting utföra uppgifter åt en annan kommun eller landsting utan hinder av lokaliseringsprincipen. Kommunutredningen bedömer att det finns ett behov av att kunna samverka framför allt i fråga om specialisttjänster som innefattar myndighetsutövning, it och digitalisering samt administration.[25]

4.10 Omstart

Som beskrivits i utredningens delbetänkande byggde politiken för den digitala förvaltningen under lång tid på centraliserade lösningar.[26] Statskontoret hade ett övergripande ansvar och förfogade en period över anslaget för it-investeringar. Med de förvaltningspolitiska reformerna under 1980- och 1990-talen begränsades denna roll successivt. År 2008 lades den myndighet, Verva, som övertagit vad som återstod av den centrala samordningen ned. Förslaget kom från Stabsstödsutredningen som menade att e-förvaltningen borde utvecklas i en federativ inriktning där de stora och resursrika myndigheterna, som Skatteverket och Försäkringskassan i nära samverkan med Regeringskansliet, bildade stommen. På så sätt skulle Sverige ”välja en annan och mer flexibel väg på e-förvaltningens område än vad till exempel en del av våra grannländer gjort då man anammat mer centralstyrda modeller”.[27]

Inrättandet av digitaliseringsmyndigheten innebär en påtaglig förändring av vad som gällt under det senaste decenniet. Den nya myndigheten kommer att ha ett större ansvar och en starkare roll än vad Verva hade, men å andra sidan inte den nästan enväldiga position som Statskontoret en gång hade. E-delegationen och eSam har på många sätt framgångsrikt fyllt ut tomrummet. De nya utmaningarna som digitaliseringen medför innebär förändringar i strukturer och strategier.

[25] SOU 2017:77 En generell rätt till kommunal avtalssamverkan, delbetänkande av Kommunutredningen.
[26] SOU 2017:23 digitalforvaltning.nu.
[27] SOU 2008:22 Ett stabstöd i tiden, s. 97.

En sådan utmaning är att många e-tjänster förutsätter stödfunktioner av infrastrukturkaraktär som inte kan hanteras inom ramen för traditionell samverkan mellan statliga myndigheter. En annan utmaning är att det legala ramverket och den digitala verkligheten måste anpassas till varandra. Dessutom måste sådant arbete förhålla sig till en samtidigt pågående digitalt driven utveckling inom EU.

Den ökade medvetenheten om digitaliseringens risker stryker under behovet av samordning och centrala funktioner med specifik kompetens och koordineringsuppgifter. Detsamma gäller tillvaratagandet av möjligheterna att hushålla väl med allmänna medel i samband med it-drift, upphandling och verksamhetsutveckling.

Det digitala samhället kan emellertid inte avstå från analoga kanaler. Dels kommer en stor grupp människor även i fortsättningen stå utanför på grund av funktionshinder, ålder, ekonomiska barriärer eller bristande intresse, dels finns det behov av analoga reservlösningar när de digitala temporärt inte är tillgängliga. Den nya organisationen för statliga lokalkontor är där en viktig komponent.

För att kommunerna ska klara av den digitala omställningen är det viktigt att det finns gemensamma lösningar och möjlighet till samverkan mellan kommunerna som inte förutsätter inrättandet av särskilda strukturer. Förslaget till samverkansavtal är därför en annan viktig förutsättning för att bygga ut den digitala förvaltningen.

En annan viktig del är systemet för elektronisk identifiering. Överväganden om detta redovisas senare i detta betänkande. Här ska dock konstateras att de fysiska identitetshandlingarnas kvalitet och processen för att fastställa individers identitet är av avgörande betydelse för den elektroniska identiteten. Grundidentifiering i samband med utfärdande av fysiska id-handlingar har avgörande betydelse för elektroniska identitetshandlingars tillförlitlighet.

Sammanfattningsvis innebär regeringens initiativ i många fall en betydande omprövning av tidigare ställningstaganden som präglat politiken för den digitala förvaltningen under lång tid.

Flera viktiga komponenter tillförs eller förändras. När de är på plats och börjar verka är det befogat att tala om en omstart av politiken för digital förvaltning.

5 Effektiv styrning av en samverkande förvaltning

5.1 Om samverkan – möjligheter och befogenheter

Utredningen bedömer:
att de offentliga myndigheterna i sitt digitaliseringsarbete måste ha stöd i rättsordningen för sina åtgärder. Behoven av samverkan mellan olika aktörer inom ramen för initiativ, utveckling och förvaltning av nationella digitala tjänster skiljer sig åt mellan olika skeden av livscykeln.

I de fall det förväntade digitaliseringsarbetet i samverkan med andra och resultatet av detta inte ryms inom myndigheternas befintliga uppdrag och befogenheter, måste det uppmärksammas så att regeringen och i förekommande fall riksdagen kan vidta åtgärder för att ändra myndigheternas uppdrag och befogenheter.

För att främja utvecklingen av den offentliga sektorns digitalisering behöver institutionaliserade forum för frivillig samverkan mellan de olika aktörerna inrättas. Det är en lämplig uppgift för den kommande digitaliseringsmyndigheten att tillhandahålla sådana. Digitaliseringsmyndigheten bör tilldelas särskilda anslagsmedel för sådan samverkan.

Utredningen föreslår:
att regeringen – i ljuset av de verksamhetsmässiga begränsningar för samverkan som gällande bestämmelser medför – i förordningen om statliga myndigheters elektroniska informationsutbyte ska reglera att statliga myndigheter i frågor om digitalisering av den offentliga förvaltningen, vid behov, får samverka även utanför sina vanliga verksamhetsområden.

Förslaget genomförs genom 2 a § i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

att digitaliseringsmyndigheten tilldelas särskilda anslagsmedel för frivillig samverkan mellan olika aktörer för att främja den offentliga sektorns digitalisering.

> De nationella digitala tjänsterna ska kunna användas inom hela den offentliga sektorn och syftar till att underlätta elektronisk hantering av ärenden och kontakter med enskilda. Exempel på sådana befintliga tjänster är Mina meddelanden och Svensk e-legitimation. Tjänsterna ska utvecklas utifrån medborgarnas behov, vilket förutsätter en bred och omfattande samverkan mellan statliga myndigheter, mellan kommunala myndigheter, mellan stat och kommun samt mellan offentlig och privat sektor.[1]

Utredningen ska lämna förslag till effektiv styrning av förvaltningsgemensamma digitala funktioner i en *samverkande* förvaltning. Uppdraget är ett av flera regeringsinitiativ som signalerar en övergång från en digital förvaltningsutveckling huvudsakligen driven genom myndighetssamverkan till en där regeringen tar en mer aktiv och drivande roll. Denna förändring ändrar dock inte den grundläggande betydelse som samverkan har i sammanhanget. Behovet av samverkan mellan statliga myndigheter minskar inte. Samverkan mellan stat, kommun och landsting måste förstärkas i väsentlig grad. Samverkan mellan offentlig och privat verksamhet har varit avgörande för att inleda uppbyggnaden av den nationella digitala infrastrukturen och kommer att fortsätta vara lika viktig.

En viktig fråga i detta sammanhang är vad som avses med begreppet samverkan. Begreppet återkommer i lagar och andra författningar, i särskilda uppdrag och myndighetsinstruktioner, i strategier och avsiktsförklaringar, regleringsbrev m.m. och kan vara generellt eller specifikt och samverkan kan vara frivillig eller obligatorisk. Även om begreppet således ofta används är det svårt att hitta en beskrivning av vad begreppet innebär – i praktiken – och vilka *förväntningar* givet det formella regelverket som kan ställas på dem som förväntas samverka. Till skillnad från denna något diffusa bild vad gäller statsförvaltningen är kommunallagens bestämmelser om hur samverkan mel-

[1] Dir. 2016:39, Effektiv styrning av nationella digitala tjänster i en samverkande förvaltning.

lan kommuner och mellan landsting kan formaliseras och genomföras formellt och i praktiken väsentligt tydligare.[2]

5.2 Samverkan i ett livscykelperspektiv

Av direktiven framgår att utredningen, bl.a. med utgångspunkt i Mina meddelanden och Svensk e-legitimation, ska analysera skillnaderna mellan hur ansvaret för olika befintliga nationella digitala tjänster är fördelat i dag och alternativ till detta.

Analysen ska utgå från ett livscykelperspektiv för de nationella digitala tjänsterna. Det handlar bland annat om att lämna förslag om hur samverkan och kravställning, eller vidareutveckling av nationella digitala tjänster, ska analyseras utifrån ett livscykelperspektiv, där hela kedjan från utveckling till avveckling ska beaktas.

Begreppet livscykel kommer i det följande att användas såsom det definieras i E-delegationens vägledning för nyttorealisering.[3] Perspektivet är en produkts, tjänst eller systems hela livslängd från idé/koncept till utveckling, produktion, drift, underhåll och avveckling.[4] Utredningen väljer att kalla den del av livscykeln som handlar om produktion, drift och underhåll för förvaltningsstadium. Utredningen behandlar inte frågan om avveckling i samverkan.

5.2.1 Samverkan om idé och utveckling

En process som leder till införande eller förändring av ett digitalt medel inom offentlig verksamhet kan inledas huvudsakligen på fyra sätt.

- Det kan vara en direkt konsekvens av en reform. När premiepensionen infördes krävde det ett helt nytt stöd för att presentera fondvalsalternativ för pensionsspararna. En reform kan också initieras inom Europeiska Unionen. En följd av eIDAS-förordningen är till exempel införandet av en nod för att förmedla gränsöverskridande digital trafik mellan myndigheter och ID-certifikatutfärdare.

[2] Kommunallagen (2017:725).
[3] E-delegationen, version 2.0, Vägledning i nyttorealisering.
[4] A.a.

- Det kan uppkomma som en följd av regeringens övergripande ambitioner vad gäller resurshushållning och effektivisering. Ett exempel på detta är inrättandet av Statens servicecenter som stödjer statliga myndigheter vad gäller personal- och ekonomiadministration.
- Myndighetens eget arbete med att utveckla sin verksamhet leder givetvis också till framtagande och utveckling av digitala medel. Styrelsen för ackreditering och kontroll, SWEDAC, införde 2004 en fullständigt digital dokumenthantering och digitaliserade helt sitt tillsynsarbete.
- Behovet kan också identifieras genom samverkan mellan myndigheter och mellan myndigheter och kommuner. Myndigheterna kan identifiera samma behov eller finna att man utifrån olika behov har användning för en gemensam digital lösning. Det kan också vara så att myndigheter har olika roller i en och samma handläggningsprocess och ser fördelar med att digitalisera processen. Mina meddelanden och projektet E-identitet för offentlig sektor[5] är exempel på lösningar av det förstnämnda fallet och SSBTEK[6] ett exempel på det sistnämnda.

Processer som leder till utveckling av digitala medel kan inledas på olika sätt. Även om genomförandet bygger på regeringsuppdrag, fordrar lagstiftning och resurstilldelning så kan den viktiga impulsen till förändringen många gånger härledas till samverkan på myndighetsnivå eller samverkan mellan stat och kommun. Även om samverkan inte alltid leder till etablerandet av en infrastrukturtjänst så är samverkan en viktig källa till utvecklandet av sådana.

E-delegationen var under ett antal år huvudkanalen för samarbete mellan myndigheterna. När delegationens regeringsuppdrag upphörde 2014 ersattes den av ett frivilligt samarbete i form av eSamverkansprogrammet (eSam). Medan samarbetet i E-delegationen hade en formell grund, saknar eSam en sådan.

I delbetänkandet underströk utredningen att det finns anledning att inspireras av, ta tillvara och i någon form behålla och utveckla de

[5] Projekt gemensamt för Försäkringskassan och Inera AB. Avses kunna bli en tjänstelegitimation för både stat, kommun och landsting.
[6] Digital tjänst för ekonomiskt bistånd.

arbetsmodeller som skapades inom ramen för E-delegationens uppdrag och bevarats inom ramen för eSam.

Utredningens förslag till instruktion för digitaliseringsmyndigheten innefattade uppgifter att stödja samverkan mellan statliga myndigheter, mellan statliga myndigheter och kommuner och mellan offentliga myndigheter och näringslivet i det digitala utvecklingsarbetet. En annan uppgift var att myndigheten i samverkan med relevanta offentliga myndigheter och aktörer skulle verka för informations- och erfarenhetsutbyte om den nationella digitala infrastrukturen och nationella digitala tjänster för att förenkla för enskilda och företag och säkerställa en effektiv och ändamålsenlig offentlig förvaltning.

Enligt förslaget skulle myndigheten även samverka med Datainspektionen, Myndigheten för samhällsskydd och beredskap samt Post- och telestyrelsen i frågor om digitalisering av förvaltningen, personlig integritet och informationssäkerhet.

Av uppdraget till organisationskommittén[7] för digitaliseringsmyndigheten framgår att en utgångspunkt för myndighetens arbete ska vara att i lämpliga delar ta tillvara kunskap och erfarenheter som eSam upparbetat, bl.a. avseende metoder och processer för samverkan. Myndigheten ska verka för en öppnare förvaltning som stödjer innovation och delaktighet, genom att bl.a. statliga myndigheter, kommuner och landsting tillgängliggör öppna data, med beaktande av de skyddsbehov som beskrivits ovan. Myndigheten ska vidare främja öppen och datadriven innovation i den offentliga sektorn.

Myndigheten ska samordna och stödja den offentliga sektorns arbete med användardriven verksamhetsutveckling. I detta ingår bl.a. stöd i samband med digitala investeringar. Inom myndigheten ska det finnas ett rådgivande organ som ska bistå myndighetschefen i strategiska frågor rörande myndighetens verksamhet och vid framtagande av föreskrifter. I rådet ska representanter för statliga myndigheter, kommuner och landsting, SKL, samt Sveriges Standardiseringsförbund ingå. Utredaren ska även lämna förslag till kompetensprofil för ledamöterna i det nämnda organet.

Utredningen anser att det är viktigt att ta till vara det engagemang, den innovationskraft och den verksamhetsnära kunskap som finns hos myndigheterna, däribland såväl de stora it-tunga myndig-

[7] Dir. 2017:117, Inrättande av en myndighet för digitalisering av den offentliga sektorn.

heterna som små och medelstora myndigheter, kommuner och landsting.

Det är viktigt att frivillig samverkan och erfarenhetsutbyte mellan statliga myndigheter, kommuner och landsting är formellt möjlig och stimuleras. Utredningen menar därför att för att främja utvecklingen av den offentliga sektorns digitalisering behöver institutionaliserade forum för frivillig samverkan mellan de olika aktörerna inrättas. Utredningen anser att det är en lämplig uppgift för den kommande digitaliseringsmyndigheten att tillhandahålla sådana. Utredningen anser även att digitaliseringsmyndigheten ska tilldelas särskilda anslagsmedel för sådan samverkan.

Utredningen anser vidare att givet begränsningarna för samverkan enligt gällande bestämmelser finns det ett stort behov av att kunna meddela föreskrifter som avviker från den allmänna regleringen i förvaltningslagen. Utredningen föreslår därför att regeringen – i ljuset av de verksamhetsmässiga begränsningar för samverkan som gällande bestämmelser medför – i förordningen om statliga myndigheters elektroniska informationsutbyte ska reglera att statliga myndigheter får samverka utanför sina verksamhetsområden i frågor om digitalisering av den offentliga förvaltningen.

5.2.2 Samverkan i ett förvaltningsstadium

Effektiv styrning och samverkan i ett förvaltningsstadium innebär, enligt utredningen, att riksdagen och regeringen har fattat beslut om en förvaltningsgemensam digital funktion[8] och de samverkande aktörernas olika roller, ansvar och uppgifter är formaliserade och utformade så att samverkan är möjlig och leder till de önskade effekterna. I sitt remissvar över Förvaltningslagsutredningens betänkande lyfte E-delegationen frågan om förutsättningarna för samverkan mellan myndigheter för att främja e-förvaltningen. Se nedan.

Enligt utredningen behöver regeringen särskilt analysera och bedöma om förväntningarna på och eller behovet av samverkan ryms inom ramen för de möjligheter och begränsningar som bl.a. förvaltningslagen, myndighetsförordningen och förordningen om de stat-

[8] Se resonemang i kapitel 6 om begreppen nationella digitala tjänster och förvaltningsgemensamma digitala funktioner.

liga myndigheternas elektroniska informationsutbyte medger. Här kan det eventuellt finnas anledning för regeringen att ompröva förväntningarna på och/eller behoven av samverkan mellan myndigheter, eller bedöma om det finns anledning att överväga specialreglering. Se nedan om avvikande bestämmelser i andra lagar eller i förordningar.

5.3 Samverkan enligt förvaltningslagen

I september 2017 fattade riksdagen beslut om en ny förvaltningslag som träder i kraft den 1 juli 2018. I sitt förslag till den nya förvaltningslagen anförde regeringen att det är angeläget att ge en klar signal om att all offentlig verksamhet – oavsett dess karaktär – ytterst måste grundas på skrivna regler i rättsordningen. Regeringen refererade till Förvaltningslagsutredningens genomgång av praxis som gav

> en klar indikation på att myndigheterna inte alltid i tillräcklig utsträckning tar reda på om att de har stöd i rättsordningen för sina åtgärder. Utvecklingen från en mer klassisk förvaltning mot en förvaltning med ökade inslag av informationsuppgifter och mera kundrelaterade aktiviteter, t.ex. i form av olika digitala självbetjäningstjänster, har också inneburit ökade risker i detta avseende. Det är därför angeläget att ge en klar signal om att all offentlig verksamhet, oavsett dess karaktär, ytterst måste grundas på skrivna regler i rättsordningen (prop. 1973:90 s. 397). Skiljelinjen mellan privaträttsliga subjekts principiella rätt till ett fritt agerande och myndigheternas skyldighet att fullgöra bestämda uppgifter i det allmännas tjänst bör alltså tydligt markeras.[9]

Förvaltningslagen gäller för handläggning av ärenden hos förvaltningsmyndigheterna och handläggning av förvaltningsärenden hos domstolarna. Enligt den ännu gällande förvaltningslagens bestämmelser gäller, om samverkan mellan myndigheter, att varje myndighet ska lämna andra myndigheter hjälp inom ramen för den egna verksamheten.[10]

I den nya förvaltningslagen[11] finns motsvarande bestämmelse under rubriken Grunderna för god förvaltning.[12] Bestämmelsen lyder på följande sätt:

[9] Prop. 2017/18:180, s. 58.
[10] 6 § förvaltningslagen (1998:223).
[11] Förvaltningslagen (2017:900).
[12] 8 § Grunderna för god förvaltning, Samverkan, förvaltningslagen (2017:900).

> En myndighet ska inom sitt verksamhetsområde samverka med andra myndigheter.
>
> En myndighet ska i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter.[13]

Förvaltningslagsutredningen[14] anförde – om samverkan – att alla myndigheter, både statliga och kommunala, verkar på det ena eller andra sättet i ”det allmännas” och därmed också i ”allmänhetens” tjänst. Det är alltså väsentligt att deras samlade ansträngningar riktas mot det gemensamma målet att erbjuda medborgarna goda och rättvisa levnadsvillkor. Förvaltningslagsutredningen menade att det förutsätter att en myndighet inte ser sin uppgift som strikt isolerad från vad en annan myndighet sysslar med utan att båda gör vad de kan för att underlätta för varandra. Denna tanke, som kom till uttryck i den klassiska formuleringen i 47 § i 1809 års regeringsform att myndigheterna ska ”räcka varandra handen”, avspeglas i modern tappning i 6 § i den nu gällande förvaltningslagen.

Enligt Förvaltningslagsutredningen hade dock den nuvarande förvaltningslagens samverkansbestämmelse fått en utformning, som delvis döljer bestämmelsens dubbla syfte.

Att ”varje myndighet ska lämna andra myndigheter hjälp inom ramen för den egna verksamheten” leder, enligt Förvaltningslagsutredningen, tankarna till att det främst är fråga om ett internt inom administrationen lämnat bistånd, avsett att t.ex. minska konsekvenserna av en ojämn medelstilldelning eller att tillföra en myndighet någon särskild sakkunskap som den saknar men en annan myndighet besitter. Någon antydan ges inte om att syftet också är att enskilda genom att myndigheterna samarbetar ska besparas ett tidsödande arbete med att vid flera tillfällen själv konsultera flera myndigheter i ett och samma ärende.

Förvaltningslagsutredningen föreslog därför att det budskap som 6 § i den ännu gällande förvaltningslagen får anses innefatta, skulle överföras till en bestämmelse i den nya lagen.

För det första ville Förvaltningslagsutredningen tona ned intrycket av att det är fråga om en mera tillfällig ”hjälp”, som en myndighet kan erbjuda en annan i ett trängt läge, genom att tala om att myndigheterna mera generellt ska ”samverka” med varandra.

---

[13] 8 § förvaltningslagen (2017:900).
[14] SOU 2010:29, En ny förvaltningslag, betänkande av Förvaltningslagsutredningen.

För det andra ville Förvaltningslagsutredningen ge en klar indikation på att denna samverkan är avsedd att underlätta för individen i kontakterna med myndigheterna. Detta genom att i ett nytt stycke, som saknar motsvarighet i 6 § i den ännu gällande förvaltningslagen, föreskriva att en myndighet ”i den utsträckning som kan anses rimlig bistå den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter”. En liknande bestämmelse återfinns nu bland de ”allmänna krav på handläggningen av ärenden” som uppställs i 7 § den ännu gällande förvaltningslagen, men Förvaltningslagsutredningen ville alltså se en sådan regel som ett inslag i den service som myndigheterna generellt, inte bara då det är fråga om formlig ärendehandläggning, ska erbjuda.

5.3.1 Myndigheterna samverkar inom sina respektive verksamhetsområden

Det är, enligt Förvaltningslagsutredningen, väsentligt att understryka, att samverkan mellan myndigheterna ska försiggå inom deras respektive verksamhetsområden och att det däri ligger två begränsningar.

För det första måste en myndighet naturligtvis prioritera sina egna huvuduppgifter och är inte – såsom Förvaltningslagsutredningen uttryckte det – tvingad att släppa vad den har för händer så snart en annan myndighet begär assistans. Det är alltid myndigheten själv som avgör, om den kan avsätta resurser för att bistå den andra myndigheten i dess verksamhet.

För det andra ger bestämmelsen inte stöd för några samverkansprojekt som faller utanför respektive myndighets verksamhetsområde. Det är, enligt Förvaltningslagsutredningen, viktigt att poängtera, att myndigheternas verksamhet enligt legalitetsprincipen styrs av de regler om arbetsuppgifterna som lagstiftaren eller annan normgivare beslutat. Några nyskapelser i form av särskilda samarbetsorgan, som oberoende av fastlagda normer tillåter sig att fatta beslut som svårligen kan härledas till den ena eller andra av de samverkande myndigheterna, får inte förekomma.[15]

[15] SOU 2010:29, En ny förvaltningslag, betänkande av Förvaltningslagsutredningen.

5.3.2 E-delegationens remissvar och regeringens argumentation för förslaget till bestämmelse om samverkan

E-delegationen tillstyrkte i sitt remissvar[16] utredningens förslag i stort men hade synpunkter i vissa delar som rörde förutsättningarna att främja e-förvaltningen, bl.a. samverkan mellan myndigheter.

E-delegationen menade att förslaget till bestämmelse om samverkan inte hade beaktat e-förvaltningens behov av samverkan mellan myndigheter. Enligt E-delegationen måste en ny förvaltningslag på ett mycket tydligare och kraftfullare sätt, med utgångspunkt i behov som är gemensamma för förvaltningen, betona myndigheternas skyldighet att samverka med varandra. Även krav på samverkan med näringslivet borde, enligt delegationens mening, komma till uttryck i en ny förvaltningslag. Utformningen av bestämmelsen främjade, enligt E-delegationen, inte tillräckligt att myndigheter samverkar med varandra för att tillgodose samhällsgemensamma behov.

Det är därmed i praktiken myndigheten som utifrån sina egna intressen får bedöma om samverkan kan anses rymmas inom dess verksamhetsområde. Utformningen befäster ett s.k. stuprörstänkande. Begränsningen till verksamhetsområdet borde, enligt delegationens mening, tas bort. Det borde vara de samverkande parternas uppgift att i samband med genomförande av gemensamma förstudier m.m. överväga vilka ekonomiska, legala och andra förutsättningar som måste komma på plats inför olika steg i en samverkansprocess.

Vidare ansåg delegationen att krav på samverkan även med andra än myndigheter borde ingå i en ny förvaltningslag eftersom e-förvaltningen inte kan utvecklas utan att företagens och marknadens förutsättningar respekteras och tas tillvara. E-delegationen ville i sammanhanget särskilt fästa uppmärksamhet på regeringens nationella handlingsplan för den svenska e-förvaltningen från maj 2008 (regeringens e-handlingsplan) och regeringens förvaltningspolitiska proposition[17] från 2010. I båda dessa dokument finns långtgående krav på att myndigheter ska samverka med varandra och med enskilda.

[16] Ds 2010:47.
[17] Prop. 2009/10:175, Offentlig förvaltning för demokrati, delaktighet och tillväxt.

I sitt förslag[18] till den nya förvaltningslagen argumenterade dock regeringen mot E-delegationen, och därmed *för* att en samverkansbestämmelse med motsvarande budskap som den nuvarande bestämmelsen i förvaltningslagen har en naturlig plats även i den nya förvaltningslagen.

För det första bör det, enligt regeringen, av bestämmelsen tydligt framgå att det är fråga om en mera generell skyldighet för myndigheter att samverka med varandra. Eftersom en myndighet alltid måste prioritera sina egna huvuduppgifter avgör den emellertid själv om den kan avsätta resurser för att hjälpa den myndighet som begär assistans. Regeringen framhöll även Förvaltningslagsutredningens förslag att bestämmelsen – i likhet med nuvarande reglering – inte ska ge stöd för några samverkansprojekt som faller utanför respektive myndighets verksamhetsområde. Regeringen pekade på E-delegationens invändning mot detta och att en sådan begränsning, enligt delegationens mening, inte tar tillräcklig hänsyn till e-förvaltningens behov av samverkan mellan myndigheter. Regeringen anförde dock att myndigheternas verksamhet, enligt legalitetsprincipen, styrs av de föreskrifter om arbetsuppgifterna som lagstiftaren eller någon annan normgivare har meddelat. Det innebär bl.a. att det inte får förekomma några nyskapelser i form av särskilda samarbetsorgan, som oberoende av tillämpliga föreskrifter fattar beslut som inte kan härledas till någon av de samverkande myndigheterna (jfr JO 1993/94 s. 458). Regeringen ansåg därför att begränsningen till verksamhetsområdet är både lämplig och väl avvägd, bl.a. eftersom en sådan huvudregel minskar risken för onödiga oklarheter och felgrepp i fråga om myndigheternas kompetens och befogenhet. Men, regeringen underströk på samma gång att:

> Detta utesluter samtidigt inte att man i specialförfattningar eller i förordningarna med myndighetsinstruktion även fortsättningsvis vid behov kan ta in särskilda föreskrifter om samverkan som går längre eller annars avviker från förvaltningslagen. Det skulle t.ex. kunna gälla föreskrifter om undantag från begränsningen till myndighetens verksamhetsområde eller om krav på att samverkan i en viss situation ska ske med andra än myndigheter. För det andra bör bestämmelsen ge en klar indikation om att samverkansskyldigheten inte enbart tar sikte på att förvaltningen

[18] Prop. 2017/18:180.

> generellt ska bli så enhetlig och effektiv som möjligt utan också är avsedd att underlätta för den enskilde i kontakterna med myndigheterna.[19]

Det vill säga att om det i andra lagar eller i förordningar finns någon bestämmelse som avviker från förvaltningslagen, tillämpas den bestämmelsen.[20] Se nedan.

5.3.3 Avvikande bestämmelser i andra lagar eller i förordningar

Enligt 3 § i den ännu så länge gällande förvaltningslagen och 4 § i den nya förvaltningslagen gäller att om en annan lag eller en förordning innehåller någon bestämmelse som avviker från denna lag, gäller den bestämmelsen.

Både konstitutionsutskottet och regeringen anförde i beredningen av den nya förvaltningslagen att det finns ett stort behov av att kunna meddela föreskrifter om förvaltningsförfarandet som avviker från den allmänna regleringen i förvaltningslagen.

Redan i förarbetena till 1971 års förvaltningslag framhölls att strävan varit att ge förfarandebestämmelserna karaktär av basregler som normalt skulle kunna tillämpas av det stora flertalet förvaltningsorgan i alla instanser och på alla verksamhetsområden. Samtidigt konstaterades det att en allmän lag inte kunde utformas så att den passar för alla situationer. På denna punkt skiljer sig inte förhållandena i dag åt från när förvaltningsrättsreformen genomfördes. I vissa fall finns det behov av att kunna ställa upp högre krav än vad som följer av den allmänna regleringen. I undantagsfall kan det också finnas behov av att göra vissa begränsningar i tillämpningsområdet för någon eller några bestämmelser i lagen. Som en allmän princip bör dock enligt propositionen alltjämt gälla att undantag bara ska förekomma om det kan motiveras av bärande sakliga och funktionella skäl.[21]

[19] Prop. 2017/18:180, s. 71.
[20] 3 § förvaltningslagen (1986:223), 4 § förvaltningslagen (2017:900).
[21] Prop. 2017/18:180, bet. 2017/18:KU2. jfr prop. 1971:30 del 2 s. 318.

5.4 Myndighetsförordningen om statliga myndigheters samarbete och samverkan

För statliga myndigheter som lyder under regeringen finns det i myndighetsförordningen en generell bestämmelse om samarbete på myndighetens eget initiativ. Av myndighetsförordningen framgår att myndigheten ska verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet.[22] Syftet är att samordna myndigheternas verksamhet med angränsande verksamheter för att underlätta för enskilda och för att undvika dubbelarbete vid myndigheterna. Ökad samverkan mellan myndigheterna borde, enligt Verksförordningsutredningen, leda till att det blir enklare för medborgare, företag, kommuner m.fl. att ha med statliga myndigheter att göra. Samverkande myndigheter bör leda till en effektivare förvaltning i stort.[23]

I myndighetsförordningen används inte begreppet samverkan utan där talas det om samarbete. Däremot används både begreppet samordna och samverkan i författningskommentarerna till förordningen.[24]

5.5 Förordningen om statliga myndigheters elektroniska informationsutbyte

Enligt 2 § i förordningen om statliga myndigheters elektroniska informationsutbyte framgår kortfattat att en myndighet i sin verksamhet ska främja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga förvaltningen.[25]

[22] 6 § myndighetsförordningen (2007:515).
[23] SOU 2004:23, Från verksförordning till myndighetsförordning, betänkande av Utredningen om en översyn av verksförordningen.
[24] SOU 2004:23, Från verksförordning till myndighetsförordning, betänkande av Utredningen om en översyn av verksförordningen.
[25] 2 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

5.6 Bestämmelser om kommunernas och landstingens samverkan

Reglerna för kommuners och landstings samverkan i form av kommunalförbund och gemensam nämnd finns i kommunallagen.[26] Av lagen framgår att kommuner och landsting får bilda kommunalförbund och lämna över skötseln av kommunala angelägenheter till sådana förbund. Kommuner och landsting får även besluta om gemensamma nämnder, dvs. att en nämnd ska vara gemensam med en annan kommun eller ett annat landsting.

Fullmäktige får besluta att en nämnd ska vara gemensam med en annan kommun eller ett annat landsting. En gemensam nämnd tillsätts i någon av de samverkande kommunerna eller landstingen och ingår i denna kommuns eller detta landstings organisation. En gemensam nämnd är, i motsats till ett kommunalförbund, inte en egen juridisk person utan ingår i en av de samverkande kommunernas eller landstingens politiska organisation. Denna kommun eller detta landsting brukar ofta omnämnas som värdkommunen eller värdlandstinget.

Ett kommunalförbund bildas genom att förbundsmedlemmarnas fullmäktige antar en förbundsordning. Kommunalförbundet är en offentligrättslig juridisk person som har egen rättskapacitet och är fristående i förhållande till sina medlemskommuner. Organisatoriskt är kommunalförbunden uppbyggda på i princip samma sätt som en kommun eller ett landsting.

5.6.1 Exempel på samverkan mellan kommuner

Ett exempel på formaliserad samverkan mellan kommuner är Norrbottens e-nämnd som har kommit till för att förverkliga regeringens intentioner för e-samhället.[27] De kommuner som samverkar genom Norrbottens e-nämnd är, förutom Luleå kommun, Arjeplogs kommun, Arvidsjaurs kommun, Bodens kommun, Gällivare kommun, Haparanda kommun, Jokkmokks kommun, Kalix kommun, Pajala kommun, Piteå kommun, Älvsbyns kommun, Överkalix kommun och Övertorneå kommun. Luleå kommun är värdkommun för nämn-

[26] 3 kap 8–9 §§ och 9 kap. kommunallagen (2017:725).
[27] https://www.lulea.se/kommun--politik/kommunens-organisation/namnder/e-namnden.html. 2017-11-12.

den. Norrbottens e-nämnd består av två politiker från varje kommun, en ledamot och en ersättare. Luleå kommun har ordförandeposten.

Nämndens inriktning för verksamheten är att med medborgarens fokus och med verksamhetens behov som utgångspunkt stödja kommunerna i Norrbotten för en snabbare utveckling inom e-förvaltning och digitaliseringen.

Norrbottens e-nämnd pekar ut tre övergripande mål, som är identiska med de övergripande målen i SKL:s strategi för eSamhället från 2011:

- Enklare vardag för privatpersoner och företag,
- Smartare och öppnare förvaltning som stödjer innovation och delaktighet,
- Högre kvalitet och effektivitet i verksamheten.

Syftet med den formaliserade samverkan i Norrbottens e-nämnd är att skapa förutsättningar för:

- att minska kostnader för initiativ som kan genomföras gemensamt,
- att säkra kompetensförsörjning,
- att effektivare utnyttja resurser genom samverkan,
- att bidra till en snabbare utveckling inom e-förvaltning och digitalisering,
- att implementera intentionerna i den nationella strategin för e-samhället.

5.6.2 Kommunutredningens förslag om vidgade möjligheter till avtalssamverkan

Enligt Kommunutredningen finns det en utbredd efterfrågan på att utvidga möjligheterna till kommunal avtalssamverkan. Behovet är brett, men gäller framför allt möjligheten att utnyttja den kompetens som finns hos anställda i andra kommuner. Områden som lyfts fram är bl.a. specialisttjänster som innefattar myndighetsutövning, it och digitalisering samt administration.

Kommunutredningen har föreslagit att det i den nya kommunallagen ska införas en bestämmelse som ska träda i kraft den 1 juli 2018 och som innebär att en kommun eller ett landsting får träffa avtal om att dess uppgifter helt eller delvis ska utföras av en annan kommun eller ett annat landsting (avtalssamverkan).[28] Genom ett sådant avtal får en kommun eller ett landsting utföra uppgifter åt en annan kommun eller landsting, utan hinder av vad som anges i kommunallagen om anknytning till kommunens eller landstingets område eller dess medlemmar (lokaliseringsprincipen). Kommuner och landsting får komma överens om att uppdra åt en anställd i den andra kommunen eller det andra landstinget att besluta på kommunens eller landstingets vägnar i ett visst ärende eller en viss grupp av ärenden (extern delegering). Vid sådan delegering av ärenden gäller bestämmelserna i kommunallagen om jäv, vissa begränsningar av möjligheten till delegation, vidaredelegation, brukarmedverkan och anmälan av beslut.

[28] SOU 2017:77, En generell rätt till kommunal avtalssamverkan, delbetänkande av Kommunutredningen.

6 Effektiv styrning av förvaltningsgemensamma digitala funktioner

6.1 Ett tydligt offentligt åtagande är utgångspunkten för effektiv styrning

Utredningen bedömer:
att det offentliga åtagandet för förvaltningsgemensamma digitala funktioner behöver regleras i författning.

I budgetpropositionen för 2018 anförde regeringen att:

> Enskildas, organisationers och företags behov och förväntningar är en utgångspunkt för den offentliga förvaltningen. Dagens snabba samhällsutveckling innebär att den offentliga sektorn måste vara både förutsebar och anpassningsbar. Det ställer höga krav på en mer sammanhållen styrning på flera nivåer.[1]

I samma budgetproposition bedömde regeringen även att lagstiftningen måste anpassas ytterligare för att ge tillräckligt stöd för digital utveckling och samverkan inom offentlig sektor.

I delbetänkandet bedömde utredningen att det från regeringens sida har varit ett medvetet val att delegera ansvaret för arbetet med e-förvaltning till myndigheterna. Att arbetet varit framgångsrikt i många avseenden kompenserade, enligt utredningen, inte för de begränsningar detta har inneburit. Utredningen konstaterade att regeringen har avstått från att använda de styrinstrument som står till buds, t.ex. genom att inte förtydliga vilka uppdrag myndigheterna har när det gäller digitalisering. Vidare saknas styrande mål för vad som ska

[1] Prop. 2017/18:1, utgiftsområde 2, s. 86.

uppnås och preciseringar av vad som ska anses vara offentliga åtaganden i den nationella digitala infrastrukturen.[2]

Motsvarande synpunkter har under flera år förts fram av flera andra utredningar i kommittéväsendet liksom i granskningar av Riksrevisionen, m.fl.

I budgetpropositionen för 2018 konstaterade regeringen ånyo att styrningen och samordningen inom den offentliga sektorn behöver stärkas så att de besparingar och nyttor som digitalisering medför ska kunna realiseras. Regeringen anförde att flera gemensamma insatser krävs för att nå regeringens mål för digitaliseringen av den offentliga förvaltningen. En sådan insats är att – huvudsakligen i enlighet med utredningens förslag i delbetänkandet – inrätta en myndighet för digitalisering av den offentliga sektorn.

Utredningens tolkning av regeringens direktiv[3] till den särskilda utredare som ska förbereda och genomföra bildandet av den nya myndigheten är, att regeringen nu har *påbörjat* ett arbete med att utveckla sin styrning av den offentliga förvaltningens digitalisering. Ett arbete som, enligt utredningens mening, måste fortsätta med full kraft för att inte den förvaltningsgemensamma digitala utvecklingen ska bromsas i onödan. Regeringens styrning av den digitala förvaltningen måste utvecklas till en effektiv och tydlig process för att skapa goda förutsättningar för den förvaltningsgemensamma digitala utvecklingen.

För att säkerställa en mer effektiv styrning av nationella digitala tjänster ska utredningen, enligt direktiven, analysera om det är mer ändamålsenligt med *en enhetlig* modell för organisering och ansvarsfördelning av förvaltningsgemensamma digitala funktioner.

Utredningen bedömer emellertid att *en* enhetlig modell för att styra samtliga nuvarande och framtida nationella digitala tjänster på samma sätt inte är ett effektivt sätt att styra. En sådan förutbestämd, enhetlig modell skulle med stor sannolikhet skapa ett stelbent och ineffektivt sätt att styra.

Hur de enskilda nationella digitala tjänsterna styrs och ska styras kommer att variera och måste bedömas från fall till fall beroende på konstitutionella krav, tekniska och ekonomiska förutsättningar, typ av funktion, samverkansbehov mellan olika aktörer etc.

---

[2] SOU 2017:23, digitalforvaltning.nu.
[3] Dir. 2017:117, Inrättande av en myndighet för digitalisering av den offentliga sektorn.

Ett problem är att det inte finns något bindande mål för området digitalisering inom den offentliga sektorn. Utredningen föreslår därför att riksdagen och regeringen ska besluta om sådana mål. Se kapitel 7.

Ett annat problem med den nuvarande styrningen är att det i den offentliga förvaltningen saknas nödvändig författningsreglering av sådana befintliga tjänster som för närvarande benämns nationella digitala tjänster, såsom Mina meddelanden och Svensk e-legitimation. Utredningen vill understryka att den offentliga förvaltningens digitala utveckling och samverkan inte kan gå utöver vad rättsordningen medger. Det handlar inte bara om att ge förvaltningen ett tillräckligt formellt stöd för digital utveckling och samverkan inom den offentliga sektorn utan även om att i författning – för var och en av de nationella digitala tjänsterna – besluta om vad som ska vara det offentliga åtagandet. I detta betänkande lämnar utredningen förslag till författningsreglering av Mina meddelanden och Svensk e-legitimation samt kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Vad som bör vara ett offentligt åtagande är i varje enskilt fall ett politiskt ställningstagande och ett politiskt beslut. Ett sådant beslut kan inte delegeras eller decentraliseras till offentliga myndigheter.

Några skäl som brukar anges för ett offentligt åtagande är effektivare samhällsekonomi, fördelningsmotiv, stabiliseringspolitik samt ansvarstagande för det medborgarna inte själva har kunskap och information nog att sköta själva, dvs. en rad olika mål och motiv som alla kan diskuteras.[4] Den privata marknaden kan inte uppfylla alla behov som är viktiga för landet och medborgarna. Vissa kollektiva nyttigheter måste i stället garanteras genom offentliga åtaganden. Offentliga åtaganden kan också motiveras av s.k. externa effekter, dvs. effekter som kan uppstå då någon inte tar önskvärd hänsyn till andra. Även stordriftsfördelar, bristande konkurrens, dålig konsumentinformation eller en skev resursfördelning kan motivera offentliga åtaganden.[5]

Förvaltningskommittén menade i betänkandet Styra och ställa – förslag till en effektivare statsförvaltning att frågan om vad som bör vara statliga myndighetsuppgifter och därmed ett statligt åtagande bör besvaras utifrån en pragmatisk ansats.

[4] Den effektiva staten, Statskontorets antologi, 2012.
[5] Ds 2000:1, Kommittéhandboken.

> Utifrån en given politisk ambition vid en viss tidpunkt bör en bedömning göras av de enskilda samhällsområdenas art och förutsättningar, innan det statliga åtagandet i form av myndighetsuppgifter närmare preciseras.[6]

Förvaltningskommittén bedömde samtidigt att de flesta statliga åtaganden förutsätter utförande av myndighetsuppgifter i någon form och bedömningar av hur uppgifter bör fördelas måste göras från fall till fall och med iakttagande av de särskilda förutsättningar som råder vid bedömningstillfället. Såväl demokrati- och rättssäkerhets- som effektivitetsargument måste beaktas.

Genom att statsmakterna beslutar om vad som ska vara offentliga åtaganden förtydligas samtidigt gränserna för vad som är myndighetsuppgifter, inte enbart i förhållande till enskilda, utan även vad som bör vara förbehållet marknadens aktörer. Detta kan exempelvis ha betydelse för avgöranden om huruvida verksamheter kan sägas vara så kallad egenregiverksamhet eller omfattas av upphandlingsbestämmelserna.[7]

Vad som slutligen bör vara en statlig myndighetsuppgift kan, enligt Förvaltningskommittén, med ett förenklat och kortfattat svar sägas kräva en politisk bedömning, som görs utifrån vid en viss tidpunkt gällande förutsättningar, politiska ambitioner, kunskaper och värderingar.[8]

Befintliga nationella digitala tjänster såsom Mina meddelanden och Svensk e-legitimation, liksom med största sannolikhet de flesta framtida nationella digitala tjänster, bygger på samverkan mellan den offentliga och privata sektorn.

Det finns därför, enligt utredningen, behov av att för *var och en* av de förvaltningsgemensamma digitala funktionerna närmare analysera och precisera omfattningen av det offentliga åtagandet i förhållande till de privata aktörernas roll. Med andra ord är det viktigt att för varje förvaltningsgemensam digital funktion fatta beslut om vilken aktör som har ansvar för vad och vad, som både formellt och i praktiken, ska vara ett offentligt åtagande som garanteras av riksdagen och regeringen.

---

[6] SOU 2008:118, Styra och ställa – förslag till en effektivare statsförvaltning.
[7] Se Kammarrätten i Stockholms dom 2017-06-21, mål nr 7355-16.
[8] SOU 2008:118, Styra och ställa, slutbetänkande av 2006 års förvaltningspolitiska kommitté.

Till detta hör även det faktum att Sveriges medlemskap i Europeiska unionen påverkar på ett flertal områden – i hög grad – innehållet i och utförandet av de nationella myndigheternas uppgifter och därmed utformningen av det offentliga åtagandet. Det gemensamma regelverket för EU:s medlemsstater kan på olika områden begränsa och/eller styra det nationella statliga åtagandet. De offentliga myndigheterna omfattas bl.a. av ett flertal för medlemsstaterna gemensamma regelverk inom olika politikområden som ställer krav på den nationella digitala förvaltningsutvecklingen och riksdagens och regeringens styrning av den digitala förvaltningen.

Utredningens ambition är att förslagen om effektiv styrning av nationella digitala tjänster ska fungera som ett effektivt stöd för de offentliga myndigheterna att nå och redovisa de resultat som riksdagen och regeringen beslutat i dessa avseenden. Utmaningen är, givet dessa utgångspunkter, att styra statliga myndigheter, kommuner och landsting mot mål som är gemensamma för hela den offentliga förvaltningen. För detta behöver riksdagen och regeringen – med ett förvaltningsövergripande perspektiv – använda en väl balanserad kombination av flera olika styrmedel.

6.2 Förvaltningsgemensamma digitala funktioner

Utredningen bedömer:
att begreppet förvaltningsgemensamma digitala funktioner på ett bättre sätt än begreppet nationella digitala tjänster, definierar och avgränsar innebörden av sådana digitala medel.

Utredningen föreslår:
att begreppet nationella digitala tjänster bör ersättas av begreppet förvaltningsgemensamma digitala funktioner.

6.2.1 Definition och terminologi

I utredningens uppdrag har ingått att, med utgångspunkt i Mina meddelanden och Svensk e-legitimation, närmare definiera vad som är en nationell digital tjänst. Enligt utredningens bedömning är begreppet nationella digitala tjänster relativt nytt. Det återfinns inte i tidigare

dokument från regeringen eller E-delegationen utan tycks aktualiseras först i direktiven till denna utredning.

Enligt utredningens direktiv är nationella digitala tjänster sådana gemensamma digitala lösningar som är av infrastrukturkaraktär och som är en avgörande förutsättning för offentlig e-tjänsteutveckling i sin helhet. De nationella digitala tjänsterna ska kunna användas inom hela den offentliga sektorn och syftar till att underlätta elektronisk hantering av ärenden och kontakter med enskilda. Formuleringen lämnar öppet för vissa tolkningar. Att nationella digitala tjänster ska kunna användas inom hela den offentliga sektorn väljer utredningen att tolka som ett mål snarare än en del av en definition. Den andra delen av meningen är däremot viktig. En nationell digital tjänst avser något som är nära kopplat till en tjänst riktad till enskilda, dvs. en fysisk eller juridisk person som inte är en myndighet eller annat offentligt organ. Som distinktion är detta viktigt. Begreppet nationell digital tjänst omfattar således inte rena internadministrativa system, men kan omfatta lösningar kopplade till exempelvis ärendehandläggning.

Enligt direktiven ska de nationella digitala tjänsterna utvecklas utifrån medborgarnas behov, vilket förutsätter en bred och omfattande samverkan mellan statliga myndigheter, mellan kommunala myndigheter, mellan stat och kommun samt mellan den offentliga och den privata sektorn.

Gemensamma digitala lösningar kan, enligt regeringen, vara lösningar som används av hela den offentliga sektorn, sektorspecifika lösningar och lösningar som utvecklas i samverkan mellan ett fåtal myndigheter.

I ljuset av detta finner utredningen det vara befogat att överväga om termen nationella digitala tjänster är den lämpligaste för det begrepp som avses. I uttrycket är det ordet ”nationell” som ska skilja det som avses från digitala tjänster i övrigt och markera att det är fråga om något som sträcker sig utanför den enskilda myndighetens ansvarsområde och kanske även överskrider gränsen för statlig och offentlig verksamhet.

Enligt utredningens uppfattning är det dock fråga om tjänster som ska tillhandahållas av myndigheter eller av enskilda med stöd av författning. Vidare är det utmärkande för deras karaktär att vara gemensamma och inte bara vara en angelägenhet för en eller ett fåtal offentliga myndigheter. De är, som regeringen framhåller, gemensamma

digitala lösningar som är av infrastrukturkaraktär och som är en avgörande förutsättning för offentlig e-tjänsteutveckling i sin helhet.

Det framstår därför som mer rättvisande att beskriva de aktuella tjänsterna som ”förvaltningsgemensamma” snarare än ”nationella”. Ordet ”nationell” implicerar också att dess motsats kan vara ”lokal”, ”regional” eller ”internationell” vilket leder tankarna fel.

Även ordet ”tjänst” bör prövas. Det kan diskuteras om ordet ”tjänst” i tillräckligt hög grad anger den särprägel som det här finns behov av att uttrycka. E-delegationen definierade en *digital tjänst* som en paketerad service eller lösning som erbjuds för att tillgodose ett behov och som förmedlas digitalt.[9] Myndigheter tillhandahåller många digitala tjänster, men de flesta av dessa innebär inga utmaningar vad gäller styrning, organisation och finansiering. Utredningen menar därför att ett annat ord än ”tjänst” bör användas. Ett lämpligare ord är enligt utredningens mening ”funktion”.

Utredningen anser att begreppet *förvaltningsgemensamma digitala funktioner* på ett tydligare sätt definierar och avgränsar innebörden av vad som här avses.

Att en funktion identifieras som en förvaltningsgemensam digital funktion innebär därmed inte automatiskt att det är staten ensam som ska tillhandahålla den eller att den ska tillhandahållas utan kostnad för brukaren. Detta är en fråga som får avgöras utifrån en bedömning av varje enskild förvaltningsgemensam digital funktion.

6.2.2 Vad kan vara en förvaltningsgemensam digital funktion?

I utredningens direktiv anges Mina meddelanden och elektroniska identitetshandlingar som exempel på förvaltningsgemensamma digitala funktioner. Bägge dessa funktioner fanns bland det som E-delegationen betraktade som strategiska förvaltningsgemensamma utvecklingsprojekt.

E-delegationen studerade också möjligheten att förverkliga idén att uppgifter bara ska behöva lämnas en gång genom att införa en databas för frivillig uppdatering av kontaktuppgifter. I Norge har införts ett nationellt kontaktregister i vilket 90 procent av befolkningen över

[9] E-delegationen, Vägledning för digital samverkan, v 4.1, s. 73.

15 år frivilligt har lagt in kontaktuppgifter, dvs. mobiltelefonnummer och privat e-postadress. Uppgifterna används av statliga myndigheter och kommuner för påminnelser.[10] I Sverige har SKL uppdragit åt Inera AB att göra en förstudie av en svensk motsvarighet.[11]

Det finns ett stort behov, bland annat hos landstingen, av säker kommunikation mellan myndigheter, som dessutom kan integreras med ärendeflöden inom myndigheterna. Systemen behöver kunna hantera behörigheter och elektroniska underskrifter. Försöksverksamhet pågår på flera håll. System för säker kommunikation mellan myndigheter kan också ses som ett exempel på en förvaltningsgemensam digital funktion.[12]

Ytterligare några exempel är standarder för förmedling av information mellan myndigheter och företag och standarder för förmedling av öppna data.

Den nod som ska förmedla gränsöverskridande digital trafik för elektronisk identifiering mellan myndigheter och utfärdare av identitetscertifikat med anledning av genomförandet av eIDAS-förordningen är ett annat exempel på en förvaltningsgemensam digital funktion, liksom det kopplingsregister som föreslås ska sammanföra utländska identitetsbeteckningar med svenska personnummer.

6.3 All offentlig makt i Sverige utgår från folket

Utredningens överväganden och förslag tar sin utgångspunkt i regeringsformen och relevanta EU-författningar och behandlar huvudsakligen riksdagens och regeringens styrning av offentliga myndigheter, dvs. kommuner, landsting och statliga myndigheter som lyder under regeringen.

> All offentlig makt i Sverige utgår från folket.
>
> Den svenska folkstyrelsen bygger på fri åsiktsbildning och på allmän och lika rösträtt. Den förverkligas genom ett representativt och parlamentariskt statsskick och genom kommunal självstyrelse.
>
> Den offentliga makten utövas under lagarna.[13]

[10] www.difi.no/rapporter-og-statistikk/nokkeltall-og-statistikk/digitalisering#4321
[11] Mina kontaktuppgifter en nationell delningstjänst för digitala kontaktuppgifter, Förstudie på uppdrag av Sveriges Kommuner och landsting 2016-12-10 – 2017-03-31, Inera 2017.
[12] Rapport Säker digital meddelandehantering mellan myndigheter Nuläges- behovs- och marknadsanalys, SKL 2016.
[13] 1 kap. 1 § regeringsformen (1974:152).

Till skillnad från de myndigheter som lyder under regeringen är varje kommun och landsting, enligt regeringsformens bestämmelser, en egen juridisk person. Styrelsen i varje kommun och varje landsting är ansvarig inför *fullmäktige*. Samtliga myndigheter under regeringen ingår i en och samma juridiska person och varje myndighets ledning är ansvarig inför *regeringen*.

Hur riksdagen och regeringen ska och får styra och följa upp de offentliga verksamheterna och deras resultat, liksom bestämmelserna för det allmännas relation till enskilda utgår från regeringsformens bestämmelser. Utredningens bedömningar och förslag till effektiv styrning av förvaltningsgemensamma digitala funktioner tar därmed sin utgångspunkt i regeringsformens bestämmelser om de offentliga myndigheterna, däribland det kommunala självstyret.

6.3.1 Regeringsformen

I regeringsformens första kapitel fastställer riksdagen statsskickets grunder. Riksdagen slår fast att all offentlig makt i Sverige utgår från folket och att den offentliga makten utövas under lagarna.

Den svenska folkstyrelsen bygger på fri åsiktsbildning och på allmän och lika rösträtt. Folkstyrelsen förverkligas genom ett representativt och parlamentariskt statsskick och genom kommunal självstyrelse. Den offentliga makten utövas under lagarna.[14]

Den offentliga makten ska utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet.

Individens personliga, ekonomiska och kulturella välfärd ska vara grundläggande mål för den offentliga verksamheten.

Det allmänna ska främja en hållbar utveckling som leder till en god miljö för nuvarande och kommande generationer.

Det allmänna ska verka för att demokratins idéer blir vägledande inom samhällets alla områden samt värna den enskildes privatliv och familjeliv. Det allmänna ska verka för att alla människor ska kunna uppnå delaktighet och jämlikhet i samhället och för att barns rätt tas till vara m.m.[15]

[14] 1 kap. 1 § regeringsformen (1974:152).
[15] 1 kap. regeringsformen (1974:152).

Riksdagen som är folkets främsta företrädare stiftar lag och en lag får inte ändras eller upphävas på annat sätt än genom lag, dvs. ingen annan än riksdagen kan ändra eller upphäva en lag. Riksdagen beslutar om skatt till staten och bestämmer hur statens resurser ska användas. Riksdagen granskar rikets styrelse och förvaltning.[16] Regeringen styr riket och är ansvarig inför riksdagen.[17]

I riket finns kommuner på lokal och regional nivå, dvs. kommuner och landsting.[18] Kommunerna och landstingen sköter lokala och regionala angelägenheter av allmänt intresse på den kommunala självstyrelsens grund. På samma grund sköter kommunerna och landstingen även de övriga angelägenheter som bestäms i lag.[19]

För rättskipningen finns det domstolar. Ingen myndighet, inte heller riksdagen, får bestämma hur en domstol ska döma i det enskilda fallet eller hur en domstol i övrigt ska tillämpa en rättsregel i ett särskilt fall. Ingen annan myndighet får heller bestämma hur dömande uppgifter ska fördelas mellan enskilda domare.

Riksdagen får inte fullgöra förvaltningsuppgifter eller rättskipningsuppgifter i vidare mån än vad som följer av grundlag[20] eller riksdagsordningen.[21] Rättstvister mellan enskilda får inte utan stöd av lag avgöras av andra myndigheter än domstolar.

För den offentliga förvaltningen finns det statliga och kommunala förvaltningsmyndigheter.[22] Ingen myndighet, inte heller riksdagen eller en kommuns beslutande organ, får bestämma hur en förvaltningsmyndighet i ett särskilt fall ska besluta i ett ärende som rör myndighetsutövning mot en enskild eller mot en kommun eller som rör tillämpning av lag.

Domstolar, förvaltningsmyndigheter och andra som fullgör offentliga förvaltningsuppgifter ska i sin verksamhet beakta allas likhet inför lagen samt iaktta saklighet och opartiskhet.[23]

---

[16] 1 kap. 4 § regeringsformen (1974:152).
[17] 1 kap. 6 § regeringsformen (1974:152).
[18] 1 kap. 7 § regeringsformen (1974:152).
[19] 14 kap. regeringsformen (1974:152).
[20] Regeringsformen, (1974:152), Successionsförordningen (1820:0926), Tryckfrihetsförordningen (1949:105) och Yttrandefrihetsgrundlagen (1991:1469).
[21] Riksdagsordningen (2014:801). Utöver grundlagarna finns riksdagsordningen, som har en särställning mellan grundlag och vanlig lag. För att ändra den krävs endast ett riksdagsbeslut, men detta måste fattas med kvalificerad majoritet, det vill säga minst tre fjärdedelar av de röstande och mer än hälften av ledamöterna. I riksdagsordningen finns detaljerade bestämmelser om riksdagen och dess arbetsformer.
[22] 1 kap. 8 § regeringsformen (1974:152).
[23] 1 kap. 9 § regeringsformen (1974:152).

Förvaltningsuppgifter kan överlämnas åt kommuner och även åt andra juridiska personer och enskilda individer. Om förvaltningsuppgiften innefattar myndighetsutövning får ett överlämnande endast göras med stöd av lag.

6.3.2 EU-förordningar och EU-direktiv

Sedan den 1 januari 1995 är Sverige är medlem i Europeiska unionen, EU. En bestämmelse om medlemskapet infördes i regeringsformens första kapitel 2010.[24]

Sverige och de övriga medlemsländerna beslutar tillsammans om nya EU-lagar, som ska gälla i alla EU-länder. Det överstatliga samarbetet innebär att medlemsstaterna har avstått från makten att själva fatta beslut inom vissa områden.[25] En stor andel av de bestämmelser som svenska medborgare och offentliga myndigheter ska följa har därmed sin grund i regler meddelade på EU-nivå och inte enligt regeringsformens bestämmelser om normgivning. De grundläggande bestämmelserna meddelas i dessa fall inte av riksdagen eller regeringen utan av organ på EU-nivå. Unionsrätten har på dessa områden företräde framför nationella bestämmelser, däribland i princip även regeringsformen och andra grundlagar. Den slutliga uttolkningen av sådana bestämmelser görs av EU-domstolen och inte av de nationella domstolar som i regeringsformen pekas ut som högsta dömande instanser, dvs. Högsta domstolen och Högsta förvaltningsdomstolen.

En EU-*förordning* är en EU-lag som gäller alla EU:s medlemsländer, de företag och myndigheter som är verksamma i länderna och ländernas medborgare. En EU-förordning som har trätt i kraft gäller direkt och likadant i alla medlemsländer som en del av den nationella lagstiftningen. En EU-förordning är direkt tillämplig vilket betyder att ett medlemsland, efter att en förordning har antagits, inte behöver göra något mer för att den ska gälla i medlemslandet. Ett medlemsland får inte göra något som går emot det som står i förordningen – EU-förordningen gäller. Det betyder att bestämmelserna inte får arbetas om eller justeras med hänsyn till medlemsländernas egna förhållan-

[24] Lag (2010:1408).
[25] Det innebär bland annat att vissa beslut som tidigare fattades i Sveriges riksdag, numera fattas gemensamt tillsammans med övriga EU-länder.

den. Varje enskild medlemsstat har dock rätten att komplettera förordningen med nationella regler i viss omfattning.

Exempel på en EU-förordning som innehåller bestämmelser om e-tjänster och förvaltningsgemensamma digitala funktioner är eIDAS-förordningen.[26]

Ett annat exempel är Europaparlamentets och rådets dataskyddsförordning kallad GDPR[27] med syftet att stärka skyddet för fysiska personer vid behandling av personuppgifter inom Europeiska unionen. Förordningen antogs den 27 april 2016 och kommer börja gälla den 25 maj 2018. Den ersätter då Dataskyddsdirektivet från 1995.[28] GDPR kommer börja gälla direkt i alla medlemsstater och ersätter då tidigare nationella bestämmelser. I Sverige kommer dataskyddsförordningen ersätta personuppgiftslagen.[29]

Ett EU-*direktiv* är en EU-lag som innehåller bindande bestämmelser som riktar sig till EU:s medlemsländer. Till skillnad mot EU-förordningar är det bara resultatet av EU-direktiven och när resultatet ska vara uppnått som är bindande. Medlemsländerna beslutar själva vad de ska göra för att uppnå resultatet. Ett EU-direktiv ger varje medlemsland handlingsutrymme och om landet redan har de regler som föreskrivs i direktivet behöver det inte göra något utan kan hänvisa till de befintliga reglerna. Om det uppstår en tvist är det EU-domstolen som ska avgöra om direktivet är uppfyllt.[30]

---

[26] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

[27] (EU) nr 2016/679), förkortat GDPR efter engelskans General Data Protection Regulation. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

[28] Dataskyddsdirektivet (95/46/EG).

[29] Personuppgiftslagen (1998:204).

[30] Exempel på EU-direktiv är PSI-direktivet. Europaparlamentet och rådet antog den 17 november 2003 det s.k. PSI-direktivet. Direktivet trädde i kraft den 31 december 2003 och innehåller minimiregler. Direktivet har i Sverige genomförts genom lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen (PSI-lagen). Kommissionen har sett över tillämpningen av direktivet och föreslagit vissa ändringar. Ändringsdirektivet antogs av Europaparlamentet och rådet den 26 juni 2013 och trädde i kraft den 27 juni 2013. Ändringsdirektivet ska ha genomförts senast den 18 juli 2015. Ändringsdirektivet föranledde vissa ändringar i den svenska PSI-lagen från och med 1 juli 2015. Syftet med PSI-lagen är att främja utvecklingen av en informationsmarknad genom att underlätta enskildas användning av handlingar som tillhandahålls av myndigheter. Lagen avser att förhindra att myndigheter beslutar om sådana villkor för vidareutnyttjande av handlingar som begränsar konkurrensen.

6.4 Effektiv styrning

Utredningen bedömer:
att styrningen är effektiv när de offentliga myndigheternas (de styrdas) agerande och resultat stämmer överens med riksdagens och regeringens (de styrandes) direktiv, önskemål och förväntningar. För att uppnå detta måste riksdagens och regeringens styrning riktas direkt till den eller de myndigheter som ska styras. Styrningen behöver anpassas både till den eller de som ska styras och till den typ av verksamhet, eller som i denna utrednings uppdrag, de förvaltningsgemensamma digitala funktioner som avses. För detta behöver riksdagen och regeringen använda och utforma en väl balanserad kombination av flera olika styrmedel.

De krav som demokratin ställer innebär att förvaltningen ska fullgöra sina uppgifter i enlighet med de beslut som fattas av riksdagen och regeringen. Förvaltningen ska vara rättssäker vilket innebär att den ska fatta materiellt riktiga beslut på grundval av gällande lagar och andra författningar. Förvaltningen ska vara effektiv vilket innebär att åstadkomma avsedda resultat och uppnå fastställda mål på ett kostnadseffektivt sätt. Förvaltningen ska vara medborgarorienterad vilket innebär att myndigheternas verksamhet ska orienteras mot ett påvisbart utbyte för medborgarna.

Resonemangen nedan tar sin huvudsakliga utgångspunkt i riksdagens och regeringens styrning av *kärnverksamheter/angelägenheter*. Utredningen menar dock att motsvarande resonemang är direkt tillämpligt även på riksdagens och regeringens styrning av den offentliga förvaltningens användning av *medel* för att genomföra sina kärnverksamheter och kommunala angelägenheter, i detta fall förvaltningsgemensamma digitala funktioner.

Det finns många definitioner av styrning. Styrning har dock alltid ett syfte eller mål. Det kan vara att förändra en verksamhet eller ett beteende, men också att se till att bevara status quo. Styrning handlar således, med en övergripande definition, om aktiviteter som genomförs i syfte att uppnå mål med hjälp av valda medel.[31]

[31] Statskontoret 2005:28, Reglering och andra styrmedel, En studie av hur staten styr kommuner och landsting.

I sitt betänkande Att styra staten – regeringens styrning av sin förvaltning analyserade Styrutredningen regeringens styrning av sin förvaltning.

Styrutredningen pekade på det självklara att styrning bygger på att det finns minst två parter och att den ena parten försöker påverka den andra partens agerande. Styrning går ut på att den styrdas agerande ska stämma överens med den styrandes direktiv, önskemål och förväntningar.

Den som styr väljer vad styrningen ska riktas mot, dvs. styrningen måste ha ett objekt. En förutsättning för styrning är också att den på något sätt förmedlas till myndigheterna. I praktiken handlar det om att styrningen behöver kopplas ihop med det eller de objekt som ska styras.

Styrutredningen betonade att en viktig grundförutsättning i alla diskussioner om styrning (och utvärdering) är att skillnaderna mellan myndigheterna är stora. Enligt Styrutredningen är det av central betydelse att styrningen utformas så att dessa skillnader beaktas.[32]

Den grundläggande styrningen av en myndighet och dess verksamhet finns i lagar, respektive myndighets instruktion och finansiering, m.m. Utgångspunkten är att de förvaltningsuppgifter som följer av vad riksdagen och regeringen har bestämt, ska vara det aktuella statliga åtagandet.

Valet av styrmedel och utformningen av dem bör övervägas och kunna förändras allt eftersom verksamheten utvecklas, de politiska prioriteringarna ändras, om det uppstår nya problem m.m.

Enligt regeringens bedömning[33] bör styrningen av förvaltningsmyndigheterna i så hög grad som möjligt vara utformad så att den bäst gynnar syftet med respektive verksamhet. Styrningen av statlig verksamhet bör utvecklas med inriktningen att kombinera olika styrformer för att skapa bästa möjliga förutsättningar för de statliga myndigheterna att förverkliga regeringens politik, utföra sina uppgifter i övrigt och upprätthålla grundläggande värden.

Styrningen bör vara tydlig, inriktad mot verksamheternas resultat, vara verksamhetsanpassad och ha ett medborgarperspektiv. Tydlig innebär bland annat att myndighetens uppdrag preciseras genom att

[32] SOU 2007:75, Att styra staten – regeringens styrning av sin förvaltning, betänkande av Styrutredningen.
[33] 2009/10:175, bet. 2009/10:FiU38, rskr. 2009/10:315.

uppgifter, regler och i förekommande fall mål och prioriteringar anges. Mål och uppgifter till myndigheterna formuleras så att respektive myndighet själv råder över eller har rimliga möjligheter att genom olika åtgärder kunna genomföra uppdraget på ett tillfredsställande sätt. Regeringen har betonat att olika styrmedel såsom ledningsform, utnämningar, instruktion, regleringsbrev, särskilda regeringsbeslut, dialog och möten bör kombineras och användas samordnat för att skapa bästa möjliga förutsättningar för statsförvaltningen att förverkliga regeringens politik.

För att bestämma styrbehovet och därmed kombinationen av styrmedel måste, enligt Ekonomistyrningsverket (ESV),[34] hänsyn tas till verksamhetens tillstånd och verksamhetens natur samt det förväntade resultatet i det enskilda fallet. Även tidsaspekten är viktig vid valet av styrmedel. En fråga här är om myndigheten och verksamheten ska styras på kort, medellång eller lång sikt. Valet av styrmedel kan också bero på om en verksamhet eller ett efterfrågat resultat är politiskt prioriterat men även om något inte fungerat som avsett. Valet av styrmedel bör, enligt ESV, även avvägas och anpassas till om det är fler myndigheter och organisationer som ska bidra till ett gemensamt resultat så att styrmedlen underlättar och bidrar till att det gemensamma resultatet kan uppnås.[35]

I styrning av offentlig verksamhet ingår att följa upp, analysera, utvärdera, bedöma, redovisa och revidera de uppnådda resultaten, hur pengarna har använts osv. Bestämmelserna om resultatredovisning m.m. finns i olika lagar och förordningar för respektive kommuner och landsting, statliga myndigheter, regeringen och riksdagen.

6.4.1 Styrobjekten – de offentliga myndigheterna

De offentliga myndigheterna är ett nödvändigt instrument för att genomföra av riksdagen och regeringen fattade beslut. Styrningen av myndigheterna är därför av stor betydelse för att statsmakterna ska kunna uppfylla det politiska mandat väljarna har gett dem.[36]

[34] ESV 2007:23, Resultat och styrning i statsförvaltningen.
[35] A.a.
[36] SOU 2008:118, Styra och ställa – förslag till en effektivare statsförvaltning, slutbetänkande av 2006 års förvaltningskommitté, s. 59.

Även om det är formella skillnader mellan de offentliga myndigheterna, dvs. statliga myndigheter, kommuner och landsting, finns det gemensamma bestämmelser som gäller för alla offentliga myndigheter.

Med myndighet menas ett statligt eller kommunalt organ som utför offentliga förvaltningsuppgifter och som en offentligrättslig författning har skapat för detta ändamål, dvs. statliga och kommunala förvaltningsmyndigheter samt domstolar. Vad som avses med ”myndighet” bestäms därmed utifrån formerna för verksamheten och inte efter arbetsuppgifternas art eller vilken funktion organet har. Det innebär att även om ett enskilt organ med stöd av regeringsformen[37] har fått offentliga arbetsuppgifter eller myndighetsutövning, kan organet inte – enligt regeringsformen – anses vara en myndighet. Att myndighetsbegreppet är organisatoriskt och inte funktionellt innebär också att även sådana myndigheter som inte har myndighetsutövning som sin huvudsakliga uppgift, är myndigheter.[38]

Regeringen föreslog att det i den nya förvaltningslagen som träder i kraft den 1 juli 2018 – efter de inledande paragraferna om lagens tillämpningsområde – skulle införas en rubrik kallad *Grunderna för god förvaltning.* Riksdagen beslutade i enlighet med regeringens förslag och bestämmelserna om legalitet, objektivitet och proportionalitet, service, tillgänglighet och samverkan i den nya förvaltningslagen lyder därmed på följande sätt:

> En myndighet får endast vidta åtgärder som har stöd i rättsordningen. I sin verksamhet ska myndigheten vara saklig och opartisk. Myndigheten får ingripa i ett enskilt intresse endast om åtgärden kan antas leda till det avsedda resultatet. Åtgärden får aldrig vara mer långtgående än vad som behövs och får vidtas endast om det avsedda resultatet står i rimligt förhållande till de olägenheter som kan antas uppstå för den som åtgärden riktas mot.[39]

Som skäl för sitt förslag angav regeringen att legalitetsprincipen brukar framhållas som ett skydd mot en nyckfull och godtycklig maktutövning från det allmännas sida. Den är en av de principer som anses kännetecknа en rättsstat. I EU:s rättssystem liksom i Europakonventionen tillskrivs denna princip en avgörande betydelse.

---

[37] 12 kap. 4 § regeringsformen (1974:152).
[38] Prop. 2009/10:224, Ett sammanhängande system för geografisk miljöinformation, s. 28.
[39] 5 § Grunderna för god förvaltning, Legalitet, objektivitet och proportionalitet, förvaltningslagen (2017:900).

Enligt regeringen är inte legalitetsprincipen enhetligt definierad men den brukar vanligtvis uppfattas som ett krav på att ingripanden mot enskilda ska ha ett klart författningsstöd. I denna betydelse är också legalitetsprincipen grundlagsfäst genom regeringsformens bestämmelse att ”den offentliga makten utövas under lagarna”. Med uttrycket lagarna som används i regeringsformen avses i detta sammanhang inte endast sådana lagar som riksdagen har beslutat utan även andra författningar och t.ex. sedvanerätt.

Legalitetsprincipen innebär alltså att myndigheternas maktutövning i vidsträckt mening måste ha stöd i någon av de källor som tillsammans bildar rättsordningen. Utan stöd i lag saknar varje myndighet befogenheter gentemot medborgarna.

Principen bör, enligt regeringen, gälla för all verksamhet hos myndigheten. Med det menas att den bör gälla för såväl handläggning av och beslutsfattande i enskilda ärenden som s.k. faktiskt handlande. Avsikten är att hindra myndigheterna att agera helt vid sidan av sina i författning fastställda förpliktelser.

Av den sjätte paragrafen – service – i den nya förvaltningslagen framgår att en myndighet ska se till att kontakterna med enskilda blir smidiga och enkla. Myndigheten ska lämna den enskilde sådan hjälp att han eller hon kan ta till vara sina intressen. Hjälpen ska ges i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet. Den ska ges utan onödigt dröjsmål.[40]

Den sjunde paragrafen innehåller en bestämmelse om tillgänglighet och innebär att en myndighet ska vara tillgänglig för kontakter med enskilda och informera allmänheten om hur och när sådana kan tas.[41]

6.5 Styrmedel

Valet av styrmedel och kombinationen av dessa är avgörande för resultatet. Riksdagen och regeringen använder flera olika styrmedel för att styra de offentliga myndigheterna. Vissa av dessa styrmedel såsom lagar, förordningar, uppdrag, finansiering, budgetmedel m.fl. är bindande för myndigheterna.

[40] 6 § förvaltningslagen (2017:900).
[41] 7 § förvaltningslagen (2017:900).

Regeringen använder även flera icke bindande styrmedel såsom nationella inriktningsdokument, handlingsplaner, överenskommelser m.fl. för att uttrycka sina ambitioner och önskad inriktning av olika frågor, politikområden m.m.

Mål kan vara bindande styrmedel eller icke bindande styrmedel. Om ett mål är bindande eller inte handlar inte om hur målet i sig är utformat. Det är den styrande som bestämmer om målet ska vara bindande för styrobjektet eller inte. Dock gäller att om målet ska vara bindande måste det kopplas ihop med det eller de objekt som ska styras.

6.5.1 Bindande styrmedel

Av regeringsformen framgår att bestämmelser *ska* meddelas av riksdagen genom lag om de avser

- enskildas personliga ställning och deras personliga och ekonomiska förhållanden inbördes,
- förhållandet mellan enskilda och det allmänna under förutsättning att föreskrifterna gäller skyldigheter för enskilda eller i övrigt avser ingrepp i enskildas personliga eller ekonomiska förhållanden,
- grunderna för kommunernas och landstingens organisation och verksamhetsformer och för den kommunala beskattningen samt
- kommunernas och landstingens befogenheter i övrigt och deras åligganden, m.m.[42]

Riksdagen kan bemyndiga regeringen att meddela föreskrifter enligt regeringsformens 8 kap. 3–5 §§. Därutöver får regeringen meddela föreskrifter om verkställighet av lag. Regeringen får även meddela förordning som inte enligt grundlag ska meddelas av riksdagen. Sådana förordningar får dock inte avse den kommunala beskattningen.[43]

En *föreskrift* är en bindande rättsregel som beslutas av en myndighet och utgår från en lag som beslutats av riksdagen eller en förord-

[42] 8 kap. 2 § regeringsformen (1974:152).
[43] 8 kap. 7 § regeringsformen (1974:152).

ning som beslutats av regeringen.[44] I vissa fall bygger föreskrifter också på EU-rätten. Av lagen eller förordningen ska det tydligt framgå att myndigheten har ett bemyndigande att utfärda föreskrifter, dvs. en rätt att besluta om och utfärda föreskrifter inom ett visst område.

En statlig myndighets roll och uppgifter regleras i myndighetens *instruktion* som beslutas av regeringen i form av en förordning. Instruktionen innehåller inte en uttömmande beskrivning av en myndighets uppgifter utan dessa anges på ett övergripande plan. I instruktionen bör myndighetens ansvarsområde, uppgifter, ledningsform och andra för myndigheten specifika förhållanden regleras.

Finansiering och finansiell styrning

I regeringsformens nionde kapitel behandlas riksdagens finansmakt. Finansmakten är rätten att bestämma över statens inkomster och förfoga över statens tillgångar, framför allt genom beslut om utgifter. Riksdagen beslutar om en beräkning av statens inkomster och om anslag för bestämda ändamål till ett bestämt belopp. Anslag och inkomster får inte användas på annat sätt än vad riksdagen har bestämt.

Det är regeringen som inom ramen för riksdagens beslut förvaltar och förfogar över statens tillgångar, om de inte avser riksdagens myndigheter eller i lag har avsatts till särskild förvaltning.

Ytterligare bestämmelser om riksdagens, regeringens och de statliga myndigheternas befogenheter och skyldigheter i fråga om finansiering av verksamheterna finns i riksdagsordningen eller i särskild lag och förordning.[45]

Kommunernas beskattningsrätt

Av regeringsformens fjortonde kapitel framgår att kommunerna får ta ut skatt för skötseln av sina angelägenheter och att riksdagen, i lag, får besluta att kommuner och landsting ska bidra till kostnaden för

[44] 8 kap. 1 § regeringsformen (1974:152).
[45] 9 kap. regeringsformen (1974:152).

andra kommuners angelägenheter, om det krävs för att uppnå likvärdiga ekonomiska förutsättningar.[46]

Ytterligare regler om kommunernas befogenheter och skyldigheter i fråga om ekonomisk förvaltning finns i kommunallagen.[47]

6.5.2 Icke bindande styrmedel

> Där staten har viljan att styra, men möjligheterna att styra med hjälp av mer detaljerad reglering är begränsade, kan vi förvänta oss ett mer frekvent användande av andra styrmedel än reglering.
>
> Annan styrning kan också vara ett första steg: ett försök att åstadkomma den förändring eller utveckling som statsmakterna önskar, utan att de ska behöva använda sig av ett starkare styrmedel som reglering. Riksdag och regering har också att ta hänsyn till den grundlagsreglerade kommunala självstyrelsen och vill helst undvika att inkräkta på den genom reglering. Visar det sig emellertid att den frivilliga vägen genom annan styrning inte fungerar tillfredsställande utifrån statsmakternas perspektiv, t.ex. att de förändringar man vill åstadkomma uppfattas går för långsamt, har riksdag och regering möjlighet att ta till lagstiftning för att nå sitt mål. /---/
>
> Det kan också finnas politiskt strategiska motiv för riksdag och regering att använda sig av annan styrning. Genom att t.ex. tillsätta en nationell samordnare tydliggör statsmakterna att en viss verksamhet är viktig. Man markerar att man tar en uppkommen situation eller ett politiskt problem på allvar. Genom att involvera fler aktörer i hanteringen av frågan t.ex. genom en överenskommelse med SKL, kan också statsmakternas handlande ges ökad legitimitet. Här finns det dock betydande skillnader mellan olika verksamhetsområden när det gäller hur regeringen väljer att använda sig av annan styrning.[48]

Det som benämns annan styrning i citatet ovan är icke bindande styrmedel. Enligt Statskontoret är olika typer av *nationella inriktningsdokument* ett sätt för regeringen att uttrycka sina mål och ambitioner inom ett område. Nationella *strategier, handlingsplaner och handlingsprogram* är exempel på nationella inriktningsdokument. Syftet med styrning med nationella inriktningsdokument är, enligt Statskontoret, att övergripande påverka utvecklingen inom ett område. Det kan även vara fråga om att regeringen vill få draghjälp från aktö-

[46] 14 kap. 4 och 5 §§ regeringsformen (1974:152).
[47] 11 kap. Ekonomisk förvaltning, Kommunallagen (2017:725).
[48] Statskontoret 2011:22, Tänk efter före, Om viss styrning av kommuner och landsting, s. 28 f.

rer som regeringen har begränsad eller ingen formell möjlighet att styra. Det kan också vara ett sätt att kraftsamla olika aktörer till en viss fråga för att på så sätt stärka samordningen.

Med några undantag är nationella inriktningsdokument normalt sett inte juridiskt bindande. Undantagen är nationella handlingsplaner som följer den gemensamma lagstiftningen inom EU.[49]

Exempel på strategier är Med medborgaren i centrum – regeringens strategi för en digital samverkande statsförvaltning,[50] som regeringen beslutade 2012. Ett annat exempel är strategin För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi[51] som regeringen beslutade den 18 maj 2017.

Överenskommelser är en uppgörelse mellan två parter t.ex. regeringen och SKL, som tillsammans förbinder sig att åstadkomma något. Överenskommelserna är inte formellt bindande *och de parter som ingår i överenskommelsen har inte ansvaret för det direkta genomförandet.* Därför blir det svårt att utkräva något formellt ansvar om en överenskommelse bryts.

Statskontoret beskriver överenskommelser som ”ett paket av olika styrmedel” och menar att överenskommelser är ett sätt för regeringen att sätta fokus på en fråga eller ange en gemensam inriktning för en fråga eller ett ansvarsområde. Överenskommelser innehåller ofta flera andra styrmedel t.ex. statsbidrag, informationsinsatser och uppföljning.[52]

Som ett exempel på överenskommelse kan nämnas att regeringen i januari 2017 ingick en överenskommelse med SKL om en handlingsplan för samverkan vid genomförande av Vision e-hälsa 2025[53] för att skapa bättre förutsättningar för fortsatt digitalisering av vård och omsorg och genomförandet av visionen. Handlingsplanen fastslår bl.a. att en gemensam styr- och samverkansorganisation ska användas.[54]

[49] Statskontoret 2016:24, Statens styrning av kommunerna.
[50] Dnr N2012/06402/ITP.
[51] Dnr N2017/03643/D.
[52] Statskontoret 2014, Om offentlig sektor, Överenskommelser som styrmedel.
[53] S2016/01874/FS.
[54] Prop. 2017/18:1, utgiftsområde 2, s. 94.

6.6 Effektivitet och god hushållning

Den offentliga förvaltningens användning av digitala medel ska leda till ökad kvalitet och effektivitet i den offentliga förvaltningen som helhet.

> Den offentliga förvaltningen och domstolarna utgör en betydande maktapparat. Ett grundläggande krav är att myndigheterna ska tjäna medborgarna, inte tvärtom. Den grundläggande demokratiska principen om att det är folket som är uppdragsgivare ställer krav på effektivitet och hushållning med statens finanser. Denna utgångspunkt ställer dock även krav på bl.a. myndigheternas kontakt med allmänheten. Kraven på effektivitet kan lätt gå ut över servicen till allmänheten, vilken kan vara både tids- och arbetskrävande. Det är viktigt att den enskilde statsanställde utifrån värdegrunden kan hantera denna konflikt. Vidare måste den statligt anställde beakta att legalitetsprincipen alltid är överordnad effektiviteten. Nyckelord för den statsanställde är lättillgänglighet, skyldighet att informera och underlätta samt måluppfyllelse.[55]

Av utredningens direktiv framgår att ytterligare effektivitetsvinster bör kunna göras genom fler innovativa lösningar i offentlig tjänsteproduktion och att det finns en stor effektiviseringspotential att ta till vara med hjälp av tekniken. Även Digitaliseringskommissionen konstaterade i sitt betänkande 2015 att digitaliseringen ändrar förutsättningarna för de offentligt finansierade verksamheterna genom att den erbjuder stora möjligheter till effektivisering och rationalisering och samtidigt högre kvalitet för individen i de tjänster som tillhandahålls.[56]

Enligt kommunallagen är kommuner och landsting skyldiga att ha en god ekonomisk hushållning i sin verksamhet och i sådan verksamhet som bedrivs genom andra juridiska personer.[57]

Enligt regeringen har kommuner och landsting stora möjligheter att själva fatta de beslut som behövs för att den egna verksamheten ska bedrivas kostnadseffektivt och med hög kvalitet. Staten har dock, enligt regeringen, ett övergripande ansvar för att samtliga kommuner och landsting har förutsättningar och kapacitet att hantera dessa frågor. Bland annat genom att förbättra ramverket för och styrningen av

[55] Värdegrundsdelegationen 2013, Den gemensamma värdegrunden för de statsanställda s. 25.
[56] SOU 2015:91, Digitaliseringens transformerande kraft, betänkande av Digitaliseringskommissionen.
[57] Kommunallagen (2017:725).

kommunsektorn arbetar regeringen, enligt vad som framgår av budgetpropositionen för 2018, aktivt med detta inom olika områden.[58]

Mål för den ekonomiska förvaltningen är att kommuner och landsting ska ha en god ekonomisk hushållning i sin verksamhet och i sådan verksamhet som bedrivs genom kommunala bolag, stiftelser, föreningar och privata utförare. Fullmäktige ska besluta om riktlinjer för god ekonomisk hushållning för kommunen eller landstinget.

Av budgeten ska det vidare framgå hur verksamheten ska finansieras och hur den ekonomiska ställningen beräknas vara vid budgetårets slut. De finansiella mål som är av betydelse för en god ekonomisk hushållning ska anges.

Budgeten ska även innehålla en plan för verksamheten under budgetåret. I planen ska det anges mål och riktlinjer som är av betydelse för en god ekonomisk hushållning. Budgeten ska även innehålla en plan för ekonomin för en period av tre år. Om fullmäktige beslutar om en utgift under löpande budgetår, ska beslutet även innefatta en anvisning om hur utgiften ska finansieras.

Både budgetlagen[59] och myndighetsförordningen[60] ger uttryck för statsmakternas viljeinriktning eller ambition för hur regeringen och myndigheterna under regeringen ska använda pengarna när de bedriver sina verksamheter. I budgetlagen, som i första hand reglerar regeringens skyldigheter och befogenheter på finansmaktens område, reglerar riksdagen att i statens verksamhet ska hög effektivitet eftersträvas och god hushållning iakttas.

Den tidigare budgetlagsutredningen[61] ansåg att kravet på hög effektivitet och god hushållning är grundläggande i statens verksamhet. Hög effektivitet innebär att den statliga verksamheten ska bedrivas så att av riksdagen avsedda mål nås i så hög grad som möjligt inom ramen för tillgängliga resurser. Verksamheten kan då sägas vara ändamålsenligt utformad.

Uttrycket god hushållning har en annan och snävare innebörd och innebär att onödiga utgifter ska undvikas, att verksamheten ska bedrivas med hög produktivitet, att statens medel ska hanteras säkert samt att statens tillgångar i övrigt och skulder ska förvaltas väl.[62]

[58] Prop. 2017/18:1, utgiftsområde 25, s. 24.
[59] 1 kap. 3 § budgetlagen (2011:203).
[60] 3 § Myndighetsförordningen (2007:515).
[61] SOU 1996:14.
[62] Prop. 1995/96:220 s. 19 f., prop. 2010/11:40, s. 124.

Uttrycket eftersträvas (hög effektivitet ska eftersträvas) ville den tidigare budgetlagsutredningen använda för att markera att effektivitet inte kan nås i absolut bemärkelse. Uppgiften var i stället att successivt och målmedvetet vidta åtgärder som gör att effektiviteten och ändamålsenligheten i verksamheten förbättras. Dock kan kraven på god hushållning sägas vara något mer absoluta än kraven på effektivitet.

Av myndighetsförordningen framgår att myndighetens ledning har ansvar för att myndighetens verksamhet bedrivs effektivt och att den hushållar väl med statens medel.[63] Statsförvaltningen ska utnyttja skattemedel ändamålsenligt och inte använda mer resurser än vad som krävs för att uppnå avsedda resultat med rätt kvalitet. Varje myndighet ska sträva efter hög effektivitet men ska samtidigt beakta statens samlade effektivitet. Statsförvaltningen ska ha en väl utvecklad kvalitet, service och tillgänglighet och därigenom bidra till Sveriges utveckling och ett effektivt EU-arbete. Myndigheterna ska ge varandra hjälp inom ramen för den egna verksamheten, verka för att genom samarbete med myndigheter och andra ta tillvara de fördelar som kan vinnas för enskilda samt för staten som helhet.[64]

Enligt förordningen om statliga myndigheters elektroniska informationsutbyte[65] ska en myndighet i sin verksamhet främja utvecklingen av ett säkert och effektivt elektroniskt informationsutbyte inom den offentliga förvaltningen.

6.6.1 Förvaltningsövergripande kostnadseffektivitet och förvaltningsgemensamma resurser i en samverkande förvaltning

Utredningen bedömer:
att en effektiv finansiell styrning och finansiering av förvaltningsgemensamma digitala funktioner innebär att riksdagen och regeringen måste styra resurserna utifrån ett förvaltningsövergripande perspektiv.

[63] 3 § myndighetsförordningen (2007:515).
[64] Budgetlagen (2011:203), förvaltningslagen (1986:223), myndighetsförordningen (2007:515), prop. 2009/10:175, bet. 2009/10:FiU38, rskr. 2009/10:315.
[65] 2 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

att kraven på kvalitet och effektivitet i de förvaltningsgemensamma digitala funktionerna måste tillgodoses och bedömas på en förvaltningsövergripande nivå.

> En aspekt som skulle behöva belysas ytterligare är finansieringsfrågan vid utveckling av lösningar som är gemensamma för flera myndigheter. Effektiviserings- och resultatkrav på varje enskild myndighet riskerar att leda till att initiativ inte kommer till stånd när kostnaden uppstår i en myndighet och nyttan uppkommer i en annan, oavsett nyttan för samhället i stort eller för den enskilda medborgaren.[66]

Av beskrivningen ovan framgår att riksdagens och regeringens bestämmelser om hushållning och effektiv hantering av skattebetalarnas pengar riktar sig till respektive offentlig myndighet, inte till förvaltningen som helhet. Undantaget är den sjätte paragrafen i myndighetsförordningen som anger att myndigheten ska lyfta blicken från enbart den egna verksamheten och *verka för att genom samarbete med andra myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet*.[67]

I budgetpropositionen för 2015 sade regeringen att arbetet med att modernisera och effektivisera den offentliga sektorn för att ge bättre service åt medborgarna till en lägre kostnad är viktigt och att en ökad samordning och digital samverkan över myndighetsgränserna har en stor utvecklingspotential i den offentliga förvaltningen. Bristande samverkan mellan myndigheter skapar inte bara problem för enskilda medborgare och företagare som kommer i kontakt med det offentliga. Det kan även medföra onödiga kostnader för staten.[68]

Statens servicecenter är ett exempel på statliga förvaltningsgemensamma resurser, dvs. resurser som är tillgängliga för alla myndigheter i statsförvaltningen. Statens servicecenter[69] har till uppgift att efter överenskommelse med myndigheter under regeringen *mot avgift* tillhandahålla tjänster som gäller administrativt stöd åt myndigheterna.

E-legitimationsnämnden och Skatteverkets förvaltning av Mina meddelanden är däremot numera direkt *anslagsfinansierade*. År 2017

[66] Polismyndighetens remissvar 2017-06-27, A 137.630/2017 över delbetänkandet SOU 2017:23, s. 3.
[67] 6 § myndighetsförordningen (2007:515).
[68] Prop. 2014/15:1, utgiftsområde 22, s. 148.
[69] Förordningen (2012:208) med instruktion för Statens servicecenter.

infördes även ett avgiftsfritt utbyte av grunddata mellan statliga myndigheter.

De grunddata som omfattas av utbytet är uppgifter i folkbokföringsregistret, näringslivsregistret, vägtrafikregistret, fastighetsregistret och viss geografisk information. Fram till och med 2016 har de registeransvariga myndigheterna fakturerat andra myndigheter för efterfrågade uppgifter. Regeringen bedömde dock att denna ordning är ineffektiv i att ett avgiftsuttag mellan myndigheter ökar de administrativa kostnaderna och bidrar till att myndigheter använder mellanhänder, med risk för sämre registerkvalitet. De anslag som finansierar Mina meddelanden, E-legitimationsnämnden och det avgiftsfria grunddatautbytet enligt ovan har finansierats genom en omfördelning av medel mellan statliga myndigheter. De alternativ till finansiering av förvaltningsgemensamma digitala funktioner är, enligt utredningens bedömning, avgifter och/eller anslag.

Avgiftsfinansiering i statlig verksamhet anses ha två huvudsakliga syften, nämligen att ersätta annan finansieringskälla eller att påverka efterfrågan på varan eller tjänsten. Ett av de vanligaste argumenten för att införa en avgift är att det anses vara rimligt att den som utnyttjar en verksamhet också betalar för den. En avgift kan öka kostnadsmedvetandet hos både producent och konsument och höja produktiviteten. En avgift kan öka varans eller tjänstens värde för konsumenten.

Inomstatliga avgifter tas ut mellan statliga myndigheter. Intäkterna från avgifterna som betalas mellan myndigheter har inte någon statsfinansiell effekt. Avgiftsfinansiering av en vara eller tjänst som enbart berör olika myndigheter är alltså fråga om interndebiteringar eller en metod att omfördela resurser inom staten. Det innebär i princip att de varor och tjänster som produceras hos en myndighet avgiftsfinansieras och att anslagsmedel i stället anvisas och tilldelas den myndighet som köper och använder tjänsten eller varan.[70]

ESV har konstaterat att i många fall är ett avgiftsfritt utlämnande mer kostnadseffektivt både för myndigheten och för användarna eftersom avgiftsuttag i sig medför en kostnad.[71] Med det menas att med avgiftsfinansiering följer även administration av avgiftshanteringen och de administrativa kostnaderna för att ta ut avgiften kan bli så höga att det inte lönar sig att ta ut någon avgift.

[70] ESV 2009:39, Förslag till utvecklad finansiell styrning.
[71] ESV 2015:63, Avgiftsförordningen och PSI-lagen.

Argument som talar emot avgiftsfinansiering är att den kan leda till en oönskad minskning av efterfrågan av tjänsten. En avgift kan även innebära att syftet med verksamheten inte uppnås eftersom det ligger i samhällets eller statsmakternas intresse att så många som möjligt får ta del av tjänsten. Enligt utredningens bedömning är avgiftsfinansiering av förvaltningsgemensamma digitala funktioner en vare sig tillräckligt förutsägbar, stabil eller långsiktig finansieringsform för att funktionerna, på ett effektivt sätt, ska kunna leverera de förväntade resultaten.

Digitaliseringsmyndigheten som utredningen föreslog i sitt delbetänkande är tänkt att vara en förvaltningsgemensam resurs för hela den offentliga sektorn. I förslaget ingår att digitaliseringsmyndigheten ska vara anslagsfinansierad och att myndighetens tjänster ska vara kostnadsfria för de offentliga myndigheterna.[72] Utredningen argumenterade att finansieringen av digitaliseringsmyndighetens samlade ansvar bör ge myndigheten långsiktiga och stabila förutsättningar att stödja förvaltningens utveckling och öka den samverkan inom hela den offentliga förvaltningen som riksdagen och regeringen vill uppnå. Utredningen föreslog därför att samtliga uppgifter i samordningsuppdraget ska finansieras med anslagsmedel.

I budgetpropositionen för 2018 föreslog regeringen att riksdagen skulle besluta om att anvisa ett förvaltningsanslag för digitaliseringsmyndigheten. Ändamålet med anslaget skulle vara att anslaget får användas för digitaliseringsmyndighetens förvaltningsutgifter. Anslaget får användas för utgifter för styrning, samordning och uppföljning av digitaliseringen av den offentliga förvaltningen samt för den nationella digitala infrastrukturen. Anslaget får användas för utgifter för E-legitimationsnämndens verksamhet i den mån den inte finansieras med avgifter samt för andra förvaltningsgemensamma tjänster och funktioner. Riksdagen beslutade enligt regeringens förslag.[73]

Utredningen noterar att det av regeringens direktiv till den särskilda utredare som ska inrätta digitaliseringsmyndigheten framgår att utredaren får lämna förslag på verksamhet som kan bli föremål för avgifter.[74] Den avgiftsbelagda verksamheten ska ha målet full kost-

[72] Anslagsfinansieringen som enligt förslaget ska föras över från E-legitimationsnämnden avsåg E-legitimationsnämndens verksamhet och E-legitimationsnämndens ansvar för federationstjänsterna.
[73] Prop. 2017/18:1, utgiftsområde 2, bet. 2017/18:FiU2, rskr. 2017/18:128 och 129.
[74] Dir. 2017:117, Inrättande av en myndighet för digitalisering av den offentliga sektorn.

nadstäckning och får inte gynna eller missgynna vissa användare. Av direktiven framgår inte om det är fråga om avgifter för frivillig uppdragsverksamhet eller om det är fråga om offentligrättsliga avgifter.

ESV har framhållit att det finns ett behov av att ta fram en långsiktigt hållbar finansieringsmodell som tar sikte på att öka den samverkan mellan de statliga myndigheterna som riksdagen och regeringen vill uppnå för att främja den digitala förvaltningen. ESV menar att finansiell styrning med anslag kan öka denna samverkan.[75]

Bestämmelserna om finansiell styrning med anslag innebär dessutom att verksamheten blir mer transparent, att finansieringsbesluten måste bli föremål för noggrann budgetberedning och beslut i hela styrkedjan och att det finns möjligheter för statsmakterna att utöva ett yttre effektiviseringstryck på verksamheterna.

Avseende avgiftsfinansiering myndigheter emellan, dvs. avgifter för frivillig uppdragsverksamhet, har utredningen inte någon annan uppfattning än ESV i denna fråga utan menar att anslagsfinansiering av förvaltningsgemensamma digitala funktioner är den bättre och mer effektiva finansieringslösningen för alla inblandade aktörer.

Utredningen menar att avgiftsfinansiering offentliga myndigheter emellan kan verka hämmande för den önskade utvecklingen och förvaltningen av förvaltningsgemensamma digitala funktioner som riksdagen och regeringen eftersträvar. Avgiftsfinansiering riskerar att verksamheten inte utförs på ett effektivt sätt för staten som helhet utan kan till och med innebära att myndigheter som har behov av myndighetens avgiftsbelagda tjänster av ekonomiska och andra skäl avstår från dem.

6.7 Närmare om statliga myndigheterna under regeringen

Under regeringen lyder den statliga förvaltningsorganisationen, dvs. Justitiekanslern och andra statliga förvaltningsmyndigheter som inte är myndigheter under riksdagen.[76] Domstolarna ingår i också i den statliga myndighetsorganisationen under regeringen. Domstolarna är dock inte förvaltningsmyndigheter. Till skillnad från kommuner och

[75] Ekonomistyrningsverkets redovisning av uppdraget Finansieringslösningar för gemensamma digitala tjänster 2016-03-01, dnr. 1.1-397/2015.
[76] 12 kap.1 § regeringsformen (1974:152).

landsting ingår de statliga myndigheterna under regeringen i en och samma juridiska person.

Det finns flera olika utgångspunkter för att räkna antalet myndigheter under regeringen. Av Statskontorets redovisning av den offentliga sektorns utveckling framgår att det i januari 2017 fanns 343 statliga myndigheter under regeringen. Dessa myndigheter är förvaltningsmyndigheter och domstolar som lyder under regeringen och som regeringen har utfärdat en förordning med instruktion för, eller som styrs av en särskild lag. I denna grupp myndigheter ingår inte myndigheter med tidsbegränsade uppdrag.[77]

I Arbetsgivarverkets redovisning av antalet myndigheter under regeringen ingår endast myndigheter med egna anställda. År 2017 hade, enligt Arbetsgivarverket, 212 myndigheter under regeringen egna anställda.

ESV i sin tur redovisar antalet myndigheter som ingår det i den statliga redovisningsorganisationen. Av redovisningen som uppdateras löpande framgår att det i november 2017 ingick 218 statliga myndigheter i den statliga redovisningsorganisationen. Av dessa var 215 myndigheter som lyder under regeringen.[78] Förteckningen innehåller uppgifter om myndighetsidentitet, organisationsnummer, departementstillhörighet, årsredovisningsskyldighet och om tillstånd att rekvirera ingående mervärdeskatt.

Även Statistiska centralbyrån för ett register över statliga myndigheter – det allmänna myndighetsregistret. Sammantaget omfattade myndighetsregistret 458 myndigheter i januari 2018.[79]

Statistiska centralbyråns uppdrag att föra registret framgår av förordningen om det allmänna förordningsregistret.[80] Enligt förordningen ska registret innehålla uppgifter om domstolar, affärsverk och övriga förvaltningsmyndigheter samt myndigheterna i utrikesrepresentationen.[81]

---

[77] Statskontoret 2017, Den offentliga sektorn i korthet 2017, dnr 2017/20-5. För närmare beskrivning av Statskontorets definition se Statskontoret (2005:32), Statsförvaltningens utveckling 1990–2005.

[78] ESV webbplats 2017-11-18. ESV redovisar samtliga 218 statliga myndigheter i den statliga redovisningsorganisationen inklusive Riksrevisionen, Riksdagens ombudsmän, JO samt Kungliga Hov- och Slottsstaten. Utredningen redovisar här dock enbart antalet myndigheter i den statliga redovisningsorganisationen som lyder under regeringen, dvs. 218-3=215.

[79] www. scb.se 2018-01-02.

[80] Förordningen (2007:755) om det allmänna myndighetsregistret.

[81] 1 § förordningen (2007:755) om det allmänna myndighetsregistret.

6.7.1 Regeringen väljer hur mycket den vill styra sina myndigheter

Enligt regeringen är myndigheternas fristående ställning och långtgående befogenheter att besluta om *hur* de egna uppgifterna ska lösas viktiga i den svenska förvaltningen och medför många fördelar. Den lägger också grunden till att myndigheterna på ett självständigt sätt ska kunna sköta sin dagliga verksamhet effektivt och rättssäkert. Den svenska förvaltningsmodellen är en förutsättning för en effektiv och utvecklingsinriktad statsförvaltning. Regeringen har samtidigt betonat att det är lika viktigt att varje myndighet, samtidigt som den har långtgående befogenheter att bestämma hur den organiserar sitt arbete, är en del av staten som helhet. Det är därför viktigt med en väl fungerande samordning och samverkan mellan myndigheterna.[82]

Varje regering väljer hur mycket den vill styra sina myndigheter. Förvaltningskommittén uttryckte det på följande sätt:

> /---/ frågan om hur mycket regeringen vill styra en enskild myndighet varierar mellan en regering och en annan, från myndighet till myndighet, från verksamhet till verksamhet och från en tid till en annan.[83]

Även om en stor del av de statliga myndigheternas verksamhet, m.m. regleras av riksdagen i olika lagar har myndigheterna under regeringen en lydnadsrelation till regeringen men inte direkt till riksdagen eller medborgarna, och inte heller till ett enskilt statsråd. Riksdagen och regeringen styr de statliga myndigheterna huvudsakligen genom författningar – riksdagen genom lagar och budgetbeslut och regeringen genom förordningar och budgetreglering. Dessa lagar och förordningar kan vara generella eller specifika. Det generella regelverket består bl.a. av förvaltningslagen, myndighetsförordningen och förordningen om budgetunderlag och årsredovisning.[84]

Alla statliga myndigheter under regeringen ska – som regel – ha en instruktion. Instruktionen är en förordning som regeringen beslutar med stöd av den s.k. restkompetensen, dvs. sådan normgivning som inte tillkommer riksdagen genom grundlag. En myndighets instruktion är oftast myndighetsspecifik men kan även vara

[82] Skr. 2013/14:155, bet. 2013/14:FiU37, rskr. 2013/14:300.
[83] SOU 2007:75, Att styra staten – regeringens styrning av sin förvaltning, betänkande av Styrutredningen, s. 45 f.
[84] Förvaltningslagen (2017:900), myndighetsförordningen (2007:515), förordningen (2000:605) om budgetunderlag och årsredovisning.

gemensam för flera myndigheter med liknande verksamhet, eller för flera myndigheter inom samma förvaltningsområde.

Gemensamma instruktioner finns för bl.a. länsstyrelserna och olika typer av domstolar såsom tingsrätter, förvaltningsrätter m.fl.

Med instruktionen bestämmer regeringen en myndighets uppgifter, ledningsform och andra förhållanden som är specifika för myndigheten.

Regeringen brukar varje år – i budgetpropositionen – redovisa sina utgångspunkter och ambitioner för sin styrning av sina myndigheter. Så även i budgetpropositionen för 2018 där regeringen framhöll att enskildas, organisationers och företags behov och förväntningar är en utgångspunkt för den offentliga förvaltningen.

Regeringen anförde att

> dagens snabba samhällsutveckling innebär att den offentliga sektorn måste vara både förutsebar och anpassningsbar. Det ställer höga krav på en mer sammanhållen styrning på flera nivåer. Regeringen vill värna och utveckla den svenska förvaltningsmodellen, med en stor tillit och ett långtgående delegerat ansvar till de statliga myndigheterna. Styrningen ska därför vara långsiktig, strategisk, verksamhetsanpassad och utgå från ett helhetsperspektiv, med tillit och förtroende som grund. Med tillitsbaserad styrning avser regeringen en styrning som både tydliggör vad som ska uppnås och ger ett så stort handlingsutrymme som situationen tillåter för den som ska utföra verksamheten. En tillitsbaserad styrning omfattar även en uppföljning och efterhandskontroll, som både ger tillräckliga underlag för fortsatt styrning och upplevs vara meningsfull och legitim av den som ska kontrolleras.
>
> /---/
>
> Behovet av samordning har i flera fall ökat och styrningen behöver i en del fall bli mer sammanhållen, t.ex. genom att utgå från verksamhetsområden snarare än enskilda myndigheter. Lokalisering och digitalisering är exempel på områden där ett helhetsperspektiv medför fördelar för staten som helhet, vilket också avspeglas i regeringens styrning.
>
> Medborgarnas förtroende för det allmänna är även fortsättningsvis en grundläggande förutsättning för den statliga förvaltningen och dess förmåga att möta förändringar.[85]

Ansvaret för den enskilda myndighetens *interna* organisation är i regel delegerat till myndighetens ledning. Regeringen har dock det övergripande ansvaret för att den statliga förvaltningen bedrivs rätts-

[85] Prop. 2017/18:1, utgiftsområde 2, 5 Statlig förvaltningspolitik, s. 86.

säkert och effektivt och att myndigheterna har en likvärdig service och tillgänglighet för alla medborgare och företag.[86]

6.7.2 Statsförvaltningen – de förvaltningspolitiska utgångspunkterna för regeringens styrning av sina myndigheter

Regeringens förvaltningspolitik som omfattar alla myndigheter under regeringen ska tydliggöra statsförvaltningens särprägel, statens ansvar och uppgifter och uppdraget att tjäna demokratin. Förvaltningspolitiken syftar till en rättssäker och effektiv statsförvaltning och till att utveckla förvaltningen som helhet och dess samlade nytta för medborgare och företag.

Den statliga förvaltningspolitiken innefattar främst frågor och generella principer, oavsett verksamhetsområde. Den statliga förvaltningspolitiken omfattar styrning, ledning, organisation och utveckling av de statliga myndigheterna samt vissa övergripande frågor om relationen mellan stat och kommun, inklusive regional ansvarsfördelning. Kommunerna och landstingen omfattas annars inte av den statliga förvaltningspolitiken. Samtidigt finns det många beröringspunkter mellan den statliga förvaltningen och de kommunala och landstingskommunala förvaltningarna.

Ur ett EU-perspektiv är förvaltningspolitiken huvudsakligen en nationell angelägenhet. Det samarbete som förekommer är, enligt den tidigare regeringen, huvudsakligen frivilligt. Det finns emellertid unionslagstiftning som på olika sätt påverkar hur de nationella myndigheterna arbetar eller är organiserade.[87]

Målet för den statliga förvaltningspolitiken som riksdagen beslutade 2010 är

> En innovativ och samverkande förvaltning som är rättssäker och effektiv, har väl utvecklad kvalitet, service och tillgänglighet och som därigenom bidrar till Sveriges utveckling och ett effektivt EU-arbete.[88]

[86] Prop. 2009/10:175.
[87] Skr. 2013/14:155, bet. 2013/14:FiU37, rskr. 2013/14:300.
[88] Prop. 2009/10:175, bet. 2009/10:FiU38, rskr. 2009/10:315.

6.7.3 Om allmänhetens förtroende

Regeringens förvaltningspolitiska skrivelse till riksdagen i mars 2014 inleds med orden

> En väl fungerande offentlig förvaltning är av avgörande betydelse för medborgarnas välfärd liksom för samhällsekonomin och den ekonomiska tillväxten.[89]

I samma skrivelse framhåller regeringen också betydelsen av att det allmänna har förtroende för de statliga myndigheterna, landstingen och kommunerna. Att den offentliga förvaltningen åtnjuter medborgares och företags förtroende är en förutsättning för att verksamheten ska fungera. Viljan att gemensamt finansiera den offentliga verksamheten förutsätter att medborgare och företag litar på att skattemedel används på ett ansvarsfullt sätt.[90]

Medborgarna ska ha förtroende för den statliga förvaltningen och känna tillit till dem som arbetar där. De anställda måste ha gott omdöme, integritet och goda kunskaper om den lagstiftning som är grunden för statsförvaltningens verksamhet. Det är dock inte tillräckligt att myndigheterna handlar opartiskt, omsorgsfullt och i övrigt korrekt i formell mening. De måste också lämna snabba, enkla och entydiga besked och hjälpa medborgare och företag att utöva sina rättigheter och fullgöra sina skyldigheter.

6.8 Närmare om kommuner och landsting

> Sveriges kommuner har ett brett uppdrag och olika roller av skiftande karaktär. /---/ Den decentraliserade samhällsmodellen ställer höga krav på kommunernas förmåga att hantera de utmaningar som följer av samhällsutvecklingen. Den förutsätter bl.a. att varje enskild kommun tar ansvar för att söka stärka sin kapacitet, förnya verksamheten, öka effektiviteten och utveckla demokratin. Ett tydligt politiskt ledarskap, en väl fungerande organisation, en effektiv styrning och ett starkt lokalt ansvarstagande är avgörande för kommunernas möjlighet att förverkliga de demokrati- och effektivitetsvärden som den kommunala självstyrelsen ska uppnå. Regleringen i RF visar att det finns högt ställda förväntningar på att kommunerna kan utföra sina uppgifter och spela en viktig roll i samhället. Kommunerna förutsätts ha förmåga att ta ett omfattande och

[89] Skr. 2013/14:155, s. 11, bet. 2013/14:FiU37, rskr. 2013/14:300.
[90] Skr. 2013/14:155, s. 11, bet. 2013/14:FiU37, rskr. 2013/14:300.

betydande ansvar för välfärd och lokal samhällsutveckling samt ha goda förutsättningar att möta framtida utmaningar.[91]

Kommuner och landsting har ansvaret för en stor del av den offentliga förvaltningen i Sverige. Varje landsting omfattar ett län om inte något annat är särskilt beslutat. Det finns 290 kommuner och 20 landsting (Gotlands kommun har ett landstingsansvar). Samtliga kommuner följer samma lagstiftning och har i huvudsak samma ansvar och uppgifter. Den enhetliga modellen bidrar till en begriplig och funktionellt utformad samhällsorganisation samt medverkar till en effektiv offentlig förvaltning och en tydlig ansvarsfördelning. Samtidigt finns stora skillnader mellan landets kommuner, vilket påverkar deras möjligheter att hantera sina uppgifter. Kommunerna och landstingen varierar starkt både till befolkning (antalet medlemmar i kommunen) och yta. Antalet invånare i kommunerna varierade 2016 mellan knappt 2 500 invånare i Bjurholms kommun till drygt 936 000 invånare i Stockholms kommun. Av tabellen nedan framgår att majoriteten av alla kommuner har som högst 25 000 invånare.

Tabell 6.1 Antal kommuner efter antal invånare

Antal invånare	Antal kommuner
Upp till 10 000	76
10 001–25 000	110
25 001–75 000	76
Över 75 000	28

Källa: Finansdepartementet, Ds 2017:60, Genomförande av webbtillgänglighetsdirektivet.

Till ytan varierade kommunernas storlek mellan nio kvadratkilometer (Sundbybergs kommun) till drygt 19 000 kvadratkilometer (Kiruna kommun).

Bland landstingen hade 2016 Stockholms läns landsting flest invånare, nästan 2 269 000 och Jämtlands läns landsting det minsta antalet, 129 000 invånare.[92] Som framgår av tabellen nedan är det endast tre landsting som har över 1 miljon invånare.

[91] Dir. 2017:13, Stärkt kapacitet i kommunerna för att möta samhällsutvecklingen.
[92] Skr. 2016/17:102, utvecklingen inom den kommunala sektorn.

Tabell 6.2 Antal landsting efter antal invånare

Antal invånare	Antal landsting
Under 1 000 000	17
Över 1 000 000	3

Källa: Finansdepartementet, Ds 2017:60, Genomförande av webbtillgänglighetsdirektivet.

Kommunernas och landstingens skiftande storlek tillsammans med bland annat skillnader i inkomstförhållanden och ålderssammansättning skapar, trots skatteutjämning och statsbidrag, betydande olikheter i kommunernas förmåga att tillhanda digitala tjänster. Samtidigt är kraven på vad kommunen eller landstinget ska utföra, som framförts ovan, lika. Denna obalans mellan förmåga och krav är en av digitaliseringens största utmaningar.

Kommunerna och landstingen är till skillnad från staten förvaltning genom förtroendevalda. Som framgår ovan är en kommun eller ett landsting en egen juridisk person.

Kommunernas och landstingens ställning, organisation och verksamhet är, förutom i regeringsformen, reglerad i kommunallagen och ett stort antal författningar – speciallagar – med inriktning på särskilda verksamheter samt EU-rätten.

Enligt regeringsformen sköter kommunerna och landstingen lokala och regionala angelägenheter av allmänt intresse på den kommunala självstyrelsens grund. På samma grund sköter kommunerna och landstingen även de övriga angelägenheter som riksdagen har bestämt i lag.[93]

Den kommunala självstyrelsen syftar ytterst till att stärka demokratin och göra den offentliga verksamheten mer effektiv. Staten kan tilldela kommunerna uppgifter och utformar styrningen av deras verksamhet. Statens styrning syftar till att säkerställa dels att kommunerna utför de tilldelade uppgifterna i enlighet med nationellt fastställda mål och krav, dels att den offentliga servicen är likvärdig och rättssäker.[94] Sverige ratificerade 1989 den Europeiska konventionen om kommunalt självstyre.[95]

[93] 14 kap. 2 § regeringsformen (1974:152).
[94] Dir. 2017:13, Stärkt kapacitet i kommunerna för att möta samhällsutvecklingen.
[95] Prop. 1988/89:119, bet. 1988/89:KU32, rskr. 1988/89:251.

Det finns inte någon lagfäst definition av vad som avses med kommunal självstyrelse men principen om kommunal självstyrelse gäller för all kommunal verksamhet, även den som är föremål för särskild reglering. Dock är det möjligt att föreskriva skyldigheter för kommuner och landsting i speciallagstiftning i de fall detta motiveras av vikten av att åstadkomma en reglering som ger likvärdig service för invånarna oberoende av var de är bosatta. En inskränkning i den kommunala självstyrelsen bör, enligt regeringsformen, inte gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett den.[96]

Vid en eventuell inskränkning av det kommunala självstyret måste den så kallade proportionalitetsprincipen beaktas.[97]

Av kommunallagen framgår att kommuner och landsting får ha hand om angelägenheter av allmänt intresse som har anknytning till kommunen eller landstingets område eller deras medlemmar.[98] Däremot får kommuner och landsting inte ha hand om sådana angelägenheter som enbart staten, en annan kommun, ett annat landsting eller någon annan ska ha hand om.[99]

För kommuner och landsting gäller *likställighetsprincipen* som innebär att kommuner och landsting ska behandla sina medlemmar lika, om det inte finns sakliga skäl till något annat.[100]

Många viktiga samhällsfunktioner är *obligatoriska uppgifter* för kommunerna och landstingen. Exempel på obligatoriska uppgifter finns inom t.ex. plan- och byggväsendet, skolväsendet, socialtjänsten samt inom hälso- och sjukvården.[101] Kommunerna och landstingen kan även bedriva *frivillig verksamhet* på t.ex. kultur- och fritidsområdet. De största verksamheterna i kommunerna är utbildning och vård och omsorg. Landstingens dominerande verksamheter är hälso- och sjukvård.[102]

Kommunerna bedriver en stor del av sin verksamhet i egen regi. Kommuner och landsting får driva näringsverksamhet om den drivs

[96] 14 kap. 3 § regeringsformen (1974:152).
[97] Prop. 2009/10:80, bet. 2009/10:KU19, rskr. 2009/10:304.
[98] 2 kap. 1 § kommunallagen (2017:725).
[99] 2 kap. 2 § kommunallagen (2017:725).
[100] 2 kap. 3 § kommunallagen (2017:725).
[101] Se bl.a. Hälso- och sjukvårdslagen (2017:30), Socialtjänstlagen (2001:453), Skollagen (2010:800), Plan- och bygglagen (2010:900).
[102] Skr. 2016/17:102, utvecklingen inom den kommunala sektorn.

utan vinstsyfte och syftar till att tillhandahålla allmännyttiga anläggningar eller tjänster åt medlemmarna.[103]

Kommuner och landsting har även möjlighet att bedriva viss verksamhet i andra juridiska personer som t.ex. aktiebolag. Även verksamheter i sådana juridiska personer omfattas av de kommunala kompetensreglerna. Det innebär att kommuner och landsting, med de begränsningar som framgår av lag, får överlämna skötseln av kommunala angelägenheter till kommunala bolag, stiftelser, föreningar och till privata utförare.[104] Fullmäktige ska för varje mandatperiod anta ett program med mål och riktlinjer för sådana kommunala angelägenheter som utförs av privata utförare. I programmet ska det också fastställas hur fullmäktiges mål och riktlinjer ska följas upp och hur allmänhetens insyn ska tillgodoses.[105]

Med köp av verksamhet avses, utöver upphandlad verksamhet där kommuner och landsting behåller huvudmannaskapet, även bidrag som ges till enskilda huvudmän inom skolväsendet. Köpen görs från föreningar, stiftelser, privata företag och enskilda personer, men även från andra kommuner, landsting, kommunalförbund och i viss utsträckning från staten.

6.8.1 Fullmäktiges och styrelsens uppgifter

I kommuner och landsting är fullmäktige ansvarig för verksamhetens resultat, kvalitet och innehåll. Kommunfullmäktige och landstingsfullmäktige beslutar i ärenden av principiell beskaffenhet eller annars av större vikt för kommunen eller landstinget, främst mål och riktlinjer för verksamheten, budget, skatt och andra viktiga ekonomiska frågor, nämndernas organisation och verksamhetsformer, årsredovisning och ansvarsfrihet m.m.[106]

Fullmäktige prövar varje år om verksamheten är ändamålsenlig och effektiv i nämnder, beredningar, kommunalförbund och finansiella samordningsförbund samt indirekt i kommunala företag.

Styrelsen ska leda och samordna förvaltningen av kommunens eller landstingets angelägenheter och ha uppsikt över övriga nämn-

[103] 2 kap. 7 § kommunallagen (2017:725).
[104] 3 kap. 11–12 §§ och 10 kap. 1–9 §§ kommunallagen (2017:725).
[105] 5 kap. 3 § kommunallagen (2017:725).
[106] 5 kap. 1 § kommunallagen (2017:725).

ders och eventuella gemensamma nämnders verksamhet. Styrelsen ska också ha uppsikt över kommunal verksamhet som bedrivs i bolag, privata utförare, stiftelser och föreningar, dvs. sådana juridiska personer som avses i kommunallagens 10 kap. 2–6 §§ och sådana kommunalförbund som kommunen eller landstinget är medlem i. Styrelsen ska varje år lämna en årsredovisning till fullmäktige.

6.8.2 Kommuner och landsting i statsbudgeten

Kommuner och landsting finansieras till en mindre del av statsbidrag från statsbudgeten. Den huvudsakliga finansieringen av kommunernas verksamheter är kommunernas egna skatteintäkter.

Statsbudgetens bidrag till finansieringen av kommunernas och landstingens verksamheter finns inom ramen för utgiftsområde 25 Allmänna bidrag till kommuner och därutöver inom respektive utgiftsområde som finansierar riktade statsbidrag till kommuner och landsting.

Det av riksdagen beslutade målet för utgiftsområde 25 Allmänna bidrag till kommuner är att skapa goda och likvärdiga ekonomiska förutsättningar för kommuner och landsting som bidrar till en effektiv kommunal verksamhet med hög kvalitet. Målet riktar sig inte till kommunerna och landstingen utan är ett mål för inriktningen och ändamålet med statens generella statsbidrag inom utgiftsområdet.

Statsbidrag

Statsbidrag innebär att en statlig myndighet betalar ut ett bidrag till en annan juridisk person, till exempel en privaträttslig organisation eller kommunal verksamhet.

Statsbidragen till kommuner och landsting består av både generella bidrag och riktade bidrag. Enligt nationalräkenskaperna uppgick statsbidragen till kommuner och landsting 2016 till 185 miljarder kronor. Av beloppet utgjordes 90 miljarder kronor av generella statsbidrag och 96 miljarder kronor av riktade statsbidrag.[107]

[107]Prop. 2017/18:1, utgiftsområde 25.

De generella statsbidragen är anslagsmedel som utbetalas på statsbudgetens utgiftssida från utgiftsområde 25 Allmänna bidrag till kommuner och utgör ett allmänt stöd till kommuner och landsting.

De generella statsbidragen är ett instrument för att bidra till kommunernas och landstingens möjlighet att driva verksamheten utifrån lokala förutsättningar.

Med riktade statsbidrag menas här statsbidrag avsedda för konsumtion från anslag under andra utgiftsområden än utgiftsområde 25. De riktade statsbidragen utbetalas från flera olika utgiftsområden. Till skillnad från de generella statsbidragen är de riktade statsbidragen avgränsade till vissa verksamheter eller prestationer. De kräver i regel någon form av motprestation och återrapportering. Antingen måste de sökas eller så fördelas de enligt en prestationsmodell. De flesta statsbidragen är ensidigt beslutade av staten, men vissa regleras genom överenskommelser mellan staten och SKL.

Enligt Statskontoret kan det finnas flera motiv för statsmakterna att besluta om riktade statsbidrag. Ett motiv har varit att staten har ansett att det finns behov av att öka styrningen av verksamheterna för att nå de nationella målen. I sin analys av statens styrning av kommunal verksamhet underströk Statskontoret att det från flera håll har riktats kritik mot en alltför stor användning av riktade statsbidrag som styrmedel. En del av kritiken handlar om den ökning av administration bidragen i allmänhet skapar, men kritiken handlar också om att de riktade bidragen skapar osäkra förutsättningar för kommuner och landsting att planera sin verksamhet.[108]

[108] Statskontoret 2016:24, Statens styrning av kommunerna.

7 Mål för den offentliga förvaltningens digitaliseringsarbete

Utredningen bedömer:
Digitaliseringen är en av samtidens mest påtagliga omvandlingsprocesser. Den offentliga förvaltningen är en viktig aktör. Statens åtagande i den digitala infrastrukturen är av avgörande betydelse inte bara för medborgarnas välfärd utan även för innovationer och näringslivsutveckling. Det är därför rimligt att digitaliseringsarbetet får en plats i den demokratiska processen för styrning och ansvarsutkrävande. Det bör därför finnas ett av riksdagen beslutat gemensamt mål för den offentliga förvaltningens digitaliseringsarbete. Målet ska vara bindande för regeringen i regeringens styrning av sina myndigheter och i förekommande fall i sin styrning av kommuner och landsting. Målet bör även vara ett riktmärke för riksdagen i riksdagens beslut om bestämmelser för kommuner och landsting.

Utredningen föreslår:
att regeringen ska föreslå riksdagen att för den offentliga förvaltningens digitaliseringsarbete besluta om målet att

Den offentliga förvaltningens användning av digitala medel ska leda till att det blir så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service. Den offentliga förvaltningens användning av digitala medel ska vara säker samt öka kvaliteten och effektiviteten i den offentliga förvaltningen som helhet.

att regeringen för de statliga myndigheternas digitaliseringsarbete beslutar om målet att

Den statliga förvaltningens användning av digitala medel ska leda till att det blir så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av den statliga förvaltningens service. De statliga myndigheternas användning av digitala medel ska vara säker samt öka kvaliteten och effektiviteten i den offentliga förvaltningen som helhet.

Förslaget genomförs genom förordningen med mål för de statliga myndigheternas digitaliseringsarbete.

att digitaliseringsmyndigheten ska stödja regeringens arbete med en samlad analys och bedömning av resultatet av den offentliga sektorns digitaliseringsarbete i förhållande till förslaget till riksdagens mål. Digitaliseringsmyndighetens analys och bedömning av resultatet redovisas i den årliga rapport som utredningen föreslagit.

att regeringen ger digitaliseringsmyndigheten ett särskilt uppdrag att utforma en metod och process för denna uppgift.

7.1 Mål och …

Digitalisering och it inom offentlig förvaltning redovisas i budgetpropositionen för 2018 inom utgiftsområde 2. Området har tidigare redovisats under utgiftsområde 22, Kommunikationer. Området digitalisering och it inom offentlig förvaltning omfattar frågor om digitalisering och it inom den offentliga förvaltningen, digital mognad, it-användning och it-investeringar i statsförvaltningen, e-handel i staten, elektronisk identifiering och underskrift, förvaltningsgemensam digital infrastruktur, t.ex. plattformar, tjänster, standarder och ramverk, samt vidareutnyttjande av information från den offentliga förvaltningen. Vidare omfattar området myndighetsstyrning av E-legitimationsnämnden.

Att området digitalisering och it inom offentlig förvaltning flyttats från utgiftsområdet 22 till utgiftsområde 2 innebär att dessa frågor inte längre omfattas av det – inom utgiftsområde 22 – riksdagsbundna målet för digitaliseringspolitiken, dvs. det mål som tidigare benämndes målet för it-politiken. Målet för digitaliseringspolitiken är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.

Inom utgiftsområde 2 Samhällsekonomi och finansförvaltning finns i dag två riksdagsbundna mål. Dessa är dels målet för finansmarknaden, dels målet för den statliga förvaltningspolitiken.

Området digitalisering inom den offentliga sektorn ingår inte i något av de delområden som dessa mål omfattar. Enligt vad som framgår av budgetpropositionen för 2018 betyder det att det inte längre finns något av riksdagen beslutat mål för området digitalisering inom den offentliga sektorn. Regeringen lämnade i budgetpropositionen för 2018 inte heller något förslag till mål för området för riksdagen att besluta om.

I budgetpropositionen för 2018, liksom i budgetpropositionen för 2017 informerade dock regeringen riksdagen om det mål som regeringen beslutat för detta delområde. Regeringens mål är *en enklare vardag för medborgare, en öppnare förvaltning som stödjer innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten.*

Regeringen bedömde att ”digitalt” ska vara förstahandsval i den offentliga förvaltningens verksamhet och i kontakter med privatpersoner och företag. Digitalt först innebär, enligt regeringen, att den offentliga förvaltningen, när det är lämpligt, ska välja digitala lösningar vid utformningen av sin verksamhet. Samtidigt ska säkerheten och skyddet för den personliga integriteten säkerställas. Med det i beaktande ska det, enligt regeringen, vara enkelt att komma i kontakt med det offentliga Sverige och uppgifter ska om det är möjligt bara behöva lämnas en gång. Den offentliga förvaltningen ska vara effektiv och samarbeta och när det är lämpligt och om möjligt ska den återanvända information, uppgifter och gemensamma lösningar. Den offentliga förvaltningen ska verka för öppenhet, innovation och delaktighet i digitala lösningar.[1]

Eftersom regeringen i budgetpropositionen endast informerat riksdagen om sitt mål för den digitala offentliga förvaltningen och riksdagen därmed inte beslutat om regeringens mål är detta mål att betrakta som en redovisning av regeringens egna ambitioner för digitaliseringen inom den offentliga sektorn. Budgetpropositionen är ett dokument som regeringen lämnar till riksdagen. Budgetpropositionen är inte ett dokument som riktar sig till regeringens myndigheter eller till kommuner och landsting. Regeringens information om målet i budgetpropositionen är inte bindande styrning för de

[1] Prop. 2017/18:1, utgiftsområde 2.

statliga myndigheterna som lyder under regeringen. För att målet ska vara bindande för myndigheterna måste det finnas med i ett dokument som riktar sig direkt till myndigheterna.

För närvarande finns inte något generellt styrande mål och återrapporteringskrav för de statliga myndigheternas digitaliseringsarbete. Utredningen har gått igenom regeringens regleringsbrev till myndigheterna 2017 och konstaterar att regeringen, med några undantag, inte omsätter sitt eget mål för digitaliseringen av den offentliga förvaltningen i de statliga myndigheternas regleringsbrev.

7.2 … resultatstyrning

Av budgetlagens bestämmelser framgår att regeringen i budgetpropositionen ska lämna en redovisning av de resultat som uppnåtts i verksamheten i förhållande till de mål som riksdagen beslutat, s.k. utgiftsområdesmål. Denna resultatredovisning ska vara anpassad till utgiftsområdena.[2] I budgetpropositionen redovisar, analyserar och bedömer regeringen resultaten (måluppfyllelsen) i förhållande till de mål som riksdagen beslutat. Riksdagens bedömning av resultaten och återkoppling till regeringen med anledning av det, finns i respektive riksdagsutskotts budgetbetänkande. Därutöver följer varje utskott upp och utvärderar riksdagsbeslut inom utskottets ämnesområde.[3]

Bestämmelsen i budgetlagen utesluter inte att regeringen kan lämna resultatredovisningar även i andra sammanhang. Enligt regeringen kan det tvärtom vara naturligt att regeringen redovisar fördjupade analyser av olika verksamheter i skrivelser och i särpropositioner. Detta är särskilt motiverat på sektorsövergripande områden där verksamheten bedrivs och finansieras från flera olika utgiftsområden. Det kan även vara lämpligt på områden där andra styrmedel än ekonomiska sådana används i stor omfattning, t.ex. lagstiftning. Riksdagen kan även begära resultatinformation för olika verksamheter när behov finns.

De myndigheter under regeringen som ingår i den statliga redovisningsorganisationen ska senast den 22 februari varje år lämna en årsredovisning till regeringen som bl.a. ska innehålla en resultatredo-

[2] 10 kap. 3 § budgetlagen (2011:203).
[3] 4 kap. 8 § regeringsformen (1974:152).

visning. I resultatredovisningen ska myndigheterna redovisa och kommentera verksamhetens resultat i förhållande till de uppgifter som framgår av myndighetens instruktion eller, i förekommande fall, till vad som anges i regleringsbrev eller andra regeringsbeslut.[4]

De statliga myndigheternas resultatredovisningar är viktiga underlag för regeringens analys och bedömning av myndigheternas verksamheter och resultat och för regeringens resultatredovisning till riksdagen.

Exempel – mål och återrapporteringskrav i regleringsbrev för 2017

De mål som regeringen beslutat i statliga myndigheters regleringsbrev är bindande styrning för de aktuella myndigheterna. Utredningen har gått igenom regeringens regleringsbrev till myndigheterna 2017 och konstaterar att regeringen, med några undantag, inte omsätter sitt eget mål för digitaliseringen av den offentliga förvaltningen i de statliga myndigheternas regleringsbrev.

Under rubriken Mål och återrapporteringskrav i Bolagsverkets regleringsbrev för 2017 framgår att Bolagsverket ska tillhandahålla behovsanpassad och lättillgänglig information och service av hög kvalitet för företag och medborgare så att företags och medborgares kontakter med myndigheten blir enklare och effektivare. Digitala tjänster ska utformas, så långt det är möjligt och där det är relevant, så att de är förstahandsvalet i medborgares, organisationers och företagskontakter med Bolagsverket. Bolagsverket ska i budgetunderlaget redogöra för de insatser som har genomförts eller som Bolagsverket planerar att genomföra fram till 2020 för att utveckla myndighetens digitala tjänster samt göra information och service behovsanpassad och lättillgänglig. Redogörelsen ska innehålla kostnader och förväntad nytta med insatserna.

Under samma rubrik framgår även att Bolagsverket ska redovisa hur myndigheten under 2017 har arbetat för att öka anslutningen av relevanta meddelandeflöden till Mina meddelanden inom myndighetens ansvarsområde.

[4] 3 kap. 1 § förordningen (2000:605) om budgetunderlag och årsredovisning.

Under rubriken Uppdrag framgår dessutom att Bolagsverket ska ansvara för basförvaltning avseende den gemensamma e-tjänsten verksamt.se. Verket ska ha ansvar för förvaltning av teknisk drift, underhåll och förvaltning av ingående system i verksamt.se samt kundtjänst och support av dessa lösningar.

I Migrationsverkets regleringsbrev för 2017, under rubriken mål och återrapporteringskrav, finns ett mål för digitalisering som innebär betydande produktivitetsökningar. I anslutning till målet – som enligt utredningens bedömning avser myndighetens interna verksamhetsutveckling – anför regeringen att it-utvecklingen i högre utsträckning än tidigare ska omfatta hela myndighetens verksamhet. It-stöd ska utvecklas och införas så att betydande produktivitetsökningar, stärkt rättssäkerhet och ett väsentligt utvecklat stöd till kärnverksamheten uppnås under 2017. Utveckling av en gemensam processtandard ska vara en grund för utvecklingen av stödet. Myndigheten ska även under 2017 ansluta till Mina meddelanden.

I sin återrapportering ska Migrationsverket redovisa måluppfyllelsen och genomförda insatser för att uppnå målet. Särskild vikt ska läggas vid insatsernas konsekvenser för verksamheten i termer av effekthemtagning. Effekterna av anslutningen till Mina meddelanden ska också redovisas. Effekter i form av förbättrad service till målgrupper och effektivitetsvinster i handläggningen ska särskilt beaktas. I återrapporteringen ska Migrationsverket även tydliggöra vilka förutsättningar som krävs för att fler målgrupper ska kunna få information genom tjänsten.

I länsstyrelsernas regleringsbrev för 2017 framgår under rubriken mål och återrapporteringskrav att länsstyrelserna (avser alla länsstyrelser) ska arbeta för att inom sina verksamhetsområden bidra till att uppfylla regeringens mål för digitalisering om en enklare vardag för medborgare och företag, en öppnare förvaltning som stödjer innovation och delaktighet samt högre kvalitet och effektivitet i verksamheten.

Enligt ett uppdrag i regleringsbrevet ska länsstyrelserna till Boverket redovisa hur långt de har kommit i övergången till en digitaliserad ärendeprocess dels när det gäller tillhandahållande av underlag för kommunernas fysiska planering, dels gällande ärendehantering som följer av kommunernas planering och bygglovsverksamhet. Länsstyrelserna ska beskriva utvecklingen i förhållande till den redovisning

som länsstyrelserna lämnade till Boverket 2016 och effekterna av denna utveckling.

Under rubriken mål och återrapporteringskrav i Livsmedelsverkets regleringsbrev för 2017 står att Livsmedelsverket ska redovisa hur myndigheten under året har arbetat för att öka anslutningen av relevanta meddelandeflöden inom myndighetens ansvarsområde till Mina meddelanden, samt andra större framsteg i myndighetens digitaliseringsarbete.

7.3 Förslag till mål för den offentliga förvaltningens digitaliseringsarbete

Om ett mål är bindande eller inte handlar inte om hur målet i sig är utformat. Det är den styrande som bestämmer om målet ska vara bindande för styrobjektet eller inte. Dock gäller att om målet ska vara bindande måste det kopplas ihop med det eller de objekt som ska styras. Inom ramen för den ekonomiska styrningen i staten beskrivs mål vanligen som önskade framtida resultat eller tillstånd vid en viss framtida tidpunkt.[5] Dessa tillstånd bör främst vara lokaliserade utanför den agerande aktörens verksamhet, dvs. i samhället som helhet eller hos individer i samhället. Mål bör i första hand avse effekter eller utfall av verksamheten. I vissa fall kan det dock finnas skäl att formulera mål som avser utvecklingsområden inom en verksamhet.[6] När målen beslutats av riksdagen och regeringen är det viktigt att mål och ambitioner når ut till ansvariga inom statsförvaltningen.[7]

I delbetänkandet[8] betonade utredningen behovet av tydliga och styrande mål och sin avsikt att återkomma till denna fråga i slutbetänkandet. I delbetänkandet föreslog utredningen även att regeringen ska lägga fast ett för alla myndigheter tydligt och styrande mål för när den digitala förvaltningen ska vara genomförd inom staten, dvs. ett tidsbestämt mål. Tidsbestämningen skulle kunna tillämpas

[5] ESV 2006:7, Måluppfyllelseanalys, Hur måluppfyllelse, effekter och effektivitet kan undersökas och rapporteras.
[6] SOU 2015:43, Vägar till ett effektivare miljöarbete, slutbetänkande av Miljömyndighetsutredningen.
[7] Prop. 2009/10:175, s. 99.
[8] SOU 2017:23, digitalforvaltning.nu, delbetänkande av Utredningen om effektiv styrning av nationella digitala tjänster.

olika för olika statliga myndigheter eftersom deras förutsättningar i digitaliseringsarbetet varierar. Utredningen menar dock att det inte hindrar att samtliga statliga myndigheter omfattas av *ett* och samma gemensamma mål för sitt digitaliseringsarbete, tvärtom är det av flera olika skäl, viktigt att alla myndigheter under regeringen har samma mål och återrapporteringskrav för sitt digitaliseringsarbete. Ett tungt vägande skäl är att enskilda i så stor utsträckning som möjligt ska få så likvärdig service som möjligt oavsett myndighet. Ett annat skäl är att underlätta samverkan mellan myndigheterna.

Utredningen menar dessutom att inte endast myndigheterna under regeringen utan alla offentliga myndigheter bör omfattas av ett och samma mål för sitt digitaliseringsarbete. Detta för att enskilda individer i sina kontakter med de offentliga myndigheterna ska kunna förvänta sig att i sina kontakter bli bemötta och få likvärdig service oavsett offentlig myndighet.

Det är även viktigt eftersom en betydande del av de offentliga myndigheternas digitaliseringsarbete handlar om att analysera vilka processer som kan stödjas av och effektiviseras med digitala medel oavsett om det avser myndigheternas externa eller interna kontakter. Men det är också viktigt eftersom de offentliga myndigheterna i sitt digitala utvecklingsarbete förväntas effektivisera och samverka med andra myndigheter och för att utvecklingen går i riktning mot att den offentliga förvaltningen har en större andel gemensamma (digitala) resurser.

Myndigheterna behöver därför på ett så konkret sätt som möjligt veta vad det är de ska sträva mot, också för att kunna bedöma om de uppfyller sina skyldigheter eller inte. Ett samlat och tydligt grepp om den offentliga förvaltningens digitalisering måste innebära att det står klart för de inblandande instanserna vad som förväntas av dem. De författningsförslag som utredningen lämnar innebär dessutom att det offentliga åtagandet avseende förvaltningsgemensamma digitala funktioner utvidgas i betydande omfattning. För att riksdagens och regeringens styrning och resultatredovisning av de offentliga myndigheternas digitaliseringsarbete – och inte minst styrningen av förvaltningsgemensamma digitala funktioner – ska kunna vara så effektiv som möjligt bedömer utredningen att de ska omfattas av ett för hela den offentliga förvaltningen gemensamt mål som riksdagen beslutat.

7.3.1 Förslag till riksdagsbundet mål för den offentliga förvaltningens digitaliseringsarbete

Det mål som utredningen föreslår att riksdagen ska besluta om överensstämmer delvis med det mål som regeringen redovisar som sitt under rubriken mål i avsnittet om Digitalisering och it inom offentlig förvaltning i budgetpropositionen för 2018.[9] Det mål som regeringen redovisar i budgetpropositionen är dock, med några undantag, inte ett bindande mål för de statliga myndigheterna som lyder under regeringen, än mindre för övriga myndigheter i den offentliga förvaltningen, dvs. kommuner och landsting. Utredningen föreslår att målet ska vara

Den offentliga förvaltningens användning av digitala medel ska leda till att det blir så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service. Den offentliga förvaltningens användning av digitala medel ska vara säker samt öka kvaliteten och effektiviteten i den offentliga förvaltningen som helhet.

Utredningens förslag till riksdagens beslut om mål för den offentliga förvaltningens digitaliseringsarbete innebär – om det genomförs – att det blir direkt bindande för *regeringen*. Det innebär bl.a. att regeringen i budgetpropositionen till riksdagen ska redovisa den offentliga förvaltningens resultat i förhållande till det av riksdagen beslutade målet.[10]

Av budgetlagens bestämmelser framgår att regeringen i budgetpropositionen ska lämna en redovisning av de resultat som uppnåtts i verksamheten i förhållande till de mål som riksdagen beslutat, s.k. utgiftsområdesmål. Denna resultatredovisning ska vara anpassad till utgiftsområdena.[11]

[9] Prop. 2017/18:1, utgiftsområde 2, s. 93.
[10] 10 kap. 3 § budgetlagen (2011:203).
[11] 10 kap. 3 § budgetlagen (2011:203).

7.3.2 Utredningen rekommenderar mål för kommunernas och landstingens digitaliseringsarbete

SKL, som inte är en myndighet utan en politiskt styrd privaträttslig arbetsgivar- och intresseorganisation för alla kommuner, landsting och regioner i landet har utformat mål för sitt arbete att driva på, stödja och samordna medlemmarna för att ta vara på digitaliseringens möjligheter. SKL strävar sedan de beslutades 2011 mot tre övergripande mål för framtidens digitala samhälle:

- en enklare vardag för privatpersoner och företag,
- smartare och öppnare förvaltning stödjer innovation och delaktighet,
- högre kvalitet och effektivitet i verksamheten.

Dessa mål ingår i SKL:s strategi för att digitalisera samhället och att förbättra den kommunala sektorns förutsättningar för utveckling av e-förvaltning.

SKL:s mål är inte bindande för kommuner och landsting. Inte heller riksdagens beslut om mål för utgiftsområden – däribland det mål som utredningen föreslår att riksdagen ska besluta – innebär att de är bindande styrmedel för kommuner och landsting. För att styrningen av digitaliseringsarbetet i hela den offentliga sektorn ska kunna sträva mot samma mål vill utredningen i ljuset av avsiktsförklaringen mellan staten och SKL för en digital förnyelse av det offentliga Sverige, rekommendera fullmäktige i kommuner och landsting att utforma egna mål i samma anda som de mål som utredningen föreslår att riksdagen och regeringen ska besluta.

Kommun- och landstingsstyrelsen lämnar en årsredovisning till fullmäktige efter varje avslutat verksamhetsår. Bestämmelserna om kommunernas och landstingens bokföring och årsredovisning finns i lagen om kommunal redovisning.[12] Där framgår bl.a. att årsredovisningens förvaltningsberättelse ska innehålla en utvärdering av om de av fullmäktige beslutade målen och riktlinjerna, som är av betydelse för en god ekonomisk hushållning, har uppnåtts och följts.

[12] 11 kap. kommunallagen (2017:725), lagen (1997:614) om kommunal redovisning.

7.3.3 Förslag till mål för de statliga myndigheternas digitaliseringsarbete

Riksdagens beslut om mål för utgiftsområden innebär dock inte att de är bindande för de statliga myndigheterna som lyder under regeringen. En förutsättning för att målen ska vara direkt bindande för myndigheterna under regeringen är att de finns med i något av de styrdokument som riktas direkt till dem. Utredningen föreslår därför att regeringen – i en ny förordning som ska gälla för myndigheterna under regeringen – ska besluta om ett mål för digitaliseringen av myndigheterna och om myndigheternas resultatredovisning i förhållande till målet.

Utredningen bedömer att det är viktigt att regeringen beslutar om ett långsiktigt mål, dvs. ett mål som ska vara styrande för de statliga myndigheternas digitaliseringsarbete i tre år eller längre. Det innebär att regeringen bör besluta om ett mål i ett styrdokument som inte – såsom regleringsbrevet – är begränsat till ett budgetår.

Det är också viktigt att alla statliga myndigheter omfattas av ett och samma mål för digitaliseringsarbetet eftersom resultatet, dvs. effekterna av digitaliseringsarbetet handlar om myndigheternas service och kontakter med enskilda och att enskilda bör kunna förvänta sig samma service och möjligheter till kontakt oavsett myndighet. Ett annat styrdokument är den förordning med instruktion som regeringen beslutar om för alla statliga myndigheter. Även om alla statliga myndigheter har en instruktion är varje instruktion myndighetsspecifik och inte ett generellt styrmedel som gäller lika för alla myndigheter. Av instruktionen framgår den specifika myndighetens uppdrag och uppgifter m.m. som formuleras i termer som svarar mot den specifika myndighetens befogenheter. Risken med att föra in ett förvaltningsgemensamt mål för de statliga myndigheternas digitaliseringsarbete i instruktionen är att det skulle komma att anpassas till den specifika myndighetens uppdrag och därmed förlora den förvaltningsövergripande inriktningen. Utredningen förordar därför att regeringen i en särskild förordning som gäller för alla statliga myndigheter som lyder under regeringen beslutar om ett gemensamt och förvaltningsövergripande mål för digitaliseringsarbetet.

Utredningens förslag till mål för de statliga myndigheternas digitaliseringsarbete är att *den statliga förvaltningens användning av digitala medel ska leda till att det blir så enkelt som möjligt för så många*

som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av den statliga förvaltningens service. De statliga myndigheternas användning av digitala medel ska vara säker samt öka kvaliteten och effektiviteten i den offentliga förvaltningen som helhet.

De myndigheter som enligt förslaget omfattas av regeringens förordning med mål för digitaliseringsarbetet ska varje år till regeringen redovisa verksamhetens resultat i förhållande till målet i sina årsredovisningar. Resultatet ska redovisas i enlighet med 3 kap. 1 § förordningen om årsredovisning och budgetunderlag.[13]

Målen ska tillämpas från och med 2019

Utredningen anser att målen bör vara beslutade och tillämpas fr.o.m. budgetåret 2019. Därmed ska regeringen respektive myndigheterna under regeringen lämna resultatredovisningen av måluppfyllelsen år 2020.

7.4 Digitaliseringsmyndigheten stödjer regeringen – följer upp och analyserar

Utredningen föreslog i delbetänkandet att det ska ingå i den kommande digitaliseringsmyndighetens uppdrag att i en rapport till regeringen senast den 15 mars årligen redovisa och analysera den offentliga sektorns digitalisering. Rapporten ska även, enligt förslaget, spegla utvecklingen inom kommuner och landsting. I uppdraget ingår att analysera om de insatser som genomförs leder till regeringens mål och om insatserna är i linje med regeringens prioriteringar och vid behov föreslå åtgärder eller förändrade regelverk.

Utredningen bedömer att det i detta uppdrag även bör ingå att stödja regeringens arbete med en samlad analys och bedömning av resultatet av samtliga offentliga myndigheters digitaliseringsarbete i förhållande till förslaget till riksdagens mål för detta och att denna analys och bedömning redovisas i den årliga rapporten.

Utredningen föreslår att regeringen ger digitaliseringsmyndigheten ett särskilt uppdrag att utforma en metod och process för denna uppgift.

[13] 3 kap. 3 § förordningen (2000:605) om årsredovisning och budgetunderlag.

8 En övergripande plan – ett ramverk – för förvaltningsgemensamma digitala funktioner

8.1 Digitalisering, infrastruktur och styrning

Den digitala infrastrukturen beskrivs ofta som bestående av en hård och mjuk del. Till hårda infrastrukturen hör teknisk utrustning för att förmedla elektroniska signaler som bredbandsnät och mobilmaster. Dit hör också den tekniska utrustning som företag och hushåll behöver för att kommunicera och bearbeta information som datorer, mobiltelefoner m.m. samt utrustning för lagring och förmedling.

Som delar av den mjuka infrastrukturen brukar nämnas lagar och annan form av reglering som standarder, branschöverenskommelser m.m. Organisation och rollfördelning är andra viktiga delar av den mjuka infrastrukturen. Leverantörer av olika former av generella tjänster är en annan central del. Hit kan man räkna söktjänster, sociala medier och liknande som används för privat bruk men även av företag och myndigheter. Det finns också särskilda infrastrukturtjänster som huvudsakligen stödjer företag och myndigheter såsom autentiserings- och verifieringstjänster, meddelandeförmedlingstjänster, informationsbehandlings- och lagringstjänster samt katalogtjänster. Till den mjuka infrastrukturen kan även räknas befolkningens digitala kompetens. Digital kompetens innefattar, enligt Digitaliseringskommissionen, säker och kritisk användning av informationssamhällets teknik i arbetslivet, på fritiden och för kommunikationsändamål. Den underbyggs av användning av datorer för att hämta fram, bedöma, lagra, producera, redovisa och utbyta information samt för att kommunicera

och delta i samarbetsnätverk via internet.[1] Digital kompetens är också i vilken utsträckning man är förtrogen med digitala verktyg och tjänster samt har förmåga att följa med i den digitala utvecklingen och dess påverkan på ens liv.

Digital kompetens innefattar kunskaper att söka information, kommunicera, interagera och producera digitalt, färdigheter att använda digitala verktyg och tjänster, förståelse för den transformering som digitaliseringen innebär i samhället med dess möjligheter och risker samt motivation att delta i utvecklingen.[2]

Den digitala infrastrukturen, både den hårda och mjuka, har inte *en* upphovsman eller ägare utan är resultatet av många olika aktörers ansträngningar. Det offentligas förutsättningar för att reglera och styra över hela denna infrastruktur har vissa begränsningar särskilt vad gäller globala tjänsteleverantörer. Samtidigt är lagar och myndigheter en del av infrastrukturen och de politiska ambitionerna för digitaliseringen avgörande för den framtida samhällsutvecklingen.

Vilken roll det offentliga ska spela i infrastrukturen är beroende av hur väl statsmakterna förmår att samla och utnyttja de resurser man förfogar över, dvs. hur pass effektiv styrningen av den offentliga verksamheten är.

8.2 Ramverk för styrning av den digitala förvaltningen

Utredningen bedömer:
att det är avgörande för den effektiva styrningen av förvaltningsgemensamma digitala funktioner att beslutsprocesserna får ett snabbare förlopp.

Utredningen föreslår:
att Regeringskansliet fastställer en intern process för att bereda initiativ till förvaltningsgemensamma digitala funktioner, utvärdera dem och i förekommande fall inom ramen för de ordinarie processerna, bereda nödvändiga beslutsunderlag.

[1] SOU 2015:28, Gör Sverige i framtiden – digital kompetens, delbetänkande av Digitaliseringskommissionen.
[2] Digitaliseringskommissionen. SOU 2015:28, Gör Sverige i framtiden – digital kompetens, delbetänkande av Digitaliseringskommissionen.

Till ramverket hör de mål som riksdagen och regeringen beslutar och den uppföljning och resultatredovisning som följer av detta. Lagstiftning som omfattar offentliga myndigheter är en viktig del av infrastrukturen och därför också en central del i styrningsramverket.

Hit hör också formerna för samverkan mellan myndigheter och mellan statliga myndigheter och kommuner och landsting. Utvecklingen av förvaltningens digitala kompetens genom kompetensutveckling av chefer och medarbetare i offentlig verksamhet kan även nämnas i sammanhanget.

Samordnande myndigheter har en mycket central roll i ramverket för digital styrning. Regeringen har föreslagit att en digitaliseringsmyndighet ska inrättas från den 1 september 2018. Även andra myndigheter har viktiga roller i den digitala styrningen. Det gäller till exempel Datainspektionen, MSB och PTS. En viktig framgångsfaktor är att digitaliseringsmyndigheten har ett ansvar att utveckla och förvalta den offentliga it-arkitekturen. För norska Difi[3] är detta en central uppgift. I Sverige har eSam tagit på sig denna roll med utgångspunkt från e-delegationens arbete.[4]

It-arkitektur beskrivs på lite olika sätt, men består av principer, rollbeskrivningar, vägledningar, modeller för utveckling, förvaltning och självutvärdering samt standarder. Ett exempel på en sådan princip är att utgå från medborgarnas behov och livshändelser när e-tjänster utvecklas.

I direktiven till organisationskommittén för bildandet av digitaliseringsmyndigheten skriver regeringen att en utgångspunkt för myndighetens arbete ska vara att i lämpliga delar ta tillvara kunskap och erfarenheter som eSam-verkansprogrammet upparbetat, bl.a. avseende metoder och processer för samverkan.[5]

Ramverket måste även reglera roller och samverkan. Vidare måste det ange vad som ska vara ett statligt åtagande i form av förvaltningsgemensamma digitala funktioner. Förvaltningsgemensamma digitala funktioner under utveckling liksom andra större förvaltningsövergripande utvecklingsprojekt samlas i en nationell utvecklingsportfölj.

Till utvecklingsportföljen måste knytas beredningsprocesser för att fånga upp och ta till vara på de offentliga myndigheternas initiativ

[3] Direktoratet for forvaltning og IKT.
[4] Vägledande principer för digital samverkan, e-delegationen 2015.
[5] Dir 2017:117 Inrättande av en myndighet för digitalisering av den offentliga sektorn.

till förvaltningsgemensamma digitala innovationer. Sådana processer behövs dels på myndighetsnivå och bör enligt utredningens mening tas fram och drivas av den kommande myndigheten för digitalisering, dels på behörig beslutsnivå.

8.3 En tidsbestämd strategi

Utredningen föreslår:
att regeringen beslutar om en tidsbestämd övergripande plan – en strategi – för digitalisering och it i den offentliga förvaltningen.

År 2012 presenterade regeringen sin Strategi för en digitalt samverkande statsförvaltning.[6] Strategin som ännu inte är avslutad skulle underlätta regeringens arbete med att utveckla statsförvaltningen, och i det sammanhanget vara regeringens plan för förvaltningsgemensamma it-frågor. De mål som ingår i strategin, dvs. en enklare vardag för medborgare, öppnare förvaltning som stödjer innovation och delaktighet och högre kvalitet och effektivitet i verksamheten skulle ange inriktningen på regeringens arbete med att förbättra statsförvaltningens förmåga att samverka digitalt. Målen skulle vidare användas för regeringens koordinering av förvaltningsgemensamma utvecklingsprojekt och för att vägleda beredningen av beslut som skulle leda till ökad samverkansförmåga genom t.ex. fler förvaltningsgemensamma funktioner eller standarder. I strategin beskrev regeringen sina målsättningar för digitala funktioner som är gemensamma för hela statsförvaltningen, såsom Mina meddelanden.

Utredningen menar att det nu är hög tid att avsluta denna strategi och ersätta den med en ny övergripande plan – en ny tidsbestämd strategi – för digitalisering och it inom den offentliga förvaltningen. Strategin bör bl.a. innehålla tydliga milstolpar för när föreslagna offentliga åtaganden och andra åtgärder ska finnas på plats. Skälen till det är flera. Dels är den nu gällande strategin till stora delar överspelad. Jämfört med 2012 har den offentliga förvaltningen 2018 ett nytt utgångsläge för sitt digitala utvecklingsarbete. Utredningen kan dock samtidigt konstatera att flera av strategins förvaltningsgemen-

[6] Näringsdepartementet 2012, N2012/6402/ITP, Regeringens strategi för en digitalt samverkande statsförvaltning – Med medborgaren i centrum.

samma utvecklingsprojekt – som när strategin beslutades bedömdes vara särskilt viktiga för statsförvaltningens förmåga att samverka digitalt fortfarande – efter mer än fem år – inte har genomförts fullt ut. Bland dessa förvaltningsgemensamma utvecklingsprojekt finns bl.a. Svensk e-legitimation och Mina meddelanden. Dels är den nuvarande strategin avgränsad till enbart den *statliga* förvaltningen och därutöver avsedd att bidra till att nå målet för digitaliseringspolitiken inom utgiftsområde 22,[7] dvs. att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.

Frågor om digitalisering och it inom den offentliga förvaltningen är i dag överflyttade från politiken för informationssamhället inom utgiftsområde 22 till utgiftsområde 2. Inom utgiftsområde 2 är digitalisering och it inom den offentliga förvaltningen ett eget delområde och är, som framgått, för närvarande i avsaknad av ett riksdagsbundet mål.

Utredningen föreslår att regeringen – i denna omstart av politiken för digital förvaltning – beslutar om en ny tidsbegränsad strategi för hela den offentliga förvaltningen tillsammans med det förslag till riksdagsbundet mål för hela den offentliga förvaltningen som utredningen lämnar i detta betänkande.

Utredningen menar att en strategi med milstolpar för när olika beslut och åtgärder bör vara genomförda ska vara tidsbegränsad till tre år. Exempel på milstolpar är de förslag för effektiv styrning av förvaltningsgemensamma digitala funktioner som utredningen lämnar i detta betänkande. Däri ingår bl.a. riksdagens och regeringens beslut om förslagen till de olika författningar som avgränsar och tydliggör det offentliga åtagandet och styrningen av förvaltningsgemensamma digitala funktioner som utredningen presenterar avseende Mina meddelanden och statlig elektronisk identitetshandling liksom de kompletterande bestämmelser till EU:s förordning om elektronisk identifiering som utredningen föreslår.

Andra exempel på milstolpar är Regeringskansliets beslut om nödvändiga processer för att bereda och bedöma förslag till nya förvaltningsgemensamma digitala funktioner och andra förvaltningsgemensamma digitala tjänster samt att digitaliseringsmyndigheten är etablerad och har börjat leverera resultat i förhållande till sin instruktion. För att sätta ett yttre tryck på digitaliseringsarbetet inom den

[7] Prop. 2011/12:1, bet. 2011/12:TU1, rskr. 2011/12:87.

offentliga förvaltningen och för att den effektiva styrningen av förvaltningsgemensamma digitala funktioner ska kunna komma på plats utan ytterligare fördröjning är tre år en lämplig tidsrymd. Därefter bör regeringen utvärdera effekterna och vidta de korrigerande åtgärder som behövs för att styra utvecklingen mot önskat mål.

8.4 Avsiktsförklaring mellan staten och Sveriges Kommuner och Landsting

Utredningen föreslår:
att regeringen tar initiativ till en förnyad avsiktsförklaring mellan staten och Sveriges Kommuner och Landsting för digitalisering och it i den offentliga sektorn.

I oktober 2015 beslöt regeringen att skriva under en avsiktsförklaring mellan staten och SKL,[8] för en digital förnyelse av det offentliga Sverige. Syftet med avsiktsförklaringen var att tydliggöra hur parterna kan stärka förutsättningarna för digital samverkan mellan staten, kommuner och landsting genom att peka ut ett antal områden för fördjupat samarbete.[9] Parterna ska verka för ett gemensamt budskap om digital förnyelse av det offentliga Sverige. Avsiktsförklaringen syftar dessutom till att öka förutsättningarna för en stärkt styrning och uppföljning av digitaliseringen av det offentliga Sverige och verka för ett gemensamt budskap.

Parterna menar att det behövs mer gemensamma digitala funktioner för att stödja utvecklingen av medborgarcentrerade lösningar. Därför ska myndigheterna i större utsträckning dela och tillsammans utveckla digitala lösningar. För att underlätta samverkan är det, enligt avsiktsförklaringen, viktigt att lösa ut frågor om bland annat förvaltningsgemensamma specifikationer för hela den offentliga sektorn, en långsiktig förvaltning av den nationella infrastrukturen och juridiska förutsättningar för en digital förnyelse av det offentliga

[8] Sveriges Kommuner och Landsting, SKL, är inte en myndighet utan en politiskt styrd privaträttslig arbetsgivar- och intresseorganisation för alla kommuner, landsting och regioner i landet.[8] Samtliga Sveriges landsting, kommuner och regioner är medlemmar i SKL. Medlemskapet är dock frivilligt och kan avslutas.
[9] 2015-10-29, N2015/07455/EF, utdrag Protokoll vid regeringssammanträde.

Sverige. Parterna kommer att fortsätta driva dessa frågor inom ramen för avsiktsförklaringen.

Avsiktsförklaringen gäller till och med utgången av 2018. Då ska behovet av en förnyad avsiktsförklaring utvärderas.

Utredningen anser att det är viktigt att regeringen och SKL som en del av en tidsbegränsad övergripande plan – en strategi – för digitalisering och it inom den offentliga förvaltningen, undertecknar en ny avsiktsförklaring. Syftet är att på så sätt tillsammans stärka och skapa synergier i det förvaltningsgemensamma arbetet med att digitalisera den offentliga förvaltningen mot ett gemensamt mål.

Enligt utredningen är det för sent att göra en sådan utvärdering efter utgången av 2018. En förnyad avsiktsförklaring behövs innan dess. Parterna har möjlighet att i samförstånd revidera avsiktsförklaringen under innevarande period.

9 Informationssäkerhet – en naturlig del i digitaliseringen

Utredningen bedömer:
För att digitaliseringen och dess effekter ska åtnjuta alla aktörers, inklusive individernas, förtroende och leva upp till förväntningarna om trygghet och säkerhet måste informationssäkerhetsarbetet inom offentliga myndigheter styras på ett mer kraftfullt sätt och därmed genomsyra samtliga digitaliseringsprocesser. En kombination av krav på ett systematiskt och riskbaserat informationssäkerhetsarbete, incidentrapportering och tillsyn tillsammans med ett ändamålsenligt stöd ska säkerställa att samhällets aktörer ges möjlighet att hantera och prioritera informationssäkerhetsbehoven.

Utredningen föreslår:
att regeringen inleder ett arbete att samordna och strukturera reglering inom informationssäkerhetsområdet,
att regeringen ger digitaliseringsmyndigheten i uppdrag att ta fram och mäta nyckeltal för informationssäkerhetsrelaterade aspekter i syfte att följa informationssäkerhetsmognaden i förhållande till digitaliseringen,
att regeringen tar fram rättsliga krav som omfattar samtliga offentliga myndigheter att införa ett systematiskt och riskbaserat informationssäkerhetsarbete och ge MSB i uppdrag att utreda hur tillsyn över informationssäkerhetsområdet och incidentrapportering kan genomföras.

Digitaliseringen är något som ofta drivs genom att visa på nytta, t.ex. genom att förenkla processer där individer har kontakt med det allmänna. Därmed frigörs resurser som annars hade lagts på administrativt arbete.

Digitaliseringen medför att offentliga myndigheter allt mer är att betrakta som informationsförädlare och sålunda måste ha tillgång till, och kunna behandla, information. Detta ställer krav på ett strukturerat arbetssätt för att säkerställa att den information som behandlas hanteras på ett säkert sätt. Med säker hantering avses både att säkra tillgång till öppen information och att information som inte är öppen ska skyddas. När det uppstår brister i informationssäkerheten kan följden bli omfattande konsekvenser både för samhället i stort och för individers integritet. Tilliten till digitaliseringen kan äventyras.

Det är ofta svårt att motivera investeringar i informationssäkerhet eftersom det sällan ger en synbar eller upplevd nytta direkt vid investeringstillfället. Informationssäkerhet kan t.o.m. av vissa betraktas som något som endast fördyrar, försvårar och riskerar att försena och till och med stoppa projekt. Många organisationer undviker därför att sätta sig in i vilka värden säker hantering av information ger på längre sikt.

Inte sällan betraktas också informationssäkerhetsfrågor som enbart it-frågor vilket innebär att säkerhetsåtgärder av administrativ och organisatorisk art mer eller mindre förbises, exempelvis utformning och följsamhet till arbetssätt och rutiner. Dessutom hänvisas resursförfrågningar till att ingå i rådande it-budget som i sin tur inte behöver vara föremål för någon strategisk satsning.

Informationssäkerhet ska genomsyra alla processer som handlar om digitalisering. Detta har påpekats även i tidigare utredningar och rapporter.

Under 2015 lämnades ett betänkande av NISU 2014[1] till regeringen. Ett av förslagen i denna utredning var att det bör etableras en nationell modell för att styra samhällets informationssäkerhet.

Även Riksrevisionen[2] har påpekat att det behövs en starkare styrning från regeringen gentemot myndigheterna, så att nödvändiga

[1] SOU 2015:23, Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten, betänkande av NISU 2014.
[2] RiR 2016:8, Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten.

säkerhetsåtgärder verkligen blir genomförda. Att enbart ta fram ett övergripande regelverk är inte tillräckligt för att säkerheten ska bli god. Om regeringen inte efterfrågar information om myndigheternas informationssäkerhet och inte framhåller vikten av god informationssäkerhet bedömer Riksrevisionen att myndigheternas ledningar inte heller kommer att prioritera frågan.

Regeringen har efter sin beredning av NISU:s betänkande och Riksrevisionens rapport tagit fram en nationell cybersäkerhetsstrategi[3] i vilken det framgår att det ska tas fram en nationell modell till stöd för ett informationssäkerhetsarbete. Huvudsyftena med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Regeringen vill genom strategin även stödja de insatser och det engagemang som redan finns i samhället för att stärka informations- och cybersäkerheten. Strategin omfattar därmed hela samhället, det vill säga statliga myndigheter, kommuner och landsting, företag, organisationer och individer.

9.1 Fragmenterad styrning av informationssäkerhet

Arbetet med informationssäkerhet är i dag till stor del varje organisations eget ansvar. I och med att organisationer i dag är allt mer beroende av andra för sin informationshantering, exempelvis i de förvaltningsgemensamma digitala funktionerna, är det nödvändigt med samordnade åtgärder för att reducera risker och behålla säkerhetsnivån. Möjligheterna att ytterligare kraftigt öka resurserna som läggs ned på informationssäkerhetsarbetet är dock begränsade inom många organisationer.

Som utredningen konstaterade i delbetänkandet[4] är det nationella informationssäkerhetsarbetet i dag uppdelat i olika, delvis överlappande, ansvarsområden, både på departements- och på myndighetsnivå. Detta gör att det i dag saknas ett enhetligt arbetssätt och enhetligt regelverk för samhällets informationssäkerhetsarbete och det finns få gemensamma krav på informationssäkerhet. Expert- och sektorsmyndigheter har, utifrån sitt specifika ansvarsområde eller

[3] Skr. 2016/17:213, Nationell strategi för samhällets informations- och cybersäkerhet.
[4] SOU 2017:23, digitalforvaltning.nu. s. 102–110.

expertområde, gett ut föreskrifter som i olika grad har bäring på informationssäkerhet.

Genom att fler aktörer – utan samordning – utfärdar regler på området finns en stor risk att fragmenteringen av kravställningen på området ökar. Detta får inte sällan till resultat att erfarenheter och kunskap som finns inte nyttjas effektivt, att de resurser som allokeras inte används inom de områden där bristerna är som störst och att utfärdade informationssäkerhetskrav fördröjs eller aldrig blir utförda på grund av oklara ansvarsförhållanden.

Det fragmenterade arbetet leder till att det saknas gemensamma riktlinjer för vilket skydd olika typer av informationstillgångar minst bör ha. Detta leder till att samma typ av information riskerar att få helt olika skydd beroende på var i förvaltningssystemet som den hanteras. Detta innebär inte sällan även effektivitetsbrister då lösningar får olika utformning vilket skapar en minskad interoperabilitet som i sin tur leder till en ökad kostnad.

Mot bakgrund av detta anser utredningen att bristen av samordnat rättsligt stöd medför svårigheter att säkerställa att offentliga aktörer har rätt förutsättningar i sitt arbete med att genomföra och förvalta digitaliseringsarbetet på ett sådant sätt att de tjänster som erbjuds uppfyller tillräckliga krav på tillgänglighet, riktighet och konfidentialitet.

9.2 Att reglera informationssäkerhet

I dagsläget har MSB föreskriftsrätt över statliga myndigheters arbete med informationssäkerhet. Av MSB:s föreskrifter om statliga myndigheters informationssäkerhet[5] framgår att

> Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. I detta arbete ska standarderna ISO/IEC 27001:2014 och ISO/IEC 27002:2014 beaktas. Tillräckliga resurser ska tilldelas för informationssäkerhetsarbetet samt löpande och regelbunden information lämnas till myndighetsledningen.[6]

[5] MSBFS 2016:1, Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet mars 2016.
[6] 7 § MSBFS 2016:1.

Nyckelorden i paragrafen är ”ledningssystem”, ”systematiskt” och ”riskbaserat”. Att informationssäkerhetsarbetet ska bedrivas som ett ledningssystem betyder att det ska ingå som en naturlig del i den dagliga verksamheten och inriktas och styras av organisationens ledning. Systematiken innebär att arbetet ska ha en tydlig struktur, bedrivas genom att ställa upp mål på kort och lång sikt och i syfte att planera, genomföra, kontrollera, följa upp, utvärdera och förbättra säkerheten i verksamhetens informationshantering.

Att ett informationssäkerhetsarbete ska vara riskbaserat innebär att det är den aktuella situationen och den aktuella informationsmängden som ställer de exakta kraven på informationssäkerhetsarbetet och de säkerhetsåtgärder som införs. En riskbedömning som genomförs i en organisation som har en informationsmängd på papper är troligen helt skild från den riskbedömning en annan organisation där samma typ av informationsmängd behandlas i ett digitaliserat och uppkopplat system.

Som framgår ovan finns det i dag en reglering inom informationssäkerhetsområdet. Den är dock inte heltäckande och den siktar in sig på de specifika expert- och sektorsmyndigheternas ansvarsområden.

Ett aktivt informationssäkerhetsarbete är en förutsättning för en fortsatt digitalisering. Det ska ses som ett baskrav i alla organisationers informationshantering. I dag finns inom andra områden krav på ett systematiskt och riskbaserat arbete, t.ex. miljö och arbetsmiljö. För arbetsmiljön gäller Arbetsmiljöverkets föreskrifter om systematiskt arbetsmiljöarbete.[7] Det är ett ledningssystem och har till sin struktur många likheter med andra standardiserade ledningssystem. Det finns dock en viktig skillnad – det är ett lagkrav att ha ett systematiskt arbetsmiljöarbete[8] som omfattar alla arbetsgivare, medan kravet på ett systematiskt och riskbaserat informationssäkerhetsarbete endast omfattar statliga myndigheter genom en föreskrift.

Målbilden för styrning inom informationssäkerhetsområdet torde vara att få motsvarande effekt av styrningen som på områdena för t.ex. miljö och arbetsmiljö. Det skulle kunna vara att ta fram lagkrav på att införa ledningssystem för informationssäkerhet (LIS) för att höja medvetenheten om området samt att få kravet att träffa samtliga offentliga myndigheter. Det kan också leda till att ge mandat för

[7] Arbetsmiljöverkets föreskrifter om systematiskt arbetsmiljöarbete (AFS 2001:1).
[8] 3 kap. 2 a § arbetsmiljölagen (1977:1160).

expert-och sektorsmyndigheter att genomföra inspektioner (tillsyn) och ha sanktionsmöjligheter som ett verktyg.

Utredningen menar att alla offentliga myndigheter ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Detta för att enskilda individer i sina kontakter med offentliga myndigheter ska kunna förvänta sig en säker informationshantering, oavsett myndighet.

9.3 Tillsyn, revision och uppföljning

Utredningen har inte kunnat finna någon samordnad tillsyn av det systematiska informationssäkerhetsarbetet. Viss tillsyn finns såsom Post- och telestyrelsen (PTS) inom området elektronisk kommunikation[9], Datainspektionen för personuppgifter[10] samt Försvarsmakten och Säkerhetspolisen gällande säkerhetsskyddet[11].

När det gäller kommuner, de som kanske kommer att erbjuda flest digitala tjänster, finns inte några lagkrav på att arbeta systematiskt med informationssäkerhet, inga krav på att rapportera incidenter och inte heller någon tillsyn.

Inom vissa delar av det offentligas verksamhet kommer tillsynen utökas i och med att NIS-direktivet[12] träder i kraft i maj 2018, men den tillsynen är endast gentemot samhällsviktig verksamhet inom de sju sektorerna energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Detta är dock bara en delmängd av de elva sektorer som MSB identifierat[13] som samhällsviktiga sektorer. Utöver de samhällsviktiga sektorerna finns all övrig offentlig verksamhet som i dagsläget i stort är helt utan tillsyn.

Vid införande av tillsyn är det viktigt att regleringens olika delar samspelar så att det inte uppstår en obalans mellan dem.[14] Om t.ex. vissa delar av tillsynsverksamheten är detaljerat reglerad med avseende på vilka prestationer en tillsynsmyndighet ska åstadkomma

[9] 7 kap. lagen (2003:389) om elektronisk kommunikation.
[10] 43 § personuppgiftslagen (1998:204).
[11] 31 § säkerhetsskyddslagen (1996:627).
[12] Direktiv (2016/1148/EU) om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
[13] Handlingsplan för skydd av samhällsviktig verksamhet (MSB597) – december 2013.
[14] Statskontoret 2012, Tänk till om tillsynen – Om utformningen av statlig tillsyn.

medan andra delar har mer övergripande målformuleringar finns en risk att den detaljerade regleringen får en starkt styrande inverkan på tillsynen, med den konsekvensen att annan mer strategiskt inriktad tillsyn får stå tillbaka. Det finns också en stor risk att organisationer som är utsatta för tillsyn fokuserar arbetet på de delar som granskas mer specifikt och att arbetet att jobba med informationssäkerhet över hela linjen får stå tillbaka.

De uppföljningar som har gjorts inom området informationssäkerhet har bland annat visat att myndigheternas granskning av sitt eget informationssäkerhetsarbete behöver effektiviseras.[15] Granskningen kan bedrivas med olika metoder och på olika nivåer. Den kan också behöva kombineras med rapportering av resultatet av genomförda granskningar för att uppnå avsedd effekt. Olika alternativa vägar för att stärka både granskning och rapportering av informationssäkerhetsarbetet bör övervägas.

Utredningen förslog i delbetänkandet att digitaliseringsmyndigheten ska följa upp och analysera utvecklingen av den offentliga sektorns digitalisering och användningen av nationella digitala tjänster baserad på nyckeltal och myndigheters rapportering till regeringen.[16] På samma sätt bör även informationssäkerhetsarbetet följas upp genom att digitaliseringsmyndigheten tar fram nyckeltal som mäter informationssäkerhetsmognaden i de organisationer som mäts gällande digitaliseringen.

Utredningen bedömer även att alla offentliga myndigheter bör omfattas av en för hela den offentliga förvaltningen gemensam reglering gällande tillsyn av informationssäkerhetsarbetet med tillhörande incidentrapportering. Hur denna tillsyn och incidentrapportering ska utformas ligger utanför denna utrednings område och bör utredas närmare. Utredningen föreslår att regeringen ger MSB, som i dag är ansvarig för att ta emot rapportering från statliga myndigheter, i uppdrag att utreda hur tillsyn och incidentrapportering inom informationssäkerhetsområdet kan genomföras för samtliga offentliga myndigheter.

[15] MSB remissvar över SOU 2015:23 Informations- och cybersäkerhet i Sverige, dnr 2015-2930.
[16] SOU 2017:23, digitalforvaltning.nu.

10 Förvaltningsgemensamma digitala funktioner och elektronisk identifiering

Utredningen bedömer:
att området för elektronisk identifiering är underreglerat,
att e-legitimation ska benämnas elektronisk identitetshandling,
att regelverk för elektroniska identitetshandlingar är en förvaltningsgemensam digital funktion,
att regelverk som anvisar hur offentliga myndigheter elektroniskt ska kontrollera individers identitet är en förvaltningsgemensam digital funktion.

Enligt utredningens direktiv finns det behov av att analysera omfattningen av det offentliga åtagandet i förhållande till de privata aktörernas roll och lämna förslag på vidareutveckling av modellen för elektroniska identitetshandlingar för att långsiktigt tillgodose den offentliga sektorns och användarnas behov samt främja innovation på den privata marknaden. Utredningen ska bland annat lämna förslag på långsiktig utformning processen för grundidentifiering, utfärdande av elektroniska identitetshandlingar och organisering av attribut- och behörighetstjänster som medger att elektroniska identitetshandlingar kan användas i olika roller, särskilt i tjänsten. I följande kapitel (10–15) behandlar utredningen de förutsättningar, bedömningar och förslag som har att göra med elektroniska identitetshandlingar för användning i Sverige.

10.1 Elektronisk identifiering – ett underreglerat område

Elektronisk identifiering är en förutsättning för att offentliga myndigheter ska kunna utveckla e-tjänster och erbjuda individer stöd och service via dessa. Det är vidare en förutsättning för många offentliga arbetsgivare för att deras anställda i sin yrkesroll ska kunna identifiera sig mot interna eller externa system på ett säkert och tillförlitligt sätt. Allt mer av kontakterna mellan individer och offentliga myndigheter liksom privata aktörer inleds via e-tjänster i vilka individen måste identifiera sig. Elektronisk identifiering innefattar:

- den elektroniska identitetshandling som individen har, hur den utformas, vem som utfärdar den liksom hur den kan användas samt
- relationer mellan användaren, den som har en e-tjänst och den som har utfärdat en elektronisk identitetshandling.

Området för elektronisk identifiering omfattar många olika delar, där olika aktörer är inblandade. Det är viktigt att elektronisk identifiering omgärdas av ett legalt och säkerhetsmässigt nät. För att elektronisk identifiering ska fungera måste det också finnas på plats utdelade ansvar för olika uppdrag. En framgångsfaktor är om det är lätt för inblandade aktörer att veta vem som har ett ansvar och vad som ska eller kan göras. Utredningen kommer i följande kapitel att återkomma till den författningsreglering som finns i dag och de pågående initiativen på området samt det förslag som utredningen lämnar. Utredningen kan emellertid redan här konstatera att området för elektronisk identifiering är underreglerat. För att komma fram till vilka delar och således vilket regelverk som skapar en eller flera förvaltningsgemensamma digitala funktioner måste varje del analyseras för sig. Nedan följer i korthet vilka delar som utredningen bedömer vara förvaltningsgemensamma och vars regelverk utgör förvaltningsgemensamma digitala funktioner. Först vill utredningen emellertid uppmärksamma begreppet e-legitimation.

10.2 Elektronisk identitetshandling *i stället för* e-legitimation

Den identitetshandling som individer använder för att identifiera sig elektroniskt kallas för e-legitimation. En legitimationshandling är en handling som användaren nyttjar för att legitimera sig. Legitimationshandlingar kallas också identitetshandlingar eller identitetskort. Enligt Svenska akademins ordbok betyder *legitimation* en handling varigenom något görs lagligt eller behörighet.[1] Begreppet innefattar därmed behörighetsstrukturer. En *identitet* kan vara hur en individ upplever sig själv, men det kan också betyda att två ting egentligen är ett och samma.[2]

En identitetshandling syftar till att visa en individs identitet och kan användas för att kontrollera att individen är den som han eller hon utger sig för att vara. Identitetskontrollen görs genom att jämföra individen med identitetshandlingen.

Utredningen menar att identitet och behörighet ska skiljas åt. Behörigheter kommer av att uppgifterna om en individ på identitetshandlingen kombineras med ett regelverk, exempelvis att individen får köpa alkoholdrycker[3] eller att någon är legitimerad för ett visst yrke, exempelvis läkare.[4] För att avgöra om en individ får köpa vin är det mer intressant om individen överensstämmer med regelverket, dvs. är över 20 år gammal, än vem individen är. För att veta om en individ är legitimerad läkare måste uppgifter om individen kopplas samman med uppgifter i registret över legitimerad hälso- och sjukvårdspersonal.

Utfärdare av elektroniska identitetshandlingar vill skilja uppgifter om en individs identitet från uppgifter om dennes behörighet. Detta eftersom behörigheter kan variera snabbt från en dag till en annan, medan identitetsuppgifterna är bestående. Utredningen menar därför att begreppet *e-legitimation är missvisande*. Begreppet antyder att det är fråga om en samling elektroniska uppgifter som utvisar både identitet och behörighet. Utredningen bedömer att det är lämpligare att fortsättningsvis tala om *elektroniska identitetshandlingar*, för att inte

[1] www.saob.se/artikel/?seek=legitimation&pz=1, 2017-12-21.
[2] www.saob.se/artikel/?unik=I_0001-0061.e20x&pz=5, 2017-12-21.
[3] 3 kap. 7 § Alkohollagen (2010:1622).
[4] Socialstyrelsen ansvarar för ett register över legitimerad hälso- och sjukvårdspersonal (HoSp). Registret innehåller aktuella uppgifter om legitimerad hälso- och sjukvårdspersonal. Uppgifterna kan användas för upplysningar om personals behörighet till apotek, arbetsgivare och allmänhet samt för tillsyn. Uppgifterna används också för statistik.

blanda samman frågor om identitet och behörighet. I det följande kommer utredningen därför att utgå från begreppet elektronisk identitetshandling.

10.3 Elektroniska identitetshandlingar är en förvaltningsgemensam digital funktion

Utredningen menar att identitetshandlingar är en förvaltningsgemensam angelägenhet. Det är viktigt för enskilda individer, offentliga myndigheter och marknadens aktörer att veta vilka identitetshandlingar som går att lita på samt vad de kan användas till. Detta gäller för fysiska såväl som elektroniska identitetshandlingar. Elektroniska identitetshandlingar är en förvaltningsgemensam digital funktion, som bör författningsregleras. Utredningen återkommer med bedömningar och förslag hur en sådan författningsreglering ska se ut.

10.4 Sätt för offentliga myndigheter att elektroniskt kontrollera individers identitet är en förvaltningsgemensam digital funktion

För att individer ska kunna använda sina elektroniska identitetshandlingar hos offentliga myndigheter måste en offentlig myndighet ha etablerat en relation till utfärdaren av den elektroniska identitetshandlingen. Etableringen av relationen mellan utfärdare och offentliga myndigheter med behov av en funktion för elektronisk identifiering är alltså redan författningsreglerad. För offentliga myndigheter etableras denna relation ofta genom upphandling och ibland genom att de beslutar om valfrigetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering. Utredningen bedömer att det finns behov att staten anvisar offentliga myndigheter ett sätt att anskaffa funktionen för elektronisk identifiering. Det är alltså en förvaltningsgemensam angelägenhet att säkerställa att individer kan använda samma elektroniska identitetshandling hos alla offentliga myndigheter. Utredningen menar att ett regelverk som säkerställer detta är en förvaltningsgemensam digital funktion och återkommer till detta i senare kapitel.

11 Processen för grundidentifiering

11.1 Vad betyder grundidentifiering?

Utredningen bedömer:
att grundidentifiering syftar till att koppla ihop en individ med uppgifter i folkbokföringsregistret och resulterar i en identitetshandling.

Av utredningens direktiv framgår inte vad som menas med processen för grundidentifiering. Utredningen bedömer att det inte heller finns någon enhetlig definition av begreppet. Det används för att beskriva flera olika företeelser, *i bland* förfarandet när en individ kopplas ihop med registrerade uppgifter om individen för första gången, *i bland* förfarandet när en individ ansöker om en ny identitetshandling men redan har en befintlig identitetshandling av samma eller annat slag att visa upp, *i bland* för den allra första registreringen som staten gör av en individ. I det senare fallet kan det t.ex. handla om registreringen av ett nyfött barn i samband med förlossningen eller av en individ som ansöker om asyl i Sverige.

Utredningen kommer inte i det följande att förhålla sig till *registrering* av uppgifter om en individ, alltså det som görs när en individ folkbokförs eller registreras som asylsökande. Utredningen kan emellertid konstatera att det påtalats brister i dessa processer, bl.a. Riksrevisionen har framfört kritik.[1]

I vissa fall används begreppet *grundidentifiering* synonymt med *ursprungsidentifiering*. Utredningen kommer inte att använda begreppet ursprungsidentifiering. I stället använder utredningen begreppet grundidentifiering, men eftersom det används för så många olika före-

[1] Folkbokföringen – ett kvalitetsarbete i uppförsbacke, RiR 2017:23.

teelser är det viktigt att beskriva hur utredningen valt att tolka begreppet. Den tolkningen utgör nämligen basen för de förslag som utredningen lämnar.

Grundidentifiering finns inte som ord i Svenska akademins ordbok. Där finns emellertid en beskrivning av ordet *identifiera*, enligt följande

> Uppfatta l. betrakta (ngt) såsom identiskt (med ngt annat), uppfatta l. betrakta (två l. flera ting l. begrepp o. d.) såsom (i grunden) samma sak; ”sätta likhetstecken mellan”, likställa (två l. flera ting)
>
> fastställa (ngns l. ngts) identitet, fastställa vem en given person l. vad en given sak är; igenkänna (ngn l. ngt ss. ngt). *Lyckas identifiera en förbrytare med hjälp av fingeravtryck.*

Givet denna utgångspunkt kan aktörer förhålla sig på olika sätt till begreppet identifiera. En individ kan styrka sin identitet genom att *identifiera sig*. Andra, exempelvis en offentlig myndighet eller en annan privat aktör, kan *identifiera någon* genom att kontrollera hans eller hennes identitet. Att identifiera sig eller identifiera någon beskrivs sammantaget som *identifiering*. I begreppet *identifiering* ligger alltså både det som individen gör och den kontroll som en annan aktör vidtar. Identifiering kan göras i många sammanhang och i relation till aktörer av olika slag.

För att identifieringen ska vara säker och tillförlitlig måste det vara bestämt vilka uppgifter om en individ som ska visas upp eller kontrolleras. I detta led kommer identitetshandlingar in. I dess mest renodlade syfte är tanken med en identitetshandling att den kopplar ihop registrerade uppgifter med fysiska kännetecken (oftast ett fotografi). Denna koppling dokumenteras på ett (plast)kort eller liknande, som kan användas vid identifiering, alltså för att individen ska kunna identifiera sig och för att någon annan ska kunna kontrollera individens identitet. Kontrollen genomförs genom att jämföra uppgifter på identitetshandlingen med den individ som man har framför sig.

Utredningen menar att det förfarande som leder fram till en identitetshandling och som innebär att en individ ska styrka sin identitet är en process som innefattar grundidentifiering.

11.2 Grundidentifiering – ett statligt ansvar

Utredningen bedömer:
att en process för utfärdande av identitetshandling, där grundidentifiering ingår, ska innefatta följande principer:

- ansökan om en identitetshandling måste göras vid ett personligt besök hos den utfärdande aktören,
- individen ska styrka sin identitet på ett tillförlitligt sätt,
- den utfärdande aktören ansvarar för att dokumentera fysiska kännetecken genom att åtminstone ta ett fotografi av individen,
- identitetshandlingen lämnas ut vid ett personligt besök hos utfärdaren.

Utredningen föreslår:
att grundidentifiering ska förbehållas den identifiering som staten utför i samband med utfärdande av de identitetshandlingar som följer principerna för grundidentifiering som utredningen har preciserat.

En tillförlitlig grundidentifiering är en förutsättning för tilliten till elektroniska identitetshandlingar. E-legitimationsnämnden påtalar i sin rapport ”Fortsatt försörjning av tjänster för e-legitimering och e-underskrift” att staten behöver utöka sitt ansvar i samband med identifiering av individer som ansöker om svenska identitetshandlingar. Nämnden påtalar att ett syfte med ett utökat statligt ansvar är *dels* att underlätta vid nyutgivning av innovativa och säkra elektroniska identitetshandlingar, *dels* att motverka s.k. id-kapningar och annat missbruk. Vidare framgår att E-legitimationsnämnden har uppfattat att det finns intresse av att staten ska utföra den grundidentifiering av individen som behövs vid nyutgivning av elektroniska identitetshandlingar och att det inte är lämpligt att genomföra detta på distans.[2]

Utredningen menar att grundidentifiering är ett led i processen att utfärda en identitetshandling. I dag utfärdar såväl statliga som privata aktörer identitetshandlingar. De statligt utfärdade handlingar

[2] Fortsatt försörjning av tjänster för e-legitimering och e-underskrift, E-legitimationsnämnden, dnr 131 645711-15/9513, s. 29.

som används som identitetshandlingar är passet, det nationella identitetskortet, identitetskortet för folkbokförda i Sverige och körkortet. Privata aktörer, men också vissa offentliga aktörer, utfärdar identitetskort med s.k. SIS-märkning.[3]

Utredningen har analyserat några av de befintliga grundidentifieringsprocesserna.[4] Av genomgången framgår att processerna skiljer sig åt – olika krav ställs inför utfärdande av olika identitetshandlingar. Detta gäller såväl för de fysiska identitetshandlingar som staten respektive privata aktörer utfärdar som för elektroniska identitetshandlingar.

I nästan alla processer gäller att individen ska styrka sin identitet. Då handlar det om att sammanföra registrerade uppgifter om en viss individ med en viss fysisk person. Med registrerade uppgifter avses framför allt sådana uppgifter som framgår av folkbokföringsregistret. Sättet som individen kan styrka sin identitet på skiljer sig åt. Har individen redan en viss sorts identitetshandling är den ofta tillräcklig för att styrka identiteten. Om individen saknar identitetshandling av visst bestämt slag krävs att andra personer med vissa närmare angivna kopplingar till individen intygar dennes identitet.[5]

Det som skiljer sig åt mellan de olika identitetshandlingarna är primärt ansöknings- och utlämnandeprocessen. Där ställs i många fall krav på att individen ska inställa sig personligen hos den utfärdande aktören vid såväl ansökan som utlämnande. I vissa fall finns det dock inga sådana krav, exempelvis är det möjligt att hämta ut ett körkort via ett postombud.[6] Ytterligare en sak som skiljer sig åt mellan de olika identitetshandlingarna är hur uppgifter om individen dokumenteras, dvs. i vissa fall ansvarar utfärdaren för att fotografera eller ta fingeravtryck av individen, i andra fall kan individen ta med

[3] Att ett identitetskort har SIS-märkning innebär att det tillverkas enligt en viss standard av en licensierad tillverkare och utfärdas av en godkänd utfärdare. Vanliga utfärdare är bankerna men det förekommer också att större företag har tillstånd att utfärda sådana identitetshandlingar till sina anställda.

[4] Passlagen (1978:302), förordningen (2005:661) om nationellt identitetskort, lagen (2015:899) om identitetskort för folkbokförda i Sverige, körkortsförordningen (1998:980), E-legitimationsnämndens tillitsramverk för Svensk e-legitimation, ref.nr: ELN-0700-v1.3.

[5] Skatteverkets föreskrifter om identitetskort, SKVFS 2009:14 och Rikspolisstyrelsens föreskrifter och allmänna råd om polismyndigheternas hantering av pass och nationellt identitetskort, RPSFS 2009:14, FAP 530-1.

[6] 8 kap. 3 § körkortsförordningen (1998:980) samt Transportstyrelsens föreskrifter om utlämnande av körkort, TSFS 2014:17.

sig eller skicka in ett fotografi som har tagits av annan men som ofta ska uppfylla vissa kriterier.[7]

Utredningen bedömer att det inte är alla processer som leder fram till identitetshandlingar som innehåller grundidentifiering. För att en process ska innehålla grundidentifiering bedömer utredningen att vissa styrande principer ska vara uppfyllda. Dessa principer är följande:

- ansökan om en identitetshandling måste göras vid ett personligt besök hos den utfärdande aktören,
- individen ska styrka sin identitet på ett tillförlitligt sätt,
- den utfärdande aktören ansvarar för att dokumentera fysiska kännetecken genom att åtminstone ta ett fotografi av individen, samt
- identitetshandlingen ska lämnas ut vid ett personligt besök hos utfärdaren.

Utredningen bedömer att det är staten som ska ansvara för grundidentifiering av individer i Sverige. Detta ställningstagande bygger dels på att det redan finns statliga identifieringsprocesser som innefattar grundidentifiering som uppfyller de principer som utredningen bedömer ska gälla, *dels* på att statliga myndigheter finns tillgängliga över stora delar av landet. Utredningen konstaterar att Polismyndigheten och Skatteverket i dag är de myndigheter som utfärdar identitetshandlingar i enlighet med de principer som utredningen beskrivit ovan. De båda myndigheterna har en god spridning över landet och redan i dag etablerade processer för ansökan och utlämnande, liksom personal som är utbildad för att lösa uppgiften.

Utredningen lämnar inte några förslag på vilka myndigheter som ska ansvara för grundidentifieringen. Detta eftersom 2017 års ID-kortsutredning, som ska lämna sitt betänkande senast den 29 mars 2019, har till uppgift att se över vilka identitetshandlingar som ska finnas i Sverige och även vilka myndigheter som ska ansvara för att ge ut dessa identitetshandlingar.[8]

[7] 6 § passlagen (1978:302), 3 § andra stycket förordningen (2005:661) om nationellt identitetskort, 2 § lagen (2015:899) om identitetskort för folkbokförda i Sverige, samt 3 kap. 15 § körkortsförordningen (1998:980) och https://www.swedbank.se/privat/kort-och-betalningar/id-kort-och-bankid/id-kort/index.htm#!/OID_234910_SV, 2017-12-17.
[8] 2017 års ID-kortsutredning, Ju 2017:12.

12 Statlig elektronisk identitetshandling

12.1 Vad är en elektronisk identitetshandling?

En elektronisk identitetshandling används av individer för att identifiera sig och av den som ska kontrollera identiteten för att få bekräftat vem som har identifierat sig. Det finns olika sätt att för lagstiftningsändamål beskriva vad en elektronisk identitetshandling är. Man kan förhålla sig till modeller och tekniska specifikationer. Det är en utmaning att undvika att genom en för detaljrik beskrivning skapa inlåsningseffekter där teknisk utveckling försvåras. Den beskrivning av vad en elektronisk identitetshandling är som finns i propositionen Myndigheters tillgång till tjänster för elektronisk identifiering utgår exempelvis från en viss teknisk lösning:

> De e-legitimationer som i dag används i den offentliga förvaltningens e-tjänster består av en privat och en publik krypteringsnyckel med tillhörande elektroniskt certifikat. Den publika nyckeln finns i certifikatet och den privata nyckeln finns hos användaren. En e-legitimation som innehåller ett certifikat gör det också möjligt för användaren att förse uppgifter med en elektronisk motsvarighet till en underskrift, dvs. en elektronisk signatur. Med hjälp av en sådan e-legitimation kan innehavaren alltså både legitimera sig och signera uppgifter elektroniskt i e-tjänster. En e-legitimation kan i dag utfärdas antingen som en fil som innehavaren kan lagra på hårddisk (mjuk lagring) eller i form av en fysisk bärare (hård lagring), exempelvis ett s.k. smart kort.
>
> Det elektroniska certifikatet är en informationsstruktur som innehåller uppgifter som utfärdaren har valt att koppla till e-legitimationen, såsom närmare uppgifter om innehavaren, certifikatets unika nummer, vem som är utfärdare och den publika krypteringsnyckeln. Certifikatet är signerat av den som har utfärdat e-legitimationen.[1]

[1] Prop. 2012/13:123, s. 17.

Utredningen anser att det är viktigt att så långt det är möjligt försöka beskriva elektronisk identifiering på ett teknikneutralt sätt.

12.1.1 Vem du är …

En elektronisk identitetshandling består av unika uppgifter om en viss individ.[2] Hur dessa unika uppgifter är sammansatta modellmässigt skiljer sig åt, beroende på utfärdare av elektronisk identitetshandling. Utredningen vill här framhålla att beskrivningen endast utgår från uppgifterna om individen.[3] En elektronisk identitetshandling kan *användas* av innehavaren för att på ett säkert sätt identifiera sig gentemot exempelvis e-tjänster. När en individ vill använda sin elektroniska identitetshandling i en viss e-tjänst, måste den som har e-tjänsten ställa en fråga till utfärdaren av den elektroniska identitetshandlingen om individen är den som hon eller han utger sig för att vara. En bekräftelse på att det är just den individen levereras i ett s.k. identitetsintyg.

12.1.2 … inte detsamma som vad du får göra

Det är viktigt att särskilja identitetsuppgifter från vad individen får göra. Identitetsuppgifter är beständiga, medan behörigheter löpande kan ändras. Med andra ord är det viktigt att inte låta det som kallas för behörighets- och åtkomstuppgifter ingå i den elektroniska identitetshandlingen. Sådana uppgifter finns i stället i de tjänster som individen identifierar sig mot och det är den som tillhandahåller tjänsterna som bestämmer vilken behörighet individen har. Genom att särskilja identitetsuppgifter och organisatorisk tillhörighet, roll eller ställning underlättas möjligheter för individer att förflytta sig över organisationsgränser samt att ändra roll och arbetsuppgifter utan att den elektroniska identitetshandlingen för den skull behöver bytas ut.

[2] Se K6.4 i Tillitsramverk för Svensk e-legitimation, Ref.nr: ELN-0700-v1.3. Detta krav innebär att fiktiva personnummer eller samordningsnummer inte får förekomma (se Vägledning för uppfyllande av tillitsramverkets krav för Svensk e-legitimation, version 2014-05-02 dnr 2 00 255001-17/9513, s. 19).

[3] Jfr s.k. färdiga elektroniska handlingar i 2 kap. 3 § andra stycket tryckfrihetsförordningen samt resonemang i prop. 2001/02:70, s. 22, Offentlighetsprincipen och informationstekniken och SOU 2010:4, allmänna handlingar i elektronisk form, s. 33, SOU 2010:4, allmänna handlingar i elektronisk form, s. 33.

Utredningen återkommer till detta i kapitlet Arbetstagare, student, ställföreträdare – och elektronisk identifiering.

12.2 Begreppet elektronisk identitetshandling

Utredningen bedömer:
att det är missvisande att beskriva elektroniska identitetshandlingar på olika tillitsnivåer med ett och samma begrepp.

Utredningen föreslår:
att regeringen ger digitaliseringsmyndigheten i uppdrag att arbeta fram olika begrepp för att beskriva elektroniska identitetshandlingar på olika tillitsnivåer.

E-legitimationsnämnden har tagit fram ett tillitsramverk[4] som bygger på internationell standard och andra internationella ramverk. Det svenska tillitsramverket som togs fram innan EU:s tillitsramverk inom ramen för eIDAS-förordningen med följd att det svenska tillitsramverket har en något högre högsta tillitsnivå än eIDAS-förordningen.[5]

Vissa regler i tillitsramverket skiljer sig åt, beroende på vilken tillitsnivå en viss elektronisk identitetshandling (i tillitsramverket benämnd e-legitimation) har. Alla elektroniska identitetshandlingar utfärdas efter ansökan. För alla elektroniska tillitsnivåer ska också en utfärdare kontrollera att uppgifterna i ansökan om sökanden är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register.[6] Med officiellt register avses bl.a. SPAR.[7]

I tillitsramverket finns regler som tar sikte på hur en individ, som ansöker om en elektronisk identitetshandling, ska identifieras och hur en elektronisk identitetshandling ska lämnas ut till individen. Huvudregeln är att detta ska göras vid personliga besök. För vissa

[4] Tillitsramverk för Svensk e-legitimation, Ref.nr: ELN-0700-v1.3.
[5] Fortsatt försörjning av tjänster för e-legitimering och e-underskrift, E-legitimationsnämnden, dnr: 131 645711-15/9513, 2016-10-25, s. 23.
[6] Se punkten K5.8 i E-legitimationsnämndens tillitsramverk.
[7] Lagen (1998:527) om det statliga personadressregistret och Vägledning till uppfyllande av tillitsramverkets krav för Svensk e-legitimation.

tillitsnivåer är det möjligt att både ansöka om och få en elektronisk identitetshandling utlämnad till sig på distans.[8]

Det finns alltså ingen enhetlig process för utfärdande av elektroniska identitetshandlingar. Det leder till att begreppet elektronisk identitetshandling har karaktären av ett samlingsnamn för alla tillitsnivåer, trots att det ställs olika krav på en identitetshandling beroende på tillitsnivå. Utredningen bedömer att det är missvisande att beskriva elektroniska identitetshandlingar på olika tillitsnivåer med ett och samma begrepp. Därtill kommer också den bedömning som utredningen gör i följande avsnitt, som innebär att elektroniska identitetshandlingar på åtminstone tillitsnivå 3 och 4 utgör elektroniska urkunder. Elektroniska identitetshandlingar på dessa tillitsnivåer bör således skiljas ut begreppsmässigt. En tanke kan vara att reservera begreppet elektronisk identitetshandling för tillitsnivå 3 och 4, medan det på lägre tillitsnivåer kan användas ett annat begrepp. Utredningen föreslår därför att digitaliseringsmyndigheten arbetar fram andra begrepp för att beskriva elektroniska identitetshandlingar på olika tillitsnivåer.

12.3 Elektronisk identitetshandling är en värdehandling

Av 2 kap. 3 § tryckfrihetsförordningen[9] följer att med handling förstås framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. Handlingsbegreppet omfattar alltså s.k. konventionella handlingar (framställning i skrift eller bild) och elektroniska handlingar (upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel). Elektroniska handlingar kan vara sammanställningar (potentiella handlingar) eller s.k. färdiga elektroniska handlingar.[10] Med en färdig elektronisk handling menas en sådan elektronisk handling som utställaren har gett ett bestämt, fixerat innehåll som går att återskapa gång på gång.

Utredningen menar att elektroniska identitetshandlingar, givet vissa förutsättningar, kan vara elektroniska urkunder. I brottsbalken

[8] Se punkterna K5.10–K5.12 i E-legitimationsnämndens tillitsramverk.
[9] Tryckfrihetsförordningen (1949:105).
[10] Se mer om färdiga elektroniska handlingar i prop. 2001/02:70, s. 22, Offentlighetsprincipen och informationstekniken och SOU 2010:4, Allmänna handlingar i elektronisk form, s. 33.

beskrivs en elektronisk urkund som en handling som upprättats till bevis eller annars är av betydelse som bevis och som har en utställarangivelse och originalkaraktär.[11]

En utställarangivelse ska enligt propositionen ha en inte obetydlig grad av säkerhet. Utställarangivelser i ordbehandlingsprogram och namn eller adressangivelser i ordinära e-postmeddelanden bedöms inte typiskt sett förtjäna tilltro. Vanlig e-post är således inte urkunder. Om en datafil lagrad på ett medium inte med säkerhet kan knytas till en utställare saknar den originalkaraktär och därmed urkundskvalitet.[12]

En elektronisk identitetshandling är avsedd att användas för att peka ut en viss individ med hög grad av säkerhet. Utredningen bedömer att åtminstone elektroniska identitetshandlingar på tillitsnivå 3 och 4 är att betrakta som elektroniska urkunder. Därmed är de också värdehandlingar, som användaren bör hantera med samma försiktighet som deras fysiska motsvarigheter. Av brottsbalken följer vidare att den som obehörigen, genom att skriva eller på liknande sätt ange en annan persons namn eller på annat sätt, framställer en falsk urkund eller ändrar eller fyller ut en äkta urkund döms, om åtgärden innebär fara i bevishänseende, för urkundsförfalskning.[13]

12.4 Identifiering med en elektronisk identitetshandling

En fysisk eller mobil bärare av en elektronisk identitetshandling kan vara ett s.k. smartkort som kan lagra elektronisk information i ett chip på kortet.[14] En mobil bärare är exempelvis en smarttelefon, surfplatta eller dator. Då finns den elektroniska identitetshandlingen som en fil på en dator eller en applikation i mobiltelefonen.

[11] 14 kap. 1 § brottsbalken (1962:700).
[12] Kommentar till 14 kap. 3 § brottsbalken, Zeteo, 2017-12-13.
[13] Jfr Högsta domstolens dom den 22 december 2017 i mål T435-17, som rörde bevisbördan i tvistemål för invändning om att en elektronisk underskrift använts obehörigen av annan än innehavaren. Tvisten gällde en elektronisk låneförbindelse. Högsta domstolen bedömde att det var långivaren som måste visa att det är den påstådda elektroniska underskriften som har använts och att, om så sker innehavaren måste göra antagligt att användningen av underskriften skett obehörigen.
[14] Ett smartkort definieras som ett kort i fickstorlek med inbyggda kretsar som kan processa information. Detta anger att det kan ta emot indata som bearbetas och levereras som utdata. https://sv.wikipedia.org/wiki/Smartkort, 2017-12-13.

12.5 Utformning av elektroniska identitetshandlingar på olika tillitsnivåer

En elektronisk identitetshandling består, som beskrivits, av uppgifter som entydigt kan kopplas till en fysisk person. Uppgifterna ska kunna användas av individen för att identifiera sig och av den förlitande aktören för att kontrollera individens identitet. Individ och användare används i dessa sammanhang som synonyma begrepp.

Autentisering är en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form.[15] Det finns tre huvudsakliga faktorer som man använder för att individers elektroniska identitetshandlingar ska vara säkra; någonting man *vet* (i praktiken koder), någonting man *är* (biometriska uppgifter) och någonting man *har* (t.ex. en dator, koddosa, mobiltelefon eller aktivt kort).[16] Ju fler av dessa som kombineras, desto större kontroll över den elektroniska identitetshandlingen kan individen ha. Aktiveringsmekanismen och personlig kod ska utformas så att det är osannolikt att en utomstående kan forcera skyddet, ens på maskinell väg.[17] Det innebär att komplexitetskraven på den personliga koden måste utformas så att resurserna som krävs för att röja den står i proportion till den elektroniska identitetshandlingens övriga säkerhetsegenskaper, innebärande att denna del inte ska vara en svagare länk än någon annan i del i kedjan av säkerhetskontroller.[18]

Det tillitsramverk som E-legitimationsnämnden har tagit fram beskriver tillitsnivå 2, 3 och 4. Utredningen återkommer i det följande

[15] Artikel 3, punkten 5 Europaparlamentets och Rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, eIDAS-förordningen.
[16] Vägledning för uppfyllande av tillitsramverkets krav för Svensk e-legitimation, s. 17.
[17] Se K6.2 i E-legitimationsnämndens tillitsramverk.
[18] Vägledning för uppfyllande av tillitsramverkets krav för Svensk e-legitimation, s. 18. Därav framgår vidare att detta kan åstadkommas på olika sätt, t.ex.: I de fall en personlig säkerhetsmodul används, att denna blockeras efter ett visst antal felaktiga aktiveringsförsök, där antalet står i proportion till aktiveringskodens komplexitet. I de fall andra tvåfaktorslösningar än personlig säkerhetsmodul används: (i) Att aktiveringen av den elektroniska identitetshandlingen tar stor maskinkapacitet i anspråk, dvs. att processen att tillgängliggöra nyckelmaterialet går till så att ett stort antal handlingar krävs för att pröva om rätt kod angivits, och att det därmed (i normalfallet) tar orimligt lång tid att genomföra en uttömmande sökning efter rätt kod. (ii) Att den personliga kodens komplexitet i termer av längd samt kombination av versaler, gemener, siffror och specialtecken medför att uttömmande sökning blir mycket omfattande resursmässigt att genomföra. (iii) Att en del i aktiveringsförfarandet görs direkt mot utfärdaren och att denne därmed kan spärra den elektroniska identiteten efter ett visst antal felaktiga försök.

till dessa tillitsnivåer. Tillitsnivå 1 kan vara ett konto som någon registrerar själv på internet, utan att styrka sin identitet. Den tillitsnivån omfattas alltså inte av E-legitimationsnämndens tillitsramverk.

12.5.1 Tillitsnivå 2

Elektroniska identitetshandlingar på tillitsnivå 2 ska enligt E-legitimationsnämndens tillitsramverk utformas så att användaren har en eller flera personliga koder som han eller hon sedan kan använda för att styrka sin identitet.[19] Med koder avses lösenord, lösenfraser, sifferkombinationer eller annan informationsmängd som inte är knuten till en särskild utrustning eller programvara.[20] Detta är alltså någonting man *vet*.

12.5.2 Tillitsnivå 3

Elektroniska identitetshandlingar på tillitsnivå 3 ska enligt E-legitimationsnämndens tillitsramverk utformas enligt en sådan tvåfaktorsprincip som består dels av elektroniskt lagrad information som användaren ska inneha, dels av något som användaren ska bruka för att aktivera den elektroniska identitetshandlingen.[21] En elektronisk identitetshandling på tillitsnivå 3 kan finnas på en fysisk eller en mobil bärare.

12.5.3 Tillitsnivå 4

Elektroniska identitetshandlingar på tillitsnivå 4 ska enligt E-legitimationsnämndens tillitsramverk utformas enligt en sådan tvåfaktorsprincip som består dels av *en personlig säkerhetsmodul* som användaren ska inneha, dels av *det som användaren ska bruka* för att aktivera säkerhetsmodulen.[22] En elektronisk identitetshandling på tillitsnivå 4 måste finnas på en fysisk bärare, alltså ett exempelvis ett s.k. smartkort.

[19] Se K6.1 i E-legitimationsnämndens tillitsramverk.
[20] Vägledning för uppfyllande av tillitsramverkets krav för Svensk e-legitimation, s. 17.
[21] Vägledning för uppfyllande av tillitsramverkets krav för Svensk e-legitimation, s. 17.
[22] Se K6.1 i E-legitimationsnämndens tillitsramverk.

12.5.4 Gemensamt för tillitsnivå 3 och 4

I de fall tvåfaktorsautentisering krävs (nivå 3 och 4) bör koder kombineras med innehav (fysisk kontroll) av en lagrad datastruktur. Av den anledningen är personliga koder den huvudregel som bör tillämpas, men andra lösningar kan godtas då säkerheten i övrigt upprätthålls genom andra kompletterande kontroller.[23] Utöver dessa krav finns det också krav i tillitsramverket på att det ska finnas möjlighet för användaren att på eget initiativ kunna byta eller begära ny personlig kod.

12.6 Processer för utfärdande av elektroniska identitetshandlingar

Av E-legitimationsnämndens tillitsramverk följer att processerna för utfärdande av elektroniska identitetshandlingar skiljer sig åt, beroende på vilken tillitsnivå en elektronisk identitetshandling har. Tillitsramverket beskriver olika processer för såväl identitetskontrollen av en individ som ansöker om en elektronisk identitetshandling, som för utlämnande av den elektroniska identitetshandlingen till individen.

En elektronisk identitetshandling utfärdas enligt tillitsramverket efter ansökan från en individ. Individen kallas då sökande.

12.6.1 Identifiering

Utgångspunkten är att utfärdare ska kontrollera sökandens identitet vid ett personligt besök, på likvärdigt sätt som vid utgivning av en fullgod identitetshandling. Med detta avses att identitetskontrollen följer en dokumenterad process och utförs av särskilt utbildad personal i utfärdarens organisation. Det förväntas också att identitetskontrollen i samband med utfärdande av den elektroniska identitetshandlingen grundas i att individen har en fullgod identitetshandling med vilken hon eller han kan styrka sin identitet.[24]

[23] Vägledning för uppfyllande av tillitsramverkets krav för Svensk e-legitimation, s. 18.
[24] Vägledning till uppfyllande av tillitsramverkets krav för Svensk e-legitimation, s. 14.

För elektroniska identitetshandlingar på tillitsnivå 2 och 3 är det emellertid möjligt att kontrollera en individs identitet på distans enligt de närmare bestämmelserna i tillitsramverket.[25]

12.6.2 Utlämnande

Även förfarandet vid *utlämnande* av en elektronisk identitetshandling skiljer sig åt beroende på tillitsnivå. Liksom vid identifiering vid ansökan om en elektronisk identitetshandling medger tillitsramverket att elektroniska identitetshandlingar på tillitsnivå 2 och 3 kan lämnas ut på distans under vissa förutsättningar. Identitetshandlingar på tillitsnivå 4 kan inte lämnas ut på distans.[26]

Utlämnandet av en elektronisk identitetshandling är en särskilt kritisk fas i utfärdandeprocessen. Det kan finnas risker att den som ska lämna ut en elektronisk identitetshandling utsätts för otillbörliga påtryckningar, liksom att det inte genomförs en tillräckligt säker identitetskontroll i samband med utlämnandet av en elektronisk identitetshandling till en individ.[27]

12.7 En statlig elektronisk identitetshandling

Utredningen föreslår:
att staten utfärdar en elektronisk identitetshandling
att staten skapar en säker grundidentifieringsprocess som kan användas av andra aktörer.

Många individer i Sverige har redan en eller flera elektroniska identitetshandlingar. Befolkningen är, som grupp betraktad, van att identifiera sig elektroniskt.

På den svenska marknaden för elektroniska identitetshandlingar finns en dominant marknadsaktör; BankID. Det finns uppgifter om

[25] Se K5.11 i E-legitimationsnämndens tillitsramverk. För att kunna ge ut en elektronisk identitetshandling på tillitsnivå 3 på distans, krävs att utfärdaren själv står en betydande rättslig eller ekonomisk risk kopplad till distansrelationen. Detta innebär i normalfallet att utfärdaren tillhandahåller en e-tjänst gentemot sökanden, där konsekvenserna för utfärdaren vid en felaktig identifiering kan komma att leda till betydande skador.
[26] Se K.6.6 i E-legitimationsnämndens tillitsramverk.
[27] Vägledning för uppfyllande av tillitsramverkets krav för Svensk e-legitimation, s. 20 ff.

att cirka 7,5 miljoner personer har BankID och att antalet användningstillfällen med BankID uppskattas till *2,5 miljarder* under 2017. När det gäller den offentliga sektorns del i den totala användningen kan dock konstateras att den är 7,1 procent, varav kommuner och landsting står för 1,9 procent och statliga myndigheter för 5,2 procent.[28] Utredningen anser att det är på grund av BankID som den svenska befolkningen har en utbredd vana att identifiera sig elektroniskt och att svenska e-tjänster är förhållandevis välutvecklade.

Trots den goda vanan hos befolkningen att identifiera sig elektroniskt finns det utmaningar på den svenska marknaden för elektroniska identitetshandlingar.

En utmaning är att en aktör har en så stor marknadsandel (jfr statistiken från BankID ovan). Det leder till att andra aktörer har svårare att ta marknadsandelar.

En annan utmaning är grundidentifieringen. För att elektroniska identitetshandlingar ska vara tillförlitliga måste aktörer på marknaden vara säkra på att en elektronisk identitetshandling pekar på rätt individ. En kritisk fas i utfärdandet av elektroniska identitetshandlingar är grundidentifieringen, dvs. den identifiering som görs när en individ ska styrka sin identitet för utfärdande av en identitetshandling. En annan kritisk fas är i samband med utlämnandet, dvs. när en individ hämtar ut sin elektroniska identitetshandling.[29] Det är viktigt att dessa kritiska faser hålls samman av en ansvarig aktör, för att minska risken för att en individ får ut en identitetshandling med uppgifter om en annan person än honom eller henne själv. Krav i tillitsramverket på fysisk identitetskontroll medför att utfärdare måste finnas tillgängliga på många ställen i landet och ha personal som kan utföra en identitetskontroll på ett tillförlitligt sätt.[30]

Ytterligare en aspekt är att det ur ett beredskaps- och kontinuitetsperspektiv finns behov av riskspridning genom att etablera ett komplement till det i dag dominerande systemet med bankutgivna elektroniska identitetshandlingar.

Det är också önskvärt att ha en elektronisk basidentitet som individen kan vara säker på kan användas för att identitetsväxla. Det innebär att individen kan använda en elektronisk identitetshandling

[28] https://www.bankid.com/assets/bankid/stats/2017/statistik-2017-10.pdf.
[29] Vägledning för uppfyllande av tillitsramverkets krav för Svensk e-legitimation, s. 20.
[30] Framtida spelplan för e-legitimering, förstudierapport på uppdrag av E-legitimationsnämnden, version 1, 2017-02-23 s. 14.

på tillitsnivå 3 och 4 som underlag vid ansökan om en annan elektronisk identitetshandling på tillitsnivå 3 eller lägre. Det är dessutom önskvärt att veta att det ska finnas minst en svensk elektronisk identitetshandling som kan anmälas för användning för gränsöverskridande identifiering enligt eIDAS-förordningen[31] och det är inte givet att bankerna kommer att vilja anmäla BankID eller Mobilt BankID för detta ändamål.

Utredningen menar att det är ett statligt ansvar att grundidentifiera individer och utfärda fysiska identitetshandlingar. Det är viktigt att hålla samman grundidentifieringen med utfärdandet av en elektronisk identitetshandling. Mot den bakgrunden bedömer utredningen att staten ska utfärda en elektronisk identitetshandling. En sådan statlig elektronisk identitetshandling ska ses som ett grundläggande underlag som kan användas antingen för identifiering i e-tjänster, eller – och mest troligt – som underlag för att kunna ansöka om andra elektroniska identitetshandlingar. Syftet med en statlig elektronisk identitetshandling är alltså att skapa förutsättningar för andra aktörer att utnyttja de resurser och den kompetens som staten har när det gäller att kontrollera individers identitet. Syftet är vidare att garntantera att Sverige kan anmäla en elektronisk identitetshandling för användning i Europa enligt eIDAS-förordningen.

Krav på den statliga elektroniska identitetshandlingen

Utredningen bedömer att de krav som ska ställas på en statlig elektronisk identitetshandling är följande.

- En statlig elektronisk identitetshandling ska vara en säker och tillförlitlig elektronisk identitetshandling på den högsta tillgängliga tillitsnivån.
- En statlig elektronisk identitetshandling ska vara en stabil lösning, som inte är beroende av att individer själva har vare sig dator, kortläsare eller mobiltelefon.
- En statlig elektronisk identitetshandling ska kunna användas hos alla offentliga myndigheter, men tanken är inte att en statlig

[31] Se vidare avsnitt 18.2.

elektronisk identitetshandling ska vara den enda elektroniska identitetshandlingen som individer har.

- En statlig elektronisk identitetshandling ska finnas på en fysisk bärare.
- En statlig elektronisk identitetshandling ska kunna användas som en back-up-lösning för individer om deras andra elektroniska identitetshandlingar fallerar.

12.7.1 Särskild grundidentifiering eller utnyttja befintlig?

Utredningen bedömer:
att det är lämpligt att utnyttja befintliga grundidentifieringar i staten för att utfärda en elektronisk identitetshandling.

Utredningen konstaterar:
att frågan om vilken eller vilka fysiska identitetshandlingar som ska bära den statliga elektroniska identitetshandlingen hanteras av 2017 års ID-kortsutredning.

Utredningen bedömer att det ska vara ett offentligt åtagande att grundidentifiera individer och utfärda en elektronisk identitetshandling. För att åstadkomma detta finns det enligt utredningen i huvudsak två olika tillvägagångssätt. Det ena är att etablera en särskild grundidentifiering i staten som resulterar i en elektronisk identitetshandling, som fästs på en nyetablerad fysisk bärare. För denna nya grundidentifiering skulle någon statlig myndighet ansvara. Det andra är att utnyttja befintliga statliga grundidentifieringar.

När det gäller det första alternativet bedömer utredningen att det inte är aktuellt. Att etablera en helt ny process för att utfärda en elektronisk identitetshandling, med tillkommande ansvar för en myndighet och dessutom att få tillräcklig spridning på den elektroniska identitetshandlingen hos befolkningen, är vare sig lämpligt eller ett effektivt sätt att hantera de offentliga resurserna.

Utredningen anser i stället att befintliga statliga grundidentifieringar ska utnyttjas. Det medför att de fysiska identitetshandlingar som staten utfärdar bör vara bärare av den statliga elektroniska identitetshandlingen.

De befintliga statliga processer som innefattar grundidentifiering och som utredningen bedömer lämpliga, utifrån de principer som utredningen bedömer ska gälla och det nuvarande regelverket, är de som gäller för passet, det nationella identitetskortet och identitetskortet för folkbokförda i Sverige.[32]

I augusti 2017 tillsattes 2017 års ID-kortsutredning, med uppdrag att utreda och lämna förslag till förändringar av de krav och rutiner som gäller för svenska identitetshandlingar. Av direktiven framgår att den utredningen ska föreslå hur antalet identitetshandlingar och utfärdare ska begränsas, analysera och föreslå hur verifieringen av äktheten och giltigheten av identitetshandlingar kan förbättras, utreda och vid behov föreslå hur identitetshandlingar bör utfärdas och utformas för att bli säkrare samt analysera och ta ställning till om fysiska identitetshandlingar bör innehålla en e-legitimation på högsta tillitsnivå.

Utredningen har samrått med 2017 års ID-kortsutredning. Med anledning av 2017 års ID-kortsutrednings uppdrag avstår utredningen från att lämna förslag på vilken myndighet som ska utfärda statliga elektroniska identitetshandlingar, eller vilken alternativt vilka fysiska bärare som sådana elektroniska identitetshandlingar ska finnas på.

12.7.2 Den statliga elektroniska identitetshandlingen ska vara på den högsta tillitsnivån

Utredningen bedömer:
att staten inte ska utfärda mobila elektroniska identitetshandlingar.

Utredningen föreslår:
att statliga elektroniska identitetshandlingar ska vara på den högsta tillitsnivån, i dag tillitsnivå 4.

[32] Passlagen (1978:302) med tillhörande passförordningen (1979:664), förordningen (2005:661) om nationellt identitetskort och lagen (2015:899) om identitetskort för folkbokförda i Sverige med tillhörande förordningen (2015:904) om identitetskort för folkbokförda i Sverige.

Tillitsnivån förutsätter fysisk bärare

Tillitsnivå 4 förutsätter i dag att den elektroniska identitetshandlingen finns på en fysisk bärare, exempelvis ett smartkort. Utredningen anser att någon eller några av de befintliga utfärdandeprocesser som innefattar grundidentifiering ska utnyttjas för att utfärda en elektronisk identitetshandling. Ur dessa processer kommer fysiska identitetshandlingar som kan, eller bör kunna, bära en elektronisk identitetshandling.

Utredningen lämnar inte förslag på en mobil statlig elektronisk identitetshandling

Utredningen har tidigare beskrivit att en elektronisk identitetshandling kan finnas som en fil på en dator eller en applikation i mobiltelefonen. Bland de som i dag använder sig av BankID, är det 90,9 procent som har mobilt BankID. Antalet utfärdade mobila BankID var i september 2017 nästan 6,5 miljoner, jämfört med i januari 2015 när det var drygt 3 miljoner.[33] De mobila lösningarna för elektroniska identitetshandlingar är alltså tilltalande för många. De erbjuder möjligheter att sköta sina ärenden gentemot banker, statliga myndigheter och andra aktörer var som helst.

Genom en mobil lösning för den statliga elektroniska identitetshandlingen skulle användandet givetvis underlättas. Utredningen bedömer emellertid den statliga elektroniska identitetshandlingen ska vara ett komplement och inte konkurrent till redan existerande eller kommande mobila plattformar. Det bästa sättet att stödja innovation är att lämna öppet för olika aktörer att presentera sina lösningar och låta brukarnas val avgöra. Ur ett nationellt säkerhetspektiv är det viktigt att undvika starka beroenden av enskilda aktörer och tekniska lösningar. Mobilitetstrenden i Sverige är stark[34] och många invånare i Sverige har en smart mobil, surfplatta och/eller dator. Här finns det utrymme för fler aktörer.

[33] Statistik från BankID, oktober 2017. https://www.bankid.com/om-oss/statistik

[34] Internetstiftelsen i Sverige (IIS) har konstaterat att 85 procent av befolkningen har tillgång till en smart mobil, vilket är en ökning i förhållande till år 2016 då 81 procent hade tillgång till en smart mobil. Vidare har 93 procent tillgång till en dator hemma, IIS rapport Svenskarna och internet 2017 – undersökning om svenskarnas internetvanor, s. 10.

12.7.3 Ska ansvariga statliga myndigheter själva utveckla den elektroniska identitetshandlingen?

Utredningen föreslår:
att de statliga myndigheter som ges i uppdrag att tillhandahålla en statlig elektronisk identitetshandling också ges i uppdrag att samverka i genomförandet av detta uppdrag.
att den statliga elektroniska identitetshandlingen ska vara statlig egendom och att ansvariga statliga myndigheter ska kunna bestämma över dess användning, oavsett om de tillhandahåller den själva eller upphandlar den.

Polismyndigheten ansvarar för att utfärda pass och nationella identitetskort. Skatteverket ansvarar för att utfärda identitetskort för folkbokförda. Varken Polismyndigheten eller Skatteverket tillverkar de bärare av identitetshandlingarna som passet, det nationella identitetskortet eller identitetskortet för folkbokförda finns på. Dessa bärare upphandlas av respektive myndighet.

På Skatteverkets identitetskort för folkbokförda finns en elektronisk identitetshandling. I dag utfärdas den av AB Svenska Pass och tidigare av Telia. Den elektroniska identitetshandlingen är upphandlad av Skatteverket, men utfärdas av AB Svenska Pass i eget namn.

Utredningen lämnar inte förslag på vilka statliga myndigheter som ska utfärda en elektronisk identitetshandling. Oavsett vilken myndighet det blir bedömer utredningen att de statliga myndigheter som ges i uppdrag att ta fram en statlig elektronisk identitetshandling måste samverka om hur den utformas. Det kan finnas olika leverantörer av fysiska identitetshandlingar, men knappast mer än en leverantör av den statliga elektroniska identitetshandlingen. Det är viktigt att den statliga elektroniska identitetshandlingen ges ut under ett enhetligt namn. Dessutom menar utredningen att det är de ansvariga myndigheterna som, oavsett leverantör av den elektroniska identitetshandlingen, måste kunna bestämma över hur den elektroniska identitetshandlingen får användas. Utredningen lämnar också förslag om att den statliga elektroniska identitetshandlingen ska följa det tillitsramverk och de tekniska specifikationer som digitaliseringsmyndigheten tar fram enligt förslaget till lag om infrastruktur och kvalitetsmärket Svensk elektronisk identitetshandling. Se mer om det nedan.

12.7.4 Den statliga elektroniska identitetshandlingen – en del av en fysisk identitetshandling eller en egen handling?

Utredningen föreslår:
att den statliga elektroniska identitetshandlingen ska särregleras i förhållande till de författningar som reglerar dess fysiska bärare.

Den statliga elektroniska identitetshandlingen ska utformas på ett sätt så att den blir en elektronisk urkund. Den ska därmed vara en egen handling, som använder en fysisk identitetshandling som bärare. Den elektroniska identitetshandlingen kräver emellertid tekniska hjälpmedel för att kunna användas för identifiering. Den går inte att uppfatta okulärt. Det finns därför enligt utredningens bedömning goda skäl att särreglera den statliga elektroniska identitetshandlingen, och inte låta den ingå som en delmängd i informationen på fysiska identitetshandlingar.

Utredningen bedömer att den statliga elektroniska identitetshandlingen måste omgärdas av en egen författningsreglering Detta för att veta vilka uppgifter om en individ som samlas in i grundidentifieringsprocessen i syfte att ingå i respektive identitetshandling.

12.7.5 Den statliga elektroniska identitetshandlingen och eIDAS-förordningen

Utredningen föreslår:
att den statliga elektroniska identitetshandlingen ska anmälas för gränsöverskridande identifiering (användning inom Europa) enligt eIDAS-förordningen.

Den statliga elektroniska identitetshandlingen som utredningen föreslår bör vara rustad för användningsområden som kommer att utvecklas inom den närmsta framtiden. Genom eIDAS-förordningen kommer individer att kunna kommunicera med myndigheter i andra medlemsstater på ett enklare sätt än vad som hittills varit möjligt. Det ligger i svenska medborgares intresse att denna möjlighet realiseras. Utredningen återkommer till vilka användningsområden som

är tänkbara. Situationen kan jämföras med att staten utfärdar pass till svenskar som vill resa utomlands.

För att säkerställa att det ska finnas tillgång till åtminstone en sådan elektronisk identitetshandling anser utredningen att det offentliga åtagandet när det gäller den statliga elektroniska identitetshandlingen ska omfatta att den ska kunna användas för gränsöverskridande identifiering.

Det finns även säkerhetsskäl för att Sverige bör anmäla en statligt utfärdad elektronisk identitetshandling för gränsöverskridande identifiering. Mer om detta i kapitel 18.

12.8 Lag om statlig elektronisk identitetshandling

Utredningen föreslår:
att det införs en lag om statlig elektronisk identitetshandling.
att målgruppen för den statliga elektroniska identitetshandlingen ska vara svenska medborgare och de som är folkbokförda i Sverige.

Förslaget genomförs genom lagen om statlig elektronisk identitetshandling.

Utredningen föreslår en lag om statlig elektronisk identitetshandling. Utöver att reglera vad en statlig elektronisk identitetshandling är, samt hur den får användas, föreslår utredningen bl.a. att alla offentliga myndigheter som kräver att individer ska identifiera sig elektroniskt ska godkänna identifiering med den statliga elektroniska identitetshandlingen.

Målgruppen för en statlig elektronisk identitetshandling kan delas in på olika sätt. Indelning kan göras utifrån individers *behov.* Då framförs oftast att individer behöver en elektronisk identitetshandling för sina privata ärenden och en annan som de använder i tjänsten. En annan indelning, som delvis överlappar, är vem individen är *i relation till något annat objekt*, exempelvis relationen individen har i förhållande till staten, en annan individ eller en organisation. En tredje indelning är vad individen har *rätt att göra*, exempelvis framföra ett fordon eller utöva en viss yrkesroll.

Utredningen föreslår att målgruppen för en statlig elektronisk identitetshandling ska vara densamma som målgruppen för de fysiska

identitetshandlingar som staten utfärdar, och vars primärsyfte *inte* är att utvisa en viss behörighet. Utredningen bedömer att det bör krävas att en individ har en viss form av anknytning till det svenska samhället för att få en statlig elektronisk identitetshandling. För de fysiska identitetshandlingarna bedömde 2007 års id-kortsutredning att personer som saknar personnummer inte har en sådan anknytning och därför inte skulle vara föremål för en statligt utfärdad fysisk identitetshandling.[35] Utredningen instämmer i den bedömningen. Det innebär att målgruppen för den statliga elektroniska identitetshandlingen bör vara de som är svenska medborgare och de som är folkbokförda i Sverige. Utanför den målgruppen faller således exempelvis arbetstagare, skolelever och individer med vissa behörigheter. Utredningen beskriver mer om dessa målgrupper i kapitel 15. Utredningens förslag om målgrupp för den statliga elektroniska identitetshandlingen omfattar inte heller de som har ett samordningsnummer eller är asylsökande. Det finns emellertid ingenting som hindrar att andra utfärdare av elektroniska identitetshandlingar tar fram lösningar också för individer i den målgruppen.

12.8.1 Personidentitetsuppgifter i den statliga elektroniska identitetshandlingen

Utredningen föreslår:
att det i lagen regleras vilka personidentitetsuppgifter som ska finnas i en statlig elektronisk identitetshandling.

I de författningar som reglerar passet, det nationella identitetskortet och identitetskortet för folkbokförda i Sverige saknas bestämmelser som anger vilka *uppgifter om en person* som ska finnas i respektive identitetshandling.[36] Det som regleras är i stället att sökanden (individen) ska styrka sin identitet och – när det gäller passet och det nationella identitetskortet – sitt svenska medborgarskap. Sedan finns det regler för hur detta ska gå till. Vilka uppgifter om en individ som

[35] SOU 2007:100, Id-kort för folkbokförda i Sverige, s. 78 ff.
[36] Passlagen (1978:302) med tillhörande passförordningen (1979:664), förordningen (2005:661) om nationellt identitetskort och lagen (2015:899) om identitetskort för folkbokförda i Sverige med tillhörande förordningen (2015:904) om identitetskort för folkbokförda i Sverige.

ska ingå i respektive identitetshandling framgår bl.a. av internationella regelverk och standarder på området.

Utredningen anser att det är viktigt att beskriva vilka personidentitetsuppgifter som den statliga elektroniska identitetshandlingen ska innehålla. Utredningen föreslår att den statliga elektroniska identitetshandlingen ska finnas på en fysisk bärare, som är en fysisk identitetshandling. Det innebär att grundidentifieringen är densamma för den fysiska och den elektroniska identitetshandlingen. Utredningen anser att det då är viktigt att veta vilka uppgifter om en individ som får behandlas i respektive identitetshandling. Därför bedömer utredningen att det bör regleras i lag vilka uppgifter om en individ som ska ingå i den elektroniska identitetshandlingen. Utredningen bedömer att de i lagen angivna uppgifterna är minimum och att regeringen eller den myndighet som regeringen bestämmer får besluta om att andra uppgifter också får ingå. Sådana andra uppgifter beskrivs som attribut.

Den identitetsbeteckning som huvudsakligen används för individer i Sverige i dag är personnummer. Personnumret innehåller födelsetid, födelsenummer och kontrollsiffra. För att få ett personnummer måste man vara folkbokförd i Sverige och för att bli folkbokförd måste man vara antingen svensk medborgare eller ha uppehållsrätt eller uppehållstillstånd här.[37] Utöver personnumret är ofta förnamn och efternamn viktigt för att veta vem en person är.

I en genomförandeförordning till eIDAS-förordningen[38] listas en minimiuppsättning av personidentitetsuppgifter för fysiska personer som ska finnas i en elektronisk identitetshandling som ska användas vid gränsöverskridande identifiering. Sådana uppgifter är nuvarande efternamn, nuvarande förnamn, födelsedatum och en unik identitetsbeteckning som satts samman av den utsändande staten enligt regelverk och som är mest beständig över tid. En minimiuppsättning för en fysisk person kan dessutom innehålla ett eller flera av följande valfria attribut: förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön. En närmare beskrivning av detta finns i avsnitt 18.4.

[37] 18–18 a §§ folkbokföringslagen (1991:481).
[38] Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

I sammanhanget vill utredningen uppmärksamma frågan om det ska ingå biometriska uppgifter i den elektroniska identitetshandlingen. Biometriska uppgifter om en individ, kan vara fingeravtryck eller digitala fotografier ur vilka biometrisk data kan uttolkas. Sådana uppgifter skapar förutsättningar för säkrare fysiska och elektroniska identitetshandlingar. I svenska pass finns numera biometriska uppgifter om passinnehavaren lagrad. Med hjälp av dessa går det att med större säkerhet säga att den som identifierar sig överensstämmer med den uppvisade identitetshandlingen. Det minskar också risken för att annan än innehavaren använder identitetshandlingen i bedrägligt syfte. Att använda biometriska uppgifter kan emellertid också innebära risker för den personliga integriteten.

Utredningen bedömer att det noga bör övervägas om elektroniska identitetshandlingar ska innehålla biometriska uppgifter. Frågan om identitetshandlingar ska innehålla biometriska uppgifter ingår i uppdraget till 2017 års ID-kortsutredning.

12.8.2 Den statliga elektroniska identitetshandlingen och förslaget om lag om infrastruktur för elektronisk identitetskontroll och kvalitetsmärket Svensk elektronisk identitetshandling

Utredningen föreslår:
att det i lagen anges att den statliga elektroniska identitetshandlingen ska vara på den högsta svenska tillitsnivån enligt tillitsramverket i lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling,
att elektronisk identitetskontroll av den statliga elektroniska identitetshandlingen ska utformas enligt tekniska specifikationer i lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling,
att det i lagen särskilt ska anges att den statliga elektroniska identitetshandlingen ska finnas på de fysiska identitetshandlingar som regeringen bestämmer,
att den statliga elektroniska identitetshandlingen ska ha samma giltighetstid som den fysiska identitetshandling som den finns på.

Utredningen lämnar i kapitel 14 förslag på en lag om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling. Utredningen bedömer att infrastrukturen ska bestå bl.a. av det tillitsramverk och de tekniska specifikationer som E-legitimationsnämnden ansvarar för att ta fram i dag. Utredningen bedömer att dessa delar ska författningsregleras och att digitaliseringsmyndigheten ska ges i uppdrag att utveckla och förvalta dem.

Utredningen bedömer att den statliga elektroniska identitetshandlingen ska uppfylla de krav som ställs också på andra utfärdare av elektroniska identitetshandlingar för att kunna få kvalitetsmärket Svensk elektronisk identitetshandling. Ansvaret för den statliga elektroniska identitetshandlingen kan komma att fördelas på flera statliga myndigheter beroende på vilken fysisk identitetshandling som den statliga elektroniska identitetshandlingen ska finnas på och vilka statliga myndigheter som i framtiden kan komma att utfärda sådana. Oavsett vilken statlig myndighet som ansvarar för att utfärda den statliga elektroniska identitetshandlingen ska kvalitetskraven vara desamma.

Högsta tillitsnivån och tekniska specifikationer

Utredningen föreslår att den statliga elektroniska identitetshandlingen ska vara på den högsta tillitsnivån enligt tillitsramverket samt att den ska följa de tekniska specifikationer som utredningen lämnar förslag på att digitaliseringsmyndigheten ska utveckla och förvalta. E-legitimationsnämnden har, som beskrivits, tagit fram tillitsramverk och tekniska specifikationer.

Utredningen har övervägt om det i lagen ska beskrivas vad den högsta tillitsnivån innebär. Tillitsnivåer är föremål för utveckling och ska anpassas efter de rådande standarder som finns på området (se närmare om utredningens förslag till lag om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling). Utredningen bedömer att det inte är lämpligt att i lag ange vad som krävs för vissa tillitsnivåer. Sådana bedömningar bör vara en uppgift för den statliga myndighet som utvecklar och förvaltar tillitsramverket.

De fysiska bärare som regeringen bestämmer

E-legitimationsnämndens högsta tillitsnivå, tillitsnivå 4, förutsätter som ovan beskrivits att den elektroniska identitetshandlingen finns på en fysisk bärare.

Utredningen bedömer att det är viktigt att i lagen ange att den eller de fysiska bärare som kan innehålla en statlig elektronisk identitetshandling är någon eller några av de fysiska identitetshandlingar som staten utfärdar. Detta för visa att den statliga elektroniska identitetshandlingen inte ska vara föremål för en egen grundidentifieringsprocess, utan i stället vara resultatet av samma process som för den eller de fysiska identitetshandlingar som staten utfärdar.

Som nämnts är frågan om vilka fysiska identitetshandlingar som ska finnas föremål för arbetet i 2017 års ID-kortsutredning. Utredningen avstår därför från att lämna förslag om vilken eller vilka fysiska identitetshandlingar som ska vara *bärare* av den statliga elektroniska identitetshandlingen. Utredningen avstår också från att lämna förslag på vilka *myndigheter* som ska utfärda den statliga elektroniska identitetshandlingen.

Giltighetstid

I och med att den fysiska bäraren ska vara en fysisk identitetshandling föreslår utredningen att giltighetstiden för den elektroniska identitetshandlingen ska vara densamma som för den fysiska identitetshandlingen.

12.8.3 Ansökan och utlämnande

Utredningen föreslår:
att ansökan om den statliga elektroniska identitetshandlingen ska lämnas hos den eller de myndigheter (utfärdande myndigheter) som regeringen bestämmer,
att ansökan om den statliga elektroniska identitetshandlingen ska lämnas i samband med ansökan om en fysisk identitetshandling,
att sökanden är skyldig att styrka sin identitet och övriga personuppgifter,
att ansökan ska avslås under vissa förutsättningar.

Den statliga elektroniska identitetshandlingen ska dela grundidentifieringsprocess med en fysisk identitetshandling. Utredningen har övervägt att föreslå hänvisningar till bestämmelser om ansökan i författningar som gäller för de fysiska bärarna. Eftersom frågan om vilka fysiska identitetshandlingar som ska finnas i Sverige är föremål för analys av 2017 års ID-kortsutredning som ska redovisa sitt uppdrag senast den 29 mars 2019, avstår utredningen från att hänvisa till någon befintlig författning eller att peka ut en viss identitetshandling. Hur bestämmelser om ansökan närmare ska utformas får övervägas inom ramen för arbetet i 2017 års ID-kortsutredning. Det förslag som utredningen lämnar utgår från hur liknande bestämmelser ser ut i författningar som reglerar fysiska identitetshandlingar i dag.

12.8.4 Den statliga elektroniska identitetshandlingen ska erkännas för identifiering hos alla statliga myndigheter, kommuner och landsting

Utredningen föreslår:
att alla offentliga myndigheter ska erkänna identifiering med den statliga elektroniska identitetshandlingen.

Den statliga elektroniska identitetshandlingen måste kunna användas. För att den ska kunna användas måste det ha etablerats en relation mellan den som ska kontrollera individens identitet och den som har utfärdat den elektroniska identitetshandlingen. Antingen den statliga myndigheten eller en av denne anlitad underleverantör måste under identitetshandlingens giltighetstid kunna intyga individens identitet i relation till de som ska kontrollera identiteten.

Utredningen anser att den statliga elektroniska identitetshandlingen ska fungera i alla e-tjänster där offentliga myndigheter kräver elektronisk identifiering. Den statliga elektroniska identitetshandlingen ska vara en grundbult i den offentliga förvaltningen. Den ska också vara beständig över tid och inte beroende av om en offentlig myndighets upphandling omfattar den. Utredningen föreslår att det i lag skapas en skyldighet för alla offentliga myndigheter som kräver elektronisk identifiering i sina e-tjänster att godta den statliga elektroniska identitetshandlingen.

Med en sådan bestämmelse kan det hävdas att den statliga elektroniska identitetshandlingen kan vara konkurrenshämmande. Utredningen bedömer emellertid att syftet med den statliga elektroniska identitetshandlingen inte är att etablera en konkurrent till övriga elektroniska identitetshandlingar. Den statliga elektroniska identitetshandlingen kommer exempelvis inte att uppfylla individers behov av mobila lösningar. Individer kommer därmed att vilja använda den statliga elektroniska identitetshandlingen för att växla till sig en annan identitetshandling. Utfärdaren av den andra identitetshandlingen kan då lita på att den grundidentifiering som staten gjort av individen är så säker som möjligt.

12.8.5 Den statliga elektroniska identitetshandlingen ska kunna användas som underlag för identitetskontroll av andra utfärdare

Utredningen föreslår:
att den statligt utfärdade elektroniska identitetshandlingen ska kunna användas som underlag för att utfärda andra elektroniska identitetshandlingar,
att regeringen eller de myndigheter som regeringen bestämmer får ställa upp villkor för när den statliga elektroniska identitetshandlingen får användas som underlag för ansökan om en annan elektronisk identitetshandling.

Genom att skapa en statligt kontrollerad process för grundidentifiering samt ansökan och utfärdande av den statliga elektroniska identitetshandlingen med högsta tillitsnivå menar utredningen att det finns förutsättningar för andra aktörer att lita på den statliga elektroniska identitetshandlingen. Fysiska identitetshandlingar som staten utfärdar accepteras normalt sett av andra aktörer i samhället. Utredningen anser att staten ska erbjuda en elektronisk motsvarighet till detta.

Utredningen föreslår att den statligt utfärdade elektroniska identitetshandlingen ska kunna användas som underlag för att utfärda andra elektroniska identitetshandlingar på tillitsnivåer som tillåter att sökanden identifierar sig på distans. *Individen* ska alltså kunna ansöka om *andra* elektroniska identitetshandlingar elektroniskt och

identifiera sig med den statliga elektroniska identitetshandlingen. Andra utfärdare av elektroniska identitetshandlingar kan därmed erbjuda sina kunder ett helt elektroniskt ansökningsförfarande, genom att exempelvis tillåta att en individ identifierar sig med den statliga elektroniska identitetshandlingen mot en e-tjänst i vilken ansökan och utlämnande av en annan elektronisk identitetshandling kan göras. Därmed kan andra utfärdare dra nytta av det statliga åtagandet att ansvara för grundidentifieringen.

Utredningen menar att det kommer att finnas starka incitament för individer att skaffa andra elektroniska identitetshandlingar än den statliga. Det starkaste incitamentet bedömer utredningen vara att den statliga elektroniska identitetshandlingen endast ska finnas på en fysisk bärare. Det innebär att individer som vill använda sin statliga elektroniska identitetshandling måste ha en kortläsare eller liknande för att kunna använda den. För vissa kommer det att fungera, men för många kommer det att framstå som trubbigt i jämförelse med dagens mobila lösningar.

Hur långt sträcker sig den utfärdande myndighetens ansvar för identifiering som användaren gör i samband med ansökan om en annan elektronisk identitetshandling?

Utredningen bedömer att den utfärdande myndighetens ansvar omfattar att verifiera identiteten hos en användare som ansöker om en annan elektronisk identitetshandling. Därefter har den utfärdande myndigheten inte något ansvar för den andra utfärdarens fortsatta hantering av uppgifterna om en individ. Med detta menar utredningen att myndighetens ansvar sträcker sig till att leverera det identitetsintyg som skapas när en annan utfärdare vill kontrollera en individs identitet.

Föreskriftsrätt

Regeringen eller de myndigheter som regeringen bestämmer behöver kunna ta fram närmare villkor för hur den statliga elektroniska identitetshandlingen ska få användas som underlag för andra elektroniska identitetshandlingar. Det kan exempelvis närmare behöva regleras vilka krav som ska ställas på utfärdare som vill använda den statliga

elektroniska identitetshandlingen som underlag för sin ansökan. Utredningen lämnar inte förslag på sådana föreskrifter eftersom de bör utformas utifrån vilka de ansvariga utfärdande myndigheterna blir.

12.8.6 Den statliga elektroniska identitetshandlingen och andra utfärdare

Utredningen föreslår:
att den utfärdande myndigheten ska registrera vilka andra elektroniska identitetshandlingar som har skapats med den statliga elektroniska identitetshandling som underlag.

Den statliga elektroniska identitetshandlingen är avsedd att vara en individs elektroniska basidentitetshandling. Det är viktigt att andra utfärdare och förlitande aktörer kan lita på den. Utredningen menar att den utfärdande myndigheten behöver veta vilka andra identitetshandlingar som har skapats med den statliga elektroniska identitetshandlingen som underlag. Om den statliga elektroniska identitetshandlingen spärras ska den utfärdande myndigheten informera de andra utfärdarna om detta. Syftet med att skapa en sådan kedja är att hålla kopplingen mellan basidentiteten och efterföljande identitetshandlingar intakt. På så sätt skapas ett system till vilket både förlitande aktörer och användare kan fästa tilltro.

12.8.7 Spärr av den statliga elektroniska identitetshandlingen

Utredningen föreslår:
att det i lagen införs regler om när den statliga elektroniska identitetshandlingen ska spärras,
att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om förfarandet vid spärr av statliga elektroniska identitetshandlingar.

De författningar som styr fysiska identitetshandlingar innehåller bestämmelser om när en identitetshandling ska återkallas eller spärras. Utredningen bedömer att det måste finnas en liknande bestämmelse i den nu föreslagna lagen. Bestämmelsen är utformad utifrån de mot-

svarande bestämmelser som finns i passlagen, förordningen om nationellt identitetskort och lagen om identitetskort för folkbokförda i Sverige. Denna kan dock behöva ses över av 2017 års ID-kortsutredning eftersom utformningen kan vara beroende av vilken eller vilka myndigheter som ska utfärda den statliga elektroniska identitetshandlingen och vilken eller vilka fysiska identitetshandlingar som den ska finnas på.

12.8.8 Processuella bestämmelser

Utredningen föreslår:
att beslut enligt lagen får överklagas till allmän förvaltningsdomstol,
att beslut enligt lagen gäller omedelbart, om inte något annat anges i beslutet.

Den statliga elektroniska identitetshandlingen ska som nämnts dela utfärdandeprocess med dess fysiska bärare. Utredningen har övervägt att föreslå hänvisningar till bestämmelser om ansökan i författningar som gäller för de fysiska bärarna. Eftersom frågan om vilka fysiska identitetshandlingar som ska finnas i Sverige är föremål för analys av 2017 års ID-kortsutredning, kan utredningen inte hänvisa till någon befintlig författning utan att peka ut en viss identitetshandling. Hur de processuella bestämmelserna närmare ska utformas får tas inom ramen för arbetet i 2017 års ID-kortsutredning. Det förslag som utredningen lämnar utgår från hur liknande bestämmelser ser ut i författningar som reglerar fysiska identitetshandlingar.

12.8.9 Personuppgiftsbehandling

Utredningen bedömer:
att den statliga elektroniska identitetshandlingen bör omfattas av samma registerförfattning som gäller för den fysiska identitetshandlingen.

Utredningen lämnar inte förslag på vilken fysisk identitetshandling som ska vara bärare av den statliga elektroniska identitetshandlingen.

Inte heller lämnar utredningen förslag på vilken myndighet som ska ansvara för att utfärda den statliga elektroniska identitetshandlingen. Regeringens ställningstaganden i dessa delar är beroende av de förslag som 2017 års ID-kortsutredning lämnar i sitt betänkande den 29 mars 2019.

Även om utredningen inte lämnar förslag på bärare eller utfärdande myndighet har utredningen bedömt att den grundidentifieringsprocess som leder fram till passet, det nationella identitetskortet respektive identitetskortet för folkbokförda i Sverige är tillräckligt säker även för den statliga elektroniska identitetshandlingen. Bestämmelserna om personuppgiftsbehandling för dessa identitetshandlingar finns i dag i passlagen, förordningen om nationellt identitetskort och lagen om identitetskort för folkbokförda i Sverige.

I promemorian Passdatalag[39] föreslogs en lag om behandling av personuppgifter i passmyndigheternas och Utrikesdepartementets passverksamhet. Syftet med den föreslagna lagen var att göra det möjligt för passmyndigheterna och Utrikesdepartementet att behandla personuppgifter på ett ändamålsenligt sätt i myndigheternas passverksamhet och att skydda människor från att deras personliga integritet kränks vid sådan behandling. Den föreslagna lagen var tänkt att ersätta de särregler om personuppgiftsbehandling som finns i passlagen och passförordningen. Promemorian innehöll också förslag till en förordning om behandling av personuppgifter i passmyndigheternas verksamhet avseende nationella identitetskort. Förordningen föreslogs ersätta de särregler om personuppgiftsbehandling som finns i förordningen om nationella identitetskort.

Utredningen konstaterar att promemorians förslag inte har lett till lagstiftning. Datainspektionen var positiv till förslaget om passdatalag, men pekade i sitt remissvar på några brister i förslaget.[40]

Utredningen bedömer att det är angeläget att frågan om personuppgiftsbehandling regleras. Utredningen bedömer också att det är en fråga som bör tas tillsammans med en bedömning av hur personuppgiftsbehandlingen för den fysiska bäraren av den statliga elektroniska identitetshandlingen ska utformas. Det är visserligen två olika sorters handlingar som en eller flera myndigheter kommer att utfärda (en fysisk och en elektronisk). Utredningen föreslår också att re-

[39] Ds 2015:44.
[40] Remissvar 2015-12-21, dnr 1641-2015.

gleringen av den statliga elektroniska identitetshandlingen ska vara skild från regleringen av den fysiska identitetshandlingen. Utredningen bedömer ändå att bestämmelserna om personuppgiftsbehandling bör hållas samman. Den verksamhet som bestämmelserna om personuppgiftsbehandling ska omfatta är den för utfärdande av identitetshandlingar, och då bör det vara samma författning som reglerar för vilka ändamål en personuppgiftsbehandling får göras.

12.8.10 Ikraftträdande

Utredningen föreslår:
att lagen träder i kraft den 1 januari 2020.

Utredningen bedömer att en statlig elektronisk identitetshandling är efterfrågad. Inte minst med beaktande av att Sverige vill kunna anmäla en statlig elektronisk identitetshandling för gränsöverskridande identifiering (användning inom Europa) enligt eIDAS-förordningen Det är angeläget att statens ansvarstagande för grundidentifiering och utfärdande av elektroniska identitetshandlingar inte ligger alltför långt bort. Samtidigt måste resultatet av 2017 års ID-kortsutredning inväntas. Med beaktande av att den utredningen ska redovisas den 29 mars 2019, bedömer utredningen att ikraftträdandet för den nu föreslagna lagen tidigast kan sättas till den 1 januari 2020.

13 Myndigheters sätt att anskaffa funktioner för elektronisk identitetskontroll

Utredningen bedömer:
att individer ska ges samma identifieringsmöjligheter oavsett vilken statlig myndighet, kommun eller landsting som de ska identifiera sig elektroniskt mot,
att det som i dag benämns tjänst för elektronisk identifiering bör benämnas funktion för elektronisk identitetskontroll.

Elektronisk identifiering har vuxit fram ur en innovativ marknad, där marknadens aktörer har haft möjlighet att utveckla, testa och marknadsföra nya lösningar. Den svenska befolkningen har en hög digital mognad. För många ingår användningen av en elektronisk identitetshandling i vardagen. I takt med utvecklingen har också fler behov tillgodosetts genom nya marknadslösningar. Exempelvis kan nämnas att mobila lösningar för elektronisk identifiering tagits fram ur en behovsdriven utvecklingsprocess. De privata aktörernas innovationer har varit gynnsamma för det offentliga Sverige, där förvaltningen har kunnat dra nytta av marknadslösningarna. Det finns, givet BankID:s dominerande ställning, en förväntan hos individer att de ska kunna använda sitt BankID för att identifiera sig inte bara mot sin bank utan också mot offentliga myndigheter.

Elektronisk identifiering är fråga om ett samspel mellan flera olika aktörer. En förutsättning för att en individ ska kunna använda en viss elektronisk identitetshandling i en e-tjänst är det finns ett avtal mellan utfärdaren och den som har e-tjänsten. När avtal av detta slag sluts mellan en utfärdare och en statlig myndighet, kommun eller ett landsting kallas utfärdaren för *leverantör* (mer om detta

nedan). Avtalet består av *dels* en rätt att ställa fråga om identiteten hos en individ, *dels* att utfärdaren/leverantören ska svara med ett identitetsintyg. I dag benämns avtalets innehåll som en *tjänst för elektronisk identifiering*.

Utredningen har tidigare analyserat begreppet identifiering och kommit fram till att det omfattar såväl att en individ identifierar sig som den kontroll som någon gör av individens identitet. Eftersom den nu aktuella tjänsten inte omfattar individen som avtalspart, och definieras som en förvaltningsgemensam digital funktion, bedömer utredningen att den bör kallas *funktion för elektronisk identitetskontroll* eftersom den syftar till att den som har en e-tjänst ska kunna kontrollera någons identitet.

Det finns i dag inget enhetligt sätt för offentliga myndigheter att anskaffa en funktion för elektronisk identitetskontroll. Varje offentlig myndighet bestämmer själv hur den ska göra. Det leder till att individer kan mötas av olika alternativ för att identifiera sig elektroniskt hos olika offentliga myndigheter.

Enligt utredningen bör målsättningen vara att individer inte ska behöva ha olika elektroniska identitetshandlingar *beroende på* vilken offentlig myndighet som de ska identifiera sig mot. Att individer kan *välja att ha* flera elektroniska identitetshandlingar är en annan sak. Utredningen bedömer dessutom att det är viktigt att det för individer är tydligt vilka elektroniska identitetshandlingar som de kan använda sig av för att identifiera sig elektroniskt mot offentliga myndigheter.

För att stimulera utveckling av e-tjänster anser utredningen att det ska vara enkelt för statliga myndigheter, kommuner och landsting att veta hur de ska anskaffa en funktion för elektronisk identitetskontroll. Tid och resurser ska inte i onödan behöva läggas på bedömningar av vilka sätt att anskaffa de funktioner som passar myndigheten bäst, än mindre på att ta fram krav som leverantörer ska uppfylla eller för att anpassa egna system utifrån olika leverantörers lösningar. För statliga myndigheter, kommuner och landsting är det dessutom viktigt att det finns möjlighet att skapa förutsättningar för att individer ska kunna identifiera sig genom de nya lösningar som uppstår på marknaden. Det ska givetvis göras med beaktande av att det vid myndighetskontakter måste ställas säkerhetskrav på teknik och tillförlitlighet.

13.1 ”Peka med hela handen”

Utredningen har i sitt arbete träffat företrädare för statliga myndigheter, kommuner och landsting och pratat om hur de ser på sättet att anskaffa funktioner för elektronisk kontroll. Det har inte varit en enhetlig bild, men på det stora hela anser de företrädare som utredningen träffat att regelverket för anskaffning av funktioner för elektronisk identitetskontroll är komplicerat. Eftersom avtal som myndigheterna sluter är mångåriga och dessutom förlängningsbara har också risker med att under lång tid vara fastlåst i ett avtal lyfts fram. Det har beskrivits som svårt för upphandlande myndigheter att avgöra vilket alternativ som är bäst för verksamheten.

13.2 Vad kan en elektronisk identitetshandling användas till?

En elektronisk identitetshandling kan *utfärdas* av olika aktörer men syftet är alltid detsamma – att intyga identitetsuppgifterna hos en individ. En elektronisk identitetshandling kan också *användas* för olika åtgärder. eSamverkansprogrammet (eSam) har närmare beskrivit detta.[1] I det följande beskriver utredningen i korthet vad en elektronisk identitetshandling kan användas till. Beskrivningarna utgår från eSams vägledning, men använder de begrepp som utredningen har bedömt ska användas.

13.2.1 En elektronisk identitetshandling kan användas för …

… tillträde

En elektronisk identitetshandling kan användas för att få tillgång till uppgifter som lämnats ut till honom eller henne i exempelvis en e-tjänst och få skydd mot att någon annan släpps in under sken av att vara den som har identifierat sig.

[1] eSam:s skrivelse Juridisk vägledning för införande av e-legitimering och e-underskrifter.

… uppgiftslämnande

En elektronisk identitetshandling kan användas för att lämna in uppgifter elektroniskt och få skydd mot att någon annan lämnar uppgifter under sken av att vara användaren.

… indirekt underskrift

En elektronisk identitetshandling kan användas som ett led för att skapa en s.k. indirekt underskrift hos t.ex. en myndighet med en från den elektroniska identitetshandlingen fristående underskriftstjänst. Med detta menas en underskrift för att skydda en elektronisk handling mot förfalskning och förnekande av underskrift på motsvarande sätt som om handlingen hade undertecknats på papper.[2] Beroende på den typ av e-tjänst som användaren nyttjar och informationsinnehållet i tjänsten kan en viss minsta skyddsnivå krävas för den elektroniska identitetshandlingen.

13.2.2 Identifiering och inloggning är inte samma sak

Utredningen bedömer:
att elektronisk identifiering och inloggning, som begrepp, bör skiljas åt.

Den som ska kontrollera identiteten är ofta den som har en e-tjänst i vilken individer som vill använda e-tjänsten måste identifiera sig. Vid en genomgång av e-tjänster i den offentliga sektorn kan utredningen konstatera att det man gränssnittsmässigt oftast möts av är att man ska *logga in* i en e-tjänst.[3] Vid inloggning kan individen välja vilken identifieringslösning som han eller hon vill använda. Utredningen anser att sådana gränssnitt gör att individen ofta tolkar elektronisk identifiering som synonymt med inloggning. Utredningen bedömer dock att det är viktigt att skilja på elektronisk identifiering och in-

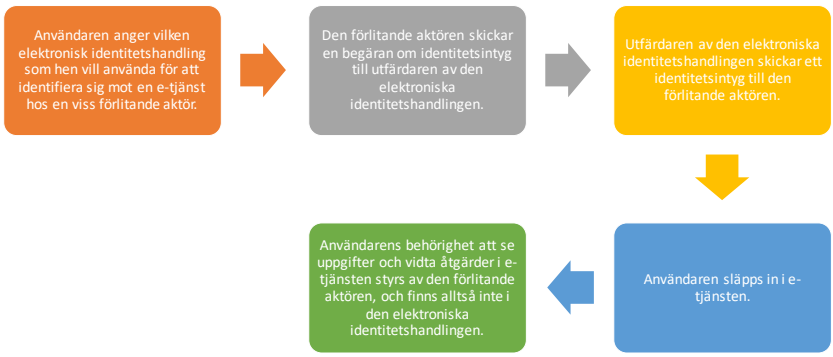
[2] Om elektroniska handlingar, se vidare E-delegationens vägledning Elektroniska original, kopior och avskrifter, 2012-06-07.
[3] Bl.a. www.forsakringskassan.se/, 2017-12-17, www.skatteverket.se/, 2017-12-17, www.csn.se/, 2017-12-17.

loggning. Risken är annars att individen betraktar identifieringen endast som *ett sätt att logga in*, och inte är uppmärksam på att han eller hon faktiskt använder sig av en elektronisk värdehandling, se också avsnitt 12.3.[4] Utredningen lämnar därför ett förslag som innebär att det måste tydliggöras för individen att när han eller hon använder sig av en elektronisk identitetshandling så *identifierar han eller hon sig.*

13.3 Process för elektronisk identifiering

Den aktör som har e-tjänsten och alltså ska kontrollera identiteten kallas i eSams vägledning för *förlitande part*. Utredningen väljer att kalla aktören för *förlitande aktör*. Part som begrepp kan leda tanken fel. Utredningen anser att aktör är ett mer neutralt begrepp. Förlitande kommer av att aktören förlitar sig på att uppgifterna i den elektroniska identitetshandlingen är korrekta och att det är rätt individ som använder sig av den.

När en individ använder sin elektroniska identitetshandling för att identifiera sig i en e-tjänst ser identifieringsprocessen ut som följer:

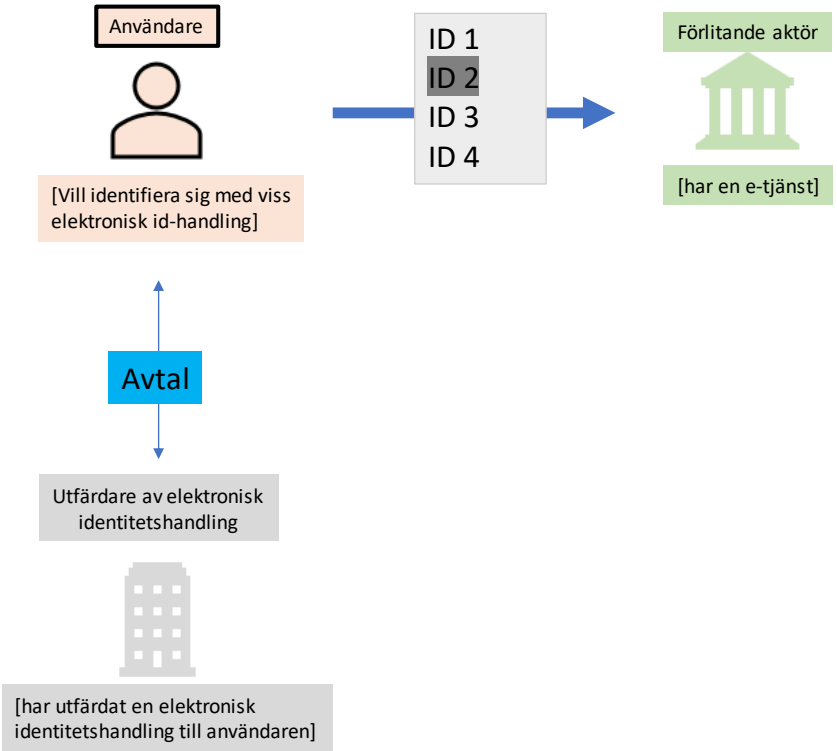


En individ som använder sin elektroniska identitetshandling, kallas för *användare*. När avtal av detta slag sluts mellan en utfärdare och en offentlig myndighet kallas utfärdaren för *leverantör.*

[4] https://computersweden.idg.se/2.2683/1.693238/e-id-varning.

13.3.1 Val av identitetshandling i en e-tjänst

En användare som vill identifiera sig mot en e-tjänst måste först välja vilken identitetshandling som han eller hon vill använda sig av.



En e-tjänst tillhandahålls av en *förlitande aktör*. Den förlitande aktören kan vara en offentlig myndighet eller ett företag. För vissa e-tjänster kräver förlitande aktörer att en användare ska identifiera sig elektroniskt innan användaren släpps in i e-tjänsten.

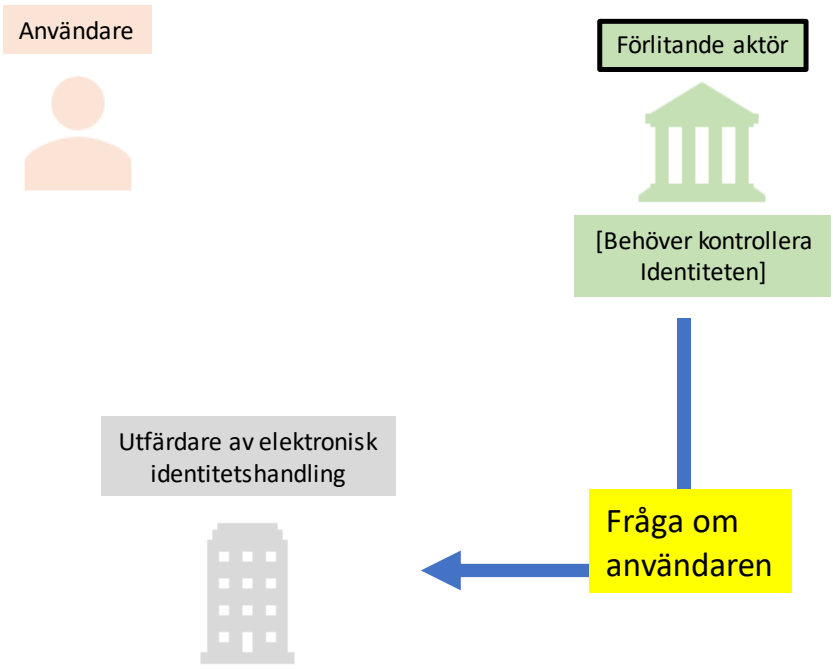
För att en *användare* ska kunna identifiera sig elektroniskt måste han eller hon ha en elektronisk identitetshandling. Användare måste ansöka om en sådan hos någon *utfärdare av elektroniska identitetshandlingar*. Mellan utfärdaren och användaren sluts ett avtal.[5] Det finns flera utfärdare av elektroniska identitetshandlingar i Sverige

[5] Läs mer om detta avtal i eSam:s skrivelse Juridisk vägledning för införande av e-legitimering och e-underskrift.

i dag. Bankernas BankID är den som används mest, men det finns också andra utfärdare av elektroniska identitetshandlingar.[6]

För att en förlitande aktör ska kunna erbjuda användaren elektronisk identifiering måste den förlitande aktören ha slutit avtal om en funktion för elektronisk identitetskontroll med en eller flera utfärdare av elektroniska identitetshandlingar. Dessa avtal kan – för offentliga myndigheter slutas på flera sätt. Utredningen återkommer till detta.

13.3.2 Fråga till utfärdaren om identitetsuppgifter

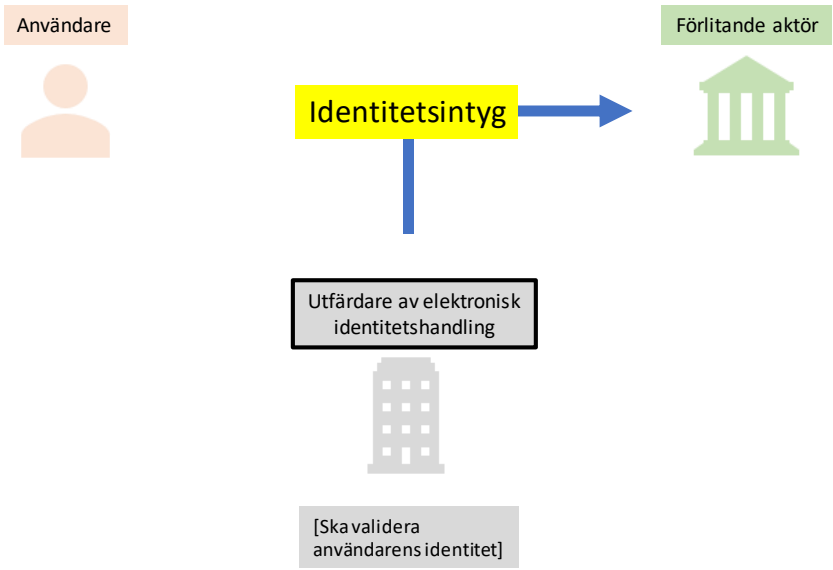


När användaren har valt vilken elektronisk identitetshandling som han eller hon vill använda för att identifiera sig, måste den förlitande aktören kontrollera användarens identitet. Detta görs genom att den förlitande aktören ställer en fråga till utfärdaren/leverantören om

[6] AB Svenska Pass, Telia, Freja eID.

användarens uppgifter stämmer.[7] Utfärdaren har ett åtagande att intyga personens identitet under den elektroniska identitetshandlingens livslängd.

13.3.3 Svar med ett s.k. identitetsintyg

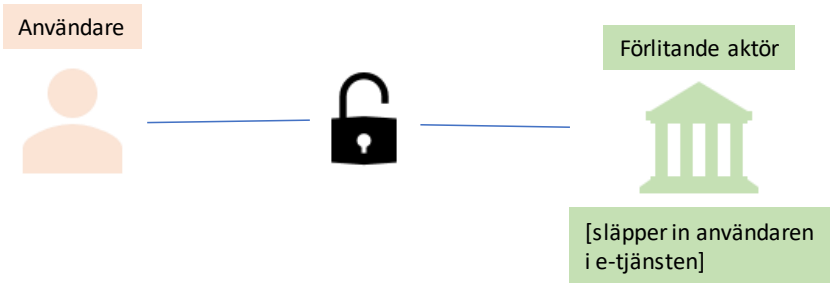


I det föregående steget ställde den förlitande aktören en fråga till utfärdaren om användarens identitet. Utfärdaren svarar genom att skicka ett s.k. identitetsintyg, som innehåller de uppgifter som den förlitande aktören behöver för att lita på att användaren är den som han eller hon utger sig för att vara. Ett identitetsintyg är en elektronisk handling som garanterar spårbarhet och säkerhet i e-tjänsten. Identitetsintyget kan användas endast en gång vilket innebär att ett nytt identitetsintyg måste utfärdas vid varje identitetskontroll.

[7] I sammanhanget bör den konstruktion som BankID har valt särskilt uppmärksammas. I dag har BankID-kollektivet formerat sig så att det finns fyra säljande banker som tecknar avtal i fri konkurrens med varandra. Den förlitande aktör som har tecknat ett avtal med en säljande bank får sedan tillgång till samtliga kunder som har BankID som elektronisk identitetshandling, oavsett vilken bank som har utfärdat BankID:t. Gentemot myndigheter är det tre av dessa säljande banker, Handelsbanken, Swedbank och Nordea, som agerar parallellt. De myndigheter som finns med på Kammarkollegiets ramavtal erbjuder t.ex. avtal med alla tre samtidigt.

I bland kan en annan aktör än utfärdaren/leverantören skicka identitetsintyget. Denna aktör kallas för *identitetsintygsutfärdare*.

13.3.4 Tillträde till e-tjänsten



När den förlitande aktören har tagit emot identitetsintyget kan användaren släppas in i e-tjänsten. Den förlitande aktören behöver inte göra egna kryptografiska kontroller av vem som har identifierat sig eller om den elektroniska identitetshandlingen är spärrad. För den förlitande aktören är det tillräckligt att ta del av uppgifterna i identitetsintyget.[8]

13.3.5 Behörighet finns i systemen, inte i den elektroniska identitetshandlingen

Den elektroniska identitetshandlingen bör inte innehålla uppgifter om användarens behörighet eller roll. Med behörighet avses vad användaren får göra, dvs. vilken åtkomst och rätt att vidta åtgärder som han eller hon har. Sådana uppgifter bör finnas hos den förlitande aktören i register, som kan ändras utan att den elektroniska identitetshandlingen behöver ändras. Med behörighet avses också uppgifter om företrädarskap, exempelvis att en användare tecknar ett visst företags firma. Sådana uppgifter finns normalt sett i andra myndigheters register, vem som exempelvis tecknar ett företags firma finns i bolagsregist-

[8] eSam:s skrivelse Juridisk vägledning för införande av e-legitimering och e-underskrift, s. 16.

ren.[9] Den sortens uppgifter kan e-tjänsten utforma för att inhämta på ett automatiserat sätt.

13.4 Närmare om relationen mellan förlitande aktör och utfärdare av elektronisk identitetshandling

Statliga myndigheter, kommuner och landsting behöver i regel anskaffa funktioner för elektronisk identitetskontroll från andra aktörer, dvs. utfärdare av elektroniska identitetshandlingar.[10] I de sammanhangen kallas den aktör som säljer funktionen för elektronisk identitetskontroll för *leverantör*. Statliga myndigheter, kommuner och landsting med behov av funktioner för elektronisk identitetskontroll har i dag tre valmöjligheter. De kan antingen

- *upphandla* en funktion för elektronisk identifiering på egen hand,
- *avropa* en funktion för elektronisk identifiering på ramavtal som Kammarkollegiet tillhandahåller, eller
- besluta om att *tillhandahålla valfrihetssystem* samt ansluta sig till det system för säker elektronisk identifiering som E-legitimationsnämnden har.

De två första möjligheterna omfattas av lagen (2016:1145) om offentlig upphandling (LOU), medan användning av den tredje möjligheten regleras i lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering (eLOV). I det följande beskrivs i korthet vad de olika alternativen innebär. Utredningen återkommer med bedömning av om alternativen är ömsesidigt uteslutande, eller om de kan vara parallella.

[9] Bolagsverket ansvarar för att registrera uppgifter om företag, bl.a. ansvarar Bolagsverket för aktiebolagsregistret och handelsregistret i vilka det finns uppgifter om aktiebolag respektive handelsbolag, enkla bolag, enskilda näringsidkare, kommanditbolag, trossamfund som utövar näringsverksamhet och ideella föreningar som utövar näringsverksamhet.
[10] Det finns exempel på myndigheter som har tagit fram egna lösningar för elektronisk identifiering. Huddinge kommun har t.ex. utvecklat en egen elektronisk identitetshandling för sina anställda.

13.4.1 Offentlig upphandling – upphandlande myndighet tilldelar kontrakt eller avropar på ramavtal

Regler om offentlig upphandling ska tillämpas när en upphandlande myndighet eller enhet tilldelar en leverantör ett kontrakt eller ingår ramavtal för varor, tjänster, byggentreprenader samt bygg- och tjänstekoncessioner. Offentlig upphandling syftar till att beskriva *hur* sådana kontrakt eller ramavtal sluts. Regler om offentlig upphandling bygger på EU-direktiv och är till stor del lika inom hela EU.

Svenska domstolar är skyldiga att följa EU-domstolens rättspraxis och möjligheterna till nationella undantag är små. Vid tillämpningen av bestämmelserna om offentlig upphandling gäller enligt upphandlingsdirektiven de grundläggande EU-rättsliga principerna om likabehandling, icke-diskriminering, öppenhet, proportionalitet och ömsesidigt erkännande.[11] Dessa grundläggande principer har sitt ursprung i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) och i EU-domstolens rättspraxis. Principerna följer alltså ytterst av fördraget och de artiklar som reglerar rätten till de fria rörligheterna.[12]

Den 26 februari 2014 antogs tre nya EU-direktiv på upphandlingsområdet.[13] Direktiven har föranlett förändringar i det svenska upphandlingsrättsliga regelverket, genom en ny lag (2016:1145) om offentlig upphandling och lag (2016:1146) om upphandling inom försörjningssektorerna samt lagen (2016:1147) om upphandling av koncessioner. De två första lagarna har ersatt tidigare lagstiftning på området,[14] medan den senare lagen är helt ny.

[11] Artikel 18 i LOU-direktivet, artikel 36 i LUF-direktivet och artikel 3 i LUK-direktivet.
[12] SOU 2016:78, Ordning och reda i välfärden, s. 488 ff.
[13] Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (nya klassiska direktivet), Europaparlamentets och rådets direktiv 2014/25/EU om upphandling av enheter som är verksamma på områdena vatten, energi, transporter och posttjänster och om upphävande av direktiv 2004/17/EG (nya försörjningsdirektivet) samt Europaparlamentets och rådets direktiv 2014/23/EU av den 26 februari 2014 om tilldelning av koncessioner (koncessionsdirektivet).
[14] Lagen (2007:1091) om offentlig upphandling och lagen (2007:1092) om upphandling inom områdena vatten, energi, transporter och posttjänster.

Tilldelning av kontrakt

En upphandlande myndighet ska tilldela den leverantör vars anbud är det ekonomiskt mest fördelaktiga för myndigheten ett kontrakt.[15] Vilket anbud som är det ekonomiskt mest fördelaktiga ska utvärderas på någon av grunderna

- bästa förhållandet mellan pris och kvalitet,
- kostnad eller
- pris.

Myndigheten ska i något av upphandlingsdokumenten ange den grund för utvärdering av anbud som den avser att använda. En följd av dessa bestämmelser är att genom upphandling kan endast en leverantör tilldelas kontraktet.

Av E-legitimationsnämndens enkätundersökning om behov av elektroniska identitetshandlingar för 2017 framgår att av den totala volymandelen elektroniska identifieringar och elektroniska underskrifter för 2017 motsvarade egen upphandling nio procent av volymandelen. Av andelen upphandlande myndigheter var det 42 procent som hade upphandlat funktionerna på egen hand.[16]

Ramavtal

Kammarkollegiet ansvarar för att upphandla samordnade ramavtal som är avsedda för andra statliga myndigheter.[17] Inom området informationsteknik gäller ansvaret för den offentliga förvaltningen. I uppgiften ingår att tillhandahålla stödverksamhet för inköp vid avrop från de samordnade ramavtal som Kammarkollegiet har upphandlat. Kammarkollegiet ska verka för att bästa möjliga villkor skapas för myndigheternas anskaffning av varor och tjänster. Inom området informationsteknik ska myndigheten särskilt beakta förvaltningsgemen-

[15] 16 kap. 1 § LOU.
[16] E-legitimationsnämndens enkätundersökning för 2017. Enkäten skickades ut till alla 500 registraturer och i juli 2017 hade 146 svar inkommit, varav hälften av svaren var från kommunal sektor och hälften från statliga myndigheter. https://www.elegnamnden.se/download/18.515a6be615c637b9aa4150e1/1505211922933/2017-09-11+E-legtimationsenk%C3%A4ten+2017+resultat.pdf, 2017-12-22.
[17] 8 a § förordningen (2007:824) med instruktion för Kammarkollegiet.

samma standarder samt intresset av innovationer och teknikneutrala lösningar. Kammarkollegiet ansvarar för ramavtal där bl.a. elektronisk identifiering och e-underskrift ingår.

Det är möjligt att avropa funktioner för identifiering på Kammarkollegiets ramavtal Programvaror och tjänster Informationsförsörjning 2014 (PT14-IF). Ramavtalet är inte inriktat på de funktioner för identifiering som används och inte heller avgränsade till funktioner för elektronisk identifiering. PT14-IF är mycket brett till sitt omfång och är i många hänseenden mer ett kommersiellt ramverk än konkret kravställning för specifika tjänster. Även om det finns exempelavrop och specifikationer ställer avrop på ramavtalet höga krav på den förlitande aktören att själv konkretisera och specificera kravställningen. Många leverantörer, t.ex. CGI, Visma och Cybercom tillhandahåller helhetslösningar där tillhörande avrop och kombinationer av avtal innefattar även avtal med en eller flera leverantörer av identitetsintyg. De agerar alltså återförsäljare av funktioner för identitetskontroll som de har upphandlat från t.ex. en bank.[18] Funktionen ligger ofta inbakad i leveransen från dessa leverantörer och syns inte som en separat del för den upphandlande myndigheten.

Av E-legitimationsnämndens enkätundersökning för 2017 framgår att av den totala volymandelen elektroniska identifieringar och elektroniska underskrifter för 2017 motsvarade avrop på ramavtal 36 procent av volymandelen. Av andelen upphandlande myndigheter var det 46 procent som avropade tjänsterna.[19]

Ändringar i ett kontrakt

Ett kontrakt eller ett ramavtal får ändras utan en ny upphandling, om det exempelvis rör sig om ändringar som är av mindre värde eller om det finns en ändrings- eller optionsklausul med visst innehåll i något av upphandlingsdokumenten i den ursprungliga upphandlingen.[20] En ändring får också göras genom en kompletterande beställning under vissa förhållanden eller om den inte är väsentlig.[21]

[18] eSam:s Juridiska vägledning för införande av e-legitimering och e-underskrifter, s. 37.
[19] E-legitimationsnämndens enkätundersökning för 2017.
[20] 17 kap. 8–14 §§ LOU.
[21] 17 kap. 14 § LOU.

13.4.2 Valfrihetssystem i fråga om funktioner för elektronisk identifiering

Vad är ett valfrihetssystem?

Utredningen har i delbetänkandet beskrivit de befintliga regelverken för valfrihetssystem.[22] När valfrihetssystem får anordnas är särskilt reglerat i lag. I dag finns det fem lagar som reglerar under vilka förhållanden och på vilket sätt upphandlande myndigheter får anordna valfrihetssystem. [23]

Valfrihetssystem bygger på att det är individen som har möjlighet att välja vilken, bland många, leverantörer som erbjuder det bästa alternativet. Med valfrihetssystem avses alltså ett förfarande där individen har rätt att välja leverantör bland de leverantörer som en statlig myndighet, kommun eller landsting har godkänt och tecknat kontrakt med för att få en tjänst utförd. Det är den som köper tjänsten – den statliga myndigheten, kommunen eller landstinget – som bestämmer villkor – krav – för hur ett kontrakt ska fullgöras liksom grunderna för den ekonomiska ersättningen. En leverantör ansöker om att få anslutas till valfrihetssystemet. Den statliga myndigheten, kommunen eller landstinget ska godta alla leverantörer som uppfyller de fastställda kraven. När godkännande lämnats tecknar den statliga myndigheten, kommunen eller landstinget kontrakt med leverantören.

I valfrihetssystem finns det ingen priskonkurrens mellan leverantörerna, eftersom ersättningen är bestämd på förhand. Det är vidare möjligt för leverantörer att ansluta sig till valfrihetssystemet löpande och den som anordnar valfrihetssystem måste löpande annonsera på en nationell webbplats för valfrihetssystem.

[22] SOU 2017:23, digitalforvaltning.nu, s. 230 f.
[23] Lagen (2008:962) om valfrihetssystem, LOV, som gäller för vissa tjänster inom hälso- och sjukvård och socialtjänster, lagen (2010:536) om valfrihet hos Arbetsförmedlingen, lagen (1993:1651) om läkarvårdsersättning och lagen (1993:1652) om ersättning för fysioterapi samt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering.

Lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering

eLOV trädde i kraft år 2013. Lagen utformades med lagen (2008:962) om valfrihetssystem (LOV) som förebild. LOV reglerar valfrihetssystem för tjänster inom hälsovård och socialtjänster. I förarbetena till LOV angavs att det kontrakt som tilldelades var att bedöma som en tjänstekoncession som inte omfattades av de då gällande EU-rättsliga upphandlingsdirektiven.[24]

Regeringen uttalade i förarbetena till eLOV att upphandling av det som då kallades för eID-tjänster (utredningen använder funktion för elektronisk identitetskontroll) skulle utformas på ett sätt som gjorde det möjligt för flera leverantörer att ansluta. Med eID-tjänster avsågs, såvitt utredningen kan bedöma, det som utredningen kallar funktion för elektronisk identitetskontroll. Det skulle vidare, enligt regeringen, vara *användaren* som hade makten att bestämma vem som skulle tillhandahålla funktionen. Därmed stod utfärdaren/leverantören risken för att användaren skulle välja en konkurrerande lösning. Utfärdare/leverantör kunde inte heller på förhand bedöma hur mycket, eller hur ofta, en användare skulle komma att använda funktionen. Dessutom var det inte säkert att utfärdarnas ersättning i valfrihetssystemet skulle motsvara den investering som utfärdaren haft i sin verksamhet eller de driftskostnader de hade för verksamheten. På dessa grunder bedömde regeringen att utfärdarna var utsatta för marknadens nycker och att de kontrakt som skulle ingås inom ramen för valfrihetssystemet var att bedöma som av samma karaktär som kontrakt som tilldelas enligt LOV.[25] I betänkandet E-legitimationsnämnden och Svensk e-legitimation beskrevs att anordnandet av valfrihetssystem var en form av upphandling.[26] Utredningen återkommer i ett senare avsnitt med förslag om att regeringen ska låta se över den rättsliga klassificeringen av eLOV. Redan här kan emellertid framhållas att valfrihetssystem i dag inte bedöms vara en form av upphandling, utan att det är fråga om en nationell lagstiftning som ska följa de upphandlingsrättsliga principerna, men som inte är upphandling.

[24] Prop. 2008/09:29 s. 55 ff och artikel 17 i Europaparlamentets och rådets direktiv 2004/18/EG om samordning av förfarandena vid offentlig upphandling av byggentreprenader, varor och tjänster.
[25] Prop. 2012/13:123, s. 31.
[26] SOU 2010:104, s. 114.

eLOV kom att utformas som en helt fristående författning från LOV. Regeringen bedömde att skillnaderna mellan funktioner för elektronisk identifiering (som utredningen föreslår ska heta elektronisk identitetskontroll) och de tjänster som omfattas av LOV gjorde att det inte framstod som ändamålsenligt att skapa en lag som i huvudsak hänvisade till bestämmelserna i LOV. Vidare bedömde regeringen att en sådan lagteknisk lösning skulle skapa otydligheter och bli svåröverskådlig.[27]

Valfrihetssystem är ett sätt bland många

När eLOV:en infördes bedömde regeringen att det borde vara upp till varje offentlig myndighet att själv avgöra om det fanns ett sådant behov att valfrihetssystem borde inrättas. Regeringen bedömde att det inte borde finnas hinder för en offentlig myndighet att upphandla tjänster för elektronisk identifiering på annat sätt eller för att upphandla tilläggstjänster för specifika behov, utöver vad som omfattas av redan inrättade valfrihetssystem.[28]

E-legitimationsnämnden är ombud för anslutna myndigheter, kommuner och landsting

eLOV gäller när en upphandlande myndighet har *beslutat* att tillämpa valfrihetssystem i fråga om funktioner för elektronisk identifiering av enskilda i myndighetens elektroniska tjänster, *anslutit sig* till ett system för säker elektronisk identifiering som tillhandahålls av den myndighet som regeringen bestämmer och *uppdragit åt* den myndigheten att i den upphandlande myndighetens namn administrera valfrihetssystemet, föra talan i samband med mål om rättelse och i förekommande fall vidta rättelser.[29]

E-legitimationsnämnden har fått regeringens uppdrag att vara den som tillhandahåller systemet för säker elektronisk identifiering.[30] Vid lagens tillkomst bedömde regeringen att E-legitimationsnämnden

[27] Prop. 2012/13:123, s. 35.
[28] Prop. 2012/13:123, s. 34.
[29] 1 § eLOV.
[30] 1 a § förordningen (2010:1497) med instruktion för E-legitimationsnämnden.

skulle inta rollen som ombud för de upphandlande myndigheterna. Regeringen anförde följande:

> E-legitimationsnämnden ska bistå de upphandlande myndigheterna i syfte att säkerställa att de krav på leverantörerna som ställs vid anskaffningen av tjänsterna och de kontrakt som tecknas är förenliga med det regelverk som gäller för identitetsfederationen. För att uppnå detta syfte bör E-legitimationsnämnden i egenskap av ombud för de upphandlande myndigheterna ansvara för hela det praktiska förfarandet. Nämnden bör alltså svara för annonsering och utformning av förfrågningsunderlag, liksom för godkännande av och tecknande av kontrakt med de intresserade leverantörer som uppfyller de krav som ställs. Ombudsrollen bör ha sådan karaktär att de upphandlande myndigheterna kommer att anses ha inrättat sina egna valfrihetssystem.
>
> En följd av att E-legitimationsnämnden inte ska agera i eget namn utan på uppdrag av den som inrättar valfrihetssystem är att det blir flera valfrihetssystem som ska samordnas av E-legitimationsnämnden. För att E-legitimationsnämnden ska kunna fullgöra sin samordningsroll och säkerställa att de parter som deltar i identitetsfederationen kan ha nödvändig tillit till att den elektroniska identifieringen är säker måste de krav som ställs på leverantörerna vara enhetliga. Olika upphandlande myndigheter kan alltså inte ha helt egna och skilda krav. Mot denna bakgrund bör det vara en förutsättning för den nya lagens tillämpning att den som beslutar att tillämpa valfrihetssystem i fråga om tjänster för elektronisk identifiering uppdrar åt den myndighet som regeringen bestämmer, vilket bör vara E-legitimationsnämnden, att administrera systemet.[31]

Valfrihetssystem enligt eLOV

Sedan eLOV trädde i kraft har E-legitimationsnämnden tagit fram tre olika valfrihetssystem;

- Valfrihetssystemet för Svensk e-legitimation,
- eID Övergångstjänst 2016 och
- 2017 E-legitimering.

De första två är stängda för nytillträde, men leveransavtalen i eID 2016 Övergångstjänst löper ut den 31 december 2018. Det tredje – 2017 E-legitimering – är det som utfärdare och myndigheter kan ansluta sig till i dag.[32] I det följande beskrivs de olika valfrihetssystemen närmare.

[31] Prop. 2012/13 :123, s. 36.
[32] Uppgifterna har lämnats av E-legitimationsnämndens kansli.

Valfrihetssystem för *Svensk e-legitimation*, annonserades i februari 2014. Den tekniska metoden för identitetsintygen följde SAML 2.0 enligt E-legitimationsnämndens tekniska specifikationer. Det första identitetsintyget per användare, eID-utfärdare och månad skulle kosta den upphandlande myndigheten 2,98 kronor och de följande transaktionerna samma månad skulle varit kostnadsfria. eID-utfärdarens ersättning skulle varit 1,98 kronor per användare, upphandlande myndighet och månad. Mellanskillnaden skulle täcka E-legitimationsnämndens kostnader. Skälet att välja den fasta prismodellen var att göra kostnaderna för de upphandlande myndigheterna förutsägbara och därmed möjliga att budgetera för. Nitton upphandlande myndigheter anslöt sig, bland dem Skatteverket och Pensionsmyndigheten. Det motsvarade cirka 50 procent av den efterfrågade transaktionsvolymen. Två stora aktörer, Försäkringskassan och Inera AB, anslöt sig emellertid inte. Det gjorde inte heller någon leverantör, varför valfrihetssystemet togs ned våren 2016. Det innebar att även de till valfrihetssystemet kopplade centrala tjänsterna[33] lades ner.

Valfrihetsystem *eID 2016 Övergångstjänst* är ett gällande valfrihetssystem där leveransavtalen löper ut den 31 december 2018. Detta valfrihetssystem är stängt för nytillträde. Den tekniska metoden för identitetsintygen väljs av leverantörerna och det finns inga centrala tjänster. Transaktionspriset för ett identitetsintyg är 17 öre. Totalt 37 myndigheter har anslutit sig och bland dem finns Försäkringskassan och Pensionsmyndigheten, vilket motsvarar 55 procent av den offentliga transaktionsvolymen. Enligt uppgifter från E-legitimationsnämndens kansli skulle en större andel upphandlande myndigheter ha varit med om det hade gått att välja den tekniska metoden SAML 2.0 enligt nämndens tekniska specifikationer och om valfrihetssystemet hade annonserats några månader tidigare än mars 2016, då de sista avropsavtalen på det tidigare ramavtalet (eID 2008) var nära att löpa ut. Både BankID och Telia:s lösning finns med i detta valfrihetssystem, för BankID genom att Swedbank, Handelsbanken och Nordea är anslutna.

Valfrihetssystem *2017 E-legitimering* är ett valfrihetssystem som öppnades i juli 2017. Valfrihetsystemet är enligt uppgift från E-legitimationsnämnden tänkt att vara huvudlösning för elektronisk

[33] Enligt uppgift från E-legitimationsnämndens kansli var de centrala tjänsterna *dels* ett metadataregister, *dels* en central anvisningstjänst som innebar en lista över inloggningsmetoder att välja mellan, *dels* en central intygskonverteringstjänst som innebar att leverantörernas tekniska metod konverterades till SAML 2.0 enligt E-legitimationsnämndens tekniska ramverk.

identifiering på tillitsnivå 3. Den tekniska metoden för identitetsintygen följer SAML 2.0 enligt E-legitimationsnämndens tekniska specifikationer.[34] Transaktionspriset för ett identitetsintyg är 17 öre, liksom i eID 2016 Övergångstjänst. Enligt uppgifter från E-legitimationsnämndens kansli är det i skrivande stund fyra upphandlande myndigheter som har anslutit sig till 2017 E-legitimering, varav Arbetsförmedlingen och Bolagsverket är de som har störst transaktionsvolym. Ingen leverantör har i skrivande stund ansökt om att få ansluta sig.

13.4.3 Valfrihetssystem är ändamålsenligt

Utredningen bedömer:
att valfrihetssystem för elektronisk identitetskontroll är både funktionellt och effektivt,
att köp av funktion för elektronisk identitetskontroll ska inriktas på eLOV.

Såväl egen upphandling som avrop på ramavtal ställer höga krav på myndigheterna för att konkretisera och specificera kravställningen. Om en statlig myndighet, kommun eller ett landsting väljer egen upphandling enligt LOU kan ett kontrakt endast tilldelas *en* leverantör. Därmed skapar vanlig upphandling inte förutsättningar för en marknad där individer ska kunna välja vilken utfärdare av elektroniska identitetshandlingar som de bedömer vara bäst. I stället är det den offentliga myndigheten som genom sin kravställning väljer åt individen. Sett utifrån individens perspektiv, och med beaktande av att statliga myndigheter, kommuner och landsting i regel upphandlar sina funktioner separat från varandra, kan det medföra att individer måste ha flera elektroniska identitetshandlingar, inte efter eget val utan på grund av att upphandlingsförfaranden har resulterat i att olika utfärdare tilldelats kontrakt hos olika offentliga myndigheter.

Valfrihetssystem har tagits fram som ett sätt att säkra att det är individen som ska ha valmöjligheterna. I delbetänkandet föreslog utredningen en lag om valfrihet för elektroniska brevlådor,[35] just för att

[34] Enligt uppgift från E-legitimationsnämndens kansli gäller detsamma för identitetsintyg från den svenska eIDAS-noden.
[35] Lagen benämns i detta betänkande lagen om valfrihet om digitala brevlådor.

säkerställa att individen ska ha möjlighet att, bland flera leverantörer av elektroniska brevlådor, själva välja den leverantör som individen uppfattar tillhandahåller den bästa kvaliteten.[36] Utredningen har således tidigare bedömt, och bedömer alltjämt, att valfrihetssystem är ett ändamålsenligt sätt för statliga myndigheter, kommuner och landsting att anskaffa digitala funktioner.

Genom valfrihetssystem skapas möjlighet för leverantörer att ansluta sig löpande. Det gör att nya innovativa lösningar kan anslutas under valfrihetssystemens livstid. Valfrihetssystem, som administreras av en myndighet, innehåller också en för de ansluta myndigheterna gemensam kravbild gentemot leverantörerna. Detta leder till att leverantörerna inte behöver specialanpassa sina lösningar utifrån en specifik offentlig myndighets behov. De ges därmed möjlighet till mer standardiserade och gemensamma funktioner för hela förvaltningen.

Utredningen bedömer att det genom valfrihetssystem skapas förutsebarhet för både offentliga myndigheter och leverantörer, liksom att det ger individen möjlighet att välja bland flera leverantörer.

eLOV är en redan befintlig författning och E-legitimationsnämnden har, som beskrivits, tagit fram några valfrihetssystem sedan lagens tillkomst. Utredningen konstaterar att det har varit svårt att få såväl offentliga myndigheter som utfärdare att ansluta till de valfrihetssystem som E-legitimationsnämnden har tagit fram. Ansluter sig inte utfärdarna vill inte de offentliga myndigheterna heller ansluta sig, eftersom de då inte får det som de behöver. Ansluter sig inte många offentliga myndigheter, vill inte utfärdare ansluta sig.

Valfrihetssystemet eID Övergångstjänst 2016 är det valfrihetssystem som varit mest framgångsrikt genom att Swedbank, Handelsbanken och Nordea – således lösningen BankID – samt Telia funnits med liksom flera offentliga myndigheter. Där fanns dock inga tekniska specifikationer med. Svårigheter tycks alltså finnas när tekniska specifikationer inkluderas i villkoren för valfrihetssystem eftersom det då ställer krav på leverantörerna att de ska anpassa sig.

Utredningen bedömer att det finns utvecklingsmöjligheter när det gäller valfrihetssystem för elektronisk identitetskontroll.

[36] digitalforvaltning.nu, SOU 2017:23, s. 233.

13.5 Sätt att anskaffa funktion för elektronisk identitetskontroll är en sak, hur trafiken till följd av funktionen sedan flödar är en annan

Förlitande aktörer ska kunna ställa frågan om en individ och få ett identitetsintyg tillbaka. Som beskrivits ingår dessa delar i en funktion för elektronisk identitetskontroll, som utredningen beskrivit att förlitande aktörer kan anskaffa på olika sätt. De olika sätten svarar samtliga på frågan *hur* den statliga myndigheten, kommunen eller landstinget anskaffar funktionen. För att leverantörer ska veta vad de har att förhålla sig till sätter den upphandlande myndigheten upp villkor för funktionen. Resultatet blir ett kontrakt mellan den förlitande aktören och en leverantör.

Med trafik menar utredningen mellan vilka aktörer som frågor respektive identitetsintyg skickas. Det mest renodlade sättet att göra detta på är att utfärdaren skickar identitetsintyget direkt till den förlitande aktören. Emellertid är det inte alltid så det går till. I bland är det en underleverantör till utfärdaren som skickar identitetsintyget, efter att ha anpassat identitetsintyget till ett intyg som är anpassat för den förlitande aktörens it-miljö.[37] Det är då fråga om en indirekt leverans.

13.6 Ändringar i eLOV

13.6.1 Tjänst för elektronisk identifiering blir funktion för elektronisk identitetskontroll

Utredningen föreslår:
att den tjänst som beskrivs i eLOV ska kallas funktion för elektronisk identitetskontroll,
att lagens namn ändras från lag om valfrihetssystem i fråga om tjänster för elektronisk identifiering till lag om valfrihetssystem i fråga om funktioner för valfrihetssystem.

Förslaget genomförs genom lag om ändring av lag om valfrihetssystem i fråga om funktion för elektronisk identitetskontroll.

[37] eSam:s skrivelse Juridisk vägledning för införande av e-legitimering och e-underskrift, s. 19.

Utredningen anser att den tjänst som i eLOV kallas för elektronisk identifiering i stället bör heta funktion för elektronisk identitetskontroll.

Utredningen har tidigare motiverat varför begreppet förvaltningsgemensam digital funktion ska användas. Som en följd av det resonemanget föreslår utredningen att begreppet tjänst i eLOV ska bytas ut mot funktion.

Som beskrivits innefattar funktionen att en förlitande aktör kan ställa fråga om en användares identitet till en leverantör och att leverantören svarar med ett identitetsintyg. Syftet med funktionen är att den förlitande aktören ska kontrollera identiteten på en användare. Funktionen måste anskaffas i förväg, alltså innan användaren ens är inblandad. Utredningen har använt begreppet identifiering för att beskriva såväl att någon identifierar sig som kontroll av annans identitet. Givet innehållet i den funktion som förlitande aktör måste anskaffa, föreslår utredningen att funktionen ska kallas elektronisk identitetskontroll.

Utredningens bedömning leder till att namnet på eLOV måste ändras, liksom de bestämmelser i lagen som beskriver det som nu kallas tjänst och det som utredningen föreslår ska kallas funktion för elektronisk identifiering.

13.6.2 Statliga myndigheter, kommuner och landsting *ska* ansluta sig till valfrihetssystem

Utredningen föreslår:
att alla statliga myndigheter, kommuner och landsting med e-tjänster som kräver elektronisk identifiering *ska* ansluta sig till valfrihetssystem som digitaliseringsmyndigheten tillhandahåller.

Utredningen anser att den valmöjlighet som statliga myndigheter, kommuner och landsting har ska ersättas av en skyldighet att ansluta sig till de valfrihetssystem för elektronisk identifiering som digitaliseringsmyndigheten tillhandahåller. På detta sätt bedömer utredningen att det skapas en tydlighet för såväl statliga myndigheter som kommuner och landsting hur de ska gå till väga för att anskaffa en funktion för elektronisk identitetskontroll.

Utredningen har övervägt alternativet att inte lägga fram detta förslag och låta det befintliga regelverket vara som det är i dag, med samtliga sätt att anskaffa funktioner för elektronisk identifiering valbara. Därmed skulle det fortsatt vara upp till statliga myndigheter, kommuner och landsting att själva besluta om de vill anordna valfrihetssystem. Vid en sammantagen bedömning anser utredningen emellertid att det ur ett förvaltningsövergripande perspektiv är mest effektivt om alla statliga myndigheter, kommuner och landsting *anvisas ett sätt* för anskaffning av funktion för elektronisk identitetskontroll.

Genom ett anvisat och ensat sätt för alla offentliga myndigheter att anskaffa funktioner för elektronisk identitetskontroll skapas förutsättningar för att individer ges samma valmöjligheter när de ska identifiera sig elektroniskt vare sig detta görs hos en statlig myndighet, kommun eller landsting. Det gör att utredningen bedömer att det är motiverat med ett förslag att statliga myndigheter, kommuner och landsting *ska* ansluta sig till valfrihetssystem. En sådan skyldighet måste regleras i lag.

13.6.3 En myndighet ges ansvar att tillhandahålla valfrihetssystem för allas räkning *i stället för* ombudsrelationer

Utredningen föreslår:
att digitaliseringsmyndigheten ska tillhandahålla valfrihetssystem för funktioner för elektronisk identifiering,
att digitaliseringsmyndigheten i eLOV benämns den upphandlande myndigheten.

Utredningen bedömer att det är naturligt att *en* myndighet utför uppgiften att tillhandahålla valfrihetssystem för de övriga statliga myndigheternas, kommunernas och landstingens räkning. Detta går att åstadkomma med den modell som finns i dag, som bygger på att E-legitimationsnämnden agerar som *ombud* för de upphandlande myndigheterna. Ett annat sätt att angripa frågan på är att *tilldela en myndighet uppgiften* att tillhandahålla valfrihetssystem för elektronisk identitetskontroll.

Ett ombud agerar på uppdrag av annan och ska företräda dennes intressen enligt de instruktioner som ges.[38] Instruktioner ges i form av en fullmakt, som kan vara såväl muntlig som skriftlig. När det gäller relationer mellan offentliga objekt brukar fullmakten vara i form av överenskommelser med angivande av hur ansvaret fördelas. Det kan finnas skriftliga fullmakter med mycket vidsträckt behörighet att företräda exempelvis ett bolag. Sådana fullmakter brukar kallas generalfullmakter. Uttrycket generalfullmakt förekommer inte i någon lagbestämmelse men används i praktiken för att beteckna att behörigheten är mycket omfattande. Något hinder att utrusta ett ombud med en sådan vidsträckt fullmakt finns inte.

Med dagens utformning av eLOV är det varje upphandlande myndighet som anordnar valfrihetssystem och överlåter åt E-legitimationsnämnden att i egenskap av ombud administrera dessa. På uppdrag av den upphandlande myndigheten tar E-legitimationsnämnden fram villkor och förhandlar med leverantörer. I förarbetena till eLOV betonades att E-legitimationsnämnden skulle företräda anslutna offentliga myndigheter som ombud.

Enligt modellen är det varje statlig myndighet, kommun eller landsting som ska betala den i valfrihetssystemet *avtalade ersättningen* till leverantören. E-legitimationsnämnden får ta ut *avgifter* från de upphandlande myndigheterna, men nämnden tar inte ut några sådana avgifter.[39]

Statliga myndigheter, kommuner eller landsting som ansluter sig till valfrihetssystem som E-legitimationsnämnden tillhandahåller kan inte påverka den närmare utformningen på valfrihetssystemet. Deras uppdrag till E-legitimationsnämnden liknar generalfullmaktens.

Eftersom en statlig myndighet, en kommun eller ett landsting inte har möjlighet att påverka det närmare innehållet i valfrihetssystemet bedömer utredningen att det finns anledning att ifrågasätta om det finns behov av att etablera en sådan ombudsrelation, eller om det går att hitta andra sätt att reglera ansvar och rollfördelning.

Ett exempel på en situation där staten har beslutat att en viss myndighet ska stödja andra myndigheter är Statens servicecenters

[38] Jfr om rättegångsombud i NJA II 1943 s. 151, där det bl.a., framgår att en part blir bunden av de processhandlingar som ett ombud företar under förutsättning att dessa ligger inom fullmaktens gränser. Jfr också 2 kap. 10 § lagen (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område.

[39] 5 § förordningen (2010:1497) med instruktion för E-legitimationsnämnden.

ansvar för att tillhandahålla tjänster som gäller administrativt stöd åt statliga myndigheter.[40] Statens servicecenter tillhandahåller bl.a. lönerelaterade tjänster. Regeringen gav i regleringsbrevet[41] för 2016 Statens servicecenter i uppdrag att redovisa en uppdaterad plan för vilka myndigheter som planeras att anslutas till de lönerelaterade tjänsterna 2017 och 2018.[42] Regeringen har vidare beslutat att vissa myndigheter *ska* ansluta sig till de lönerelaterade tjänster som Statens servicecenter ansvarar för.[43] Här har regeringen alltså styrt vissa statliga myndigheter till att använda de lönerelaterade tjänster som Statens servicecenter tillhandahåller. I promemorian som föregick förordningen konstaterades följande:

> I de lönerelaterade bastjänster som tillhandahålls av Statens servicecenter ingår handläggande uppgifter, kundsupport och tillgång till systemstöd, inklusive drift, underhåll och förvaltning. I systemstödet ingår upphandling och införande av nya systemstöd samt viss utbildning av personal. Myndigheterna behöver således inte ha egen personal för hantering av dessa uppgifter, och inte heller ha egna licenser eller avtal om systemstöden. Myndigheterna behöver dock utföra vissa moment, såsom leverans av löneunderlag samt uppföljning av tjänsteleveranser.
>
> Enligt bestämmelserna i myndighetsförordningen ansvarar varje myndighet inför regeringen för verksamheten och för att den bedrivs effektivt och enligt gällande rätt. Dessa bestämmelser innebär att Statens servicecenter är ansvarigt för att de tjänster som tillhandahålls myndigheterna är effektiva och att de myndigheter som ansluter sig till tjänsterna är ansvariga för att t.ex. korrekta uppgifter ges till servicecentret och för att följa upp tjänsteleveranser. Den närmare ansvarsfördelningen mellan Statens servicecenter och anslutande myndigheter bestäms i de enskilda överenskommelserna, där även formerna för samverkan rörande bl.a. intern styrning och kontroll regleras. Det är Statens servicecenters och de anslutande myndigheternas gemensamma ansvar att se till att överenskommelserna blir ändamålsenligt utformade. En central uppföljning och utvärdering av anslutningarna bör dock ske i ett senare skede.[44]

[40] 1§ förordningen (2012:208) med instruktion för Statens servicecenter.
[41] Regleringsbrev för budgetåret 2016 för Statens servicecenter, Fi 2015/05652/RS.
[42] Regeringen har uttalat att styrningen av anslutningen av myndigheter till Statens servicecenter behöver stärkas. Regeringen har därför aviserat att anslutningen till Statens servicecenters lönerelaterade bastjänster ska förordningsregleras. Syftet är att påskynda arbetet med att effektivisera statens administrativa stödverksamhet och skapa ett ökat fokus på myndigheternas kärnverksamhet, prop. 2015/16:1 utg. omr. 2, s. 53.
[43] 1 § förordningen (2015:665) om statliga myndigheters användning av Statens servicecenters tjänster.
[44] Myndigheters användning av Statens servicecenters tjänster, Finansdepartementet Avdelningen för offentlig förvaltning, april 2015, s. 10 f.

Den konstruktion som regeringen valt för Statens servicecenter innefattar såvitt utredningen kan bedöma inte att Statens servicecenter anses vara ombud i relation till de myndigheter som regeringen beslutat ska ansluta sig till de lönerelaterade tjänsterna. Där handlar det i stället om att Statens servicecenter tillhandahåller de lönerelaterade tjänsterna åt myndigheterna.

Utredningen har analyserat E-legitimationsnämndens roll som ombud för upphandlande myndigheter i förhållande till utredningens förslag om att statliga myndigheter, kommuner och landsting ska ansluta sig till valfrihetssystem i fråga om funktioner för elektronisk identifiering. Utredningen bedömer att förslagen sammantagna också ändrar sättet att betrakta rollfördelningen. Genom utredningens förslag har statliga myndigheter, kommuner och landsting inte längre beslutanderätt när det gäller frågan *om* de ska anordna valfrihetssystem. Därmed är det enligt utredningens bedömning inte längre fråga om att digitaliseringsmyndigheten[45] ska vara ombud för de statliga myndigheterna, kommunerna och landstingen eftersom ombudsförhållanden bygger på frivillig tilldelning av uppgifter.

Utredningen föreslår att digitaliseringsmyndigheten ska vara avtalspart i relation till leverantörerna. Utredningen menar att detta förslag inte medför någon ändring i sak av vad E-legitimationsnämnden gör i dag och vad den framtida digitaliseringsmyndigheten ska göra när den tar över E-legitimationsnämndens uppgifter. Förslaget syftar endast till att beskriva rollfördelningen i valfrihetssystem och inte till att ändra sättet som trafiken med frågor och identitetsintyg flödar. Avsikten med förslagen är alltså *inte* att digitaliseringsmyndigheten ska inträda som mellanhand i trafiken mellan leverantör och förlitande aktör.

Förslaget ska därtill kopplas samman med utredningens förslag om lag om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling. Utredningen föreslår i kapitel 14 att digitaliseringsmyndigheten bl.a. ska tillhandahålla ett register med utfärdare och förlitande aktörer. Registret skapar förutsättningar för att trafiken – alltså frågan om en användares identitetsuppgifter och svaret i form av identitetsintyget – flödar på ett korrekt sätt. Det blir digitaliseringsmyndigheten som ska bestämma vill-

[45] Enligt direktiv 2017:117 ska E-legitimationsnämndens uppgifter tas över av den nya myndigheten för digitalisering av den offentliga verksamheten fr.o.m. den 1 september 2018.

koren för valfrihetssystemen. Utredningen bedömer att villkor bör kunna skapas som inriktas på hur trafiken mellan leverantör och förlitande aktör ska flöda, samt de närmare villkoren för ansvarsutkrävande till följd av fel i trafiken mellan förlitande aktör och leverantör.

I lagen kommer digitaliseringsmyndigheten att benämnas den upphandlande myndigheten, se emellertid utredningens förslag om översyn av eLOV.

13.6.4 Undantag från skyldigheten att ansluta sig

Utredningen föreslår:
att regeringen får besluta om undantag från skyldigheten för statliga myndigheter, kommuner och landsting att ansluta sig till valfrihetssystem om det finns särskilda skäl.

Utredningen bedömer att det måste finnas möjlighet för statliga myndigheter, kommuner och landsting att undantas från skyldigheten att ansluta sig till valfrihetssystem som digitaliseringsmyndigheten tillhandahåller. Sådant undantag kan beviljas om det finns särskilda skäl. Utredningen bedömer att sådana *särskilda skäl* kan vara att den statliga myndigheten, kommunen eller landstinget är bunden av befintliga avtalsvillkor som gör att den inte kan ansluta sig till valfrihetssystem eller att den måste genomföra omfattande tekniska anpassningar av sina egna system innan den kan följa de villkor som gäller inom valfrihetssystem.

13.7 Ersättningsmodell

Utredningen föreslår:
att dagens ersättningsmodell för funktion för elektronisk identitetskontroll ändras på så sätt att utfärdare av elektroniska identitetshandlingar ska fakturera Kammarkollegiet för det antal identitetsintyg som statliga myndigheter, kommuner och landsting har begärt inom ramen för valfrihetssystem.

att Kammarkollegiet tilldelas anslagsmedel för den ersättning som ska betalas till leverantörer för statliga myndigheters, kommuners och landstings användning av funktion för elektronisk identitetskontroll.

I dag fakturerar leverantören varje månad respektive statlig myndighet, kommun eller landsting för det antal identitetsintyg som har förmedlats inom ramen för valfrihetssystem. Ersättningsmodellen bygger på en s.k. tickkostnad, dvs. att varje identitetsintyg ersätts med en viss, på förhand, angiven summa. Det har framkommit att detta sätt att fakturera är otympligt och ineffektivt för leverantörerna som *dels* måste veta mängden trafik som respektive statliga myndighet, kommun eller landsting har begärt, *dels* måste ha en faktureringsorganisation för detta. Modellen är även administrativt otymplig för de offentliga myndigheterna. Utredningen bedömer att det finns anledning att förenkla ersättningsmodellen.

Utredningen föreslår inte någon ändring i sättet som ersättningen ska beräknas. Däremot föreslår utredningen ändringar som tar sikte på hur leverantörer ska fakturera för de statliga myndigheternas, kommunernas och landstingens användning.

Utredningen menar att den ersättning som ska betalas för användning av den förvaltningsgemensamma funktionen för elektronisk identitetskontroll ska vara en förvaltningsgemensam utgift.

Utredningen föreslår att dagens ersättningsmodell för funktion för elektronisk identitetskontroll ändras på så sätt att leverantörer ska fakturera Kammarkollegiet för det totala antal identitetsintyg som statliga myndigheter, kommuner och landsting har begärt inom ramen för valfrihetssystem. Det innebär att de offentliga myndigheterna inte själva faktureras av leverantören, utan att leverantören ersätts av Kammarkollegiet. För leverantörerna medför det att de inte behöver analysera hur stor del av den totala användningen som en viss statlig myndighet, kommun eller landsting har stått för under en viss tid.

Kammarkollegiet har till uppgift att ansvara för bl.a. betalning av statens utgifter, om något annat inte följer av särskilda föreskrifter.[46] Utredningen bedömer att det är lämpligt att Kammarkollegiet har

[46] 5 § förordningen (2007:824) om instruktion för Kammarkollegiet. Ny lydelse av bestämmelsen träder i kraft den 1 januari 2018.

denna uppgift, trots att Kammarkollegiet inte är avtalspart. Utredningen bedömer att denna uppgift bör rymmas inom Kammarkollegiets befintliga instruktionsenliga uppdrag. Kammarkollegiets uppgifter i denna del bör anslagsfinansieras.

13.8 Krav på kvalitetsmärket Svensk elektronisk identitetshandling

Utredningen föreslår:
att det i upphandlingsdokumentet för valfrihetssystemet ska ingå krav på att elektroniska identitetshandlingar ska ha kvalitetsmärket Svensk elektronisk identitetshandling för att utfärdaren ska få ansluta sig till valfrihetssystem.

Ett valfrihetssystem bygger på att en aktör uppställer vilka villkor som gäller för en viss vara eller tjänst och att den ekonomiska ersättningen är bestämd på förhand. Alla leverantörer som uppfyller villkoren ska godtas. I eLOV beskrivs att den upphandlande myndigheten ska annonsera valfrihetssystem på en nationell webbplats samt att där ska såväl annonsen som upphandlingsdokumenten finnas.[47] Begreppet upphandlingsdokument i eLOV har samma betydelse som i LOU och avser varje dokument som en upphandlande myndighet använder för att beskriva eller fastställa innehållet i upphandlingen.[48] Med upphandlingsdokument menas bl.a. annonser om upphandling, förhandsannonser, tekniska specifikationer, förslag till kontraktsvillkor och upplysningar om allmänt tillämpliga skyldigheter samt eventuella kompletterande dokument.[49]

Utredningen kommer i det följande att beskriva vad som menas med kvalitetsmärket Svensk elektronisk identitetshandling. Kortfattat ska kvalitetsmärket Svensk elektronisk identitetshandling tjäna som en signal för individer om vilka elektroniska identitetshandlingar som har genomgått ett granskningsförfarande. Elektroniska identitetshandlingar innehåller uppgifter om individer som bör omgärdas av krav på säkerhet. Kvalitetsmärket syftar till att säkerställa

[47] 4 § eLOV.
[48] 1 kap. 23 § LOU.
[49] Prop. 2015/16:195 s. 944.

detta. En kvalitetsmärkning medför emellertid inte att en utfärdare får sälja elektronisk identitetskontroll till offentliga myndigheter. Om kvalitetsmärket ska fylla det syfte som utredningen avser måste det finnas en koppling mellan det sätt som utredningen bedömer att statliga myndigheter, kommuner och landsting ska anvisas för anskaffning av funktion för elektronisk identitetskontroll och kvalitetsmärket.

Utredningen har övervägt olika alternativ. Ett alternativ är att kvalitetsmärket endast skulle avse de elektroniska identitetshandlingar som finns i valfrihetssystem. Det alternativet har emellertid utredningen valt bort eftersom det kan hända att det finns utfärdare som inte riktar sin verksamhet alls mot den offentliga sektorn, men som ändå vill erbjuda sina kunder en kvalitetsmärkt elektronisk identitetshandling.

Utredningen föreslår i stället att digitaliseringsmyndigheten i upphandlingsdokumenten ska ställa krav på att leverantörer som ansluter sig ska ha kvalitetsmärket Svensk elektronisk identitetshandling för att få delta. Någon ändring i lagtexten bedöms inte vara nödvändig för genomförandet av detta förslag.

13.9 Rättslig översyn av eLOV

Utredningen föreslår:
att regeringen låter göra en rättslig översyn av eLOV.

Välfärdsutredningen uttalade i sitt betänkande Ordning och reda i välfärden att anordnande av valfrihetssystem är en form av auktorisationssystem som kan utformas mer fristående från de detaljerade krav som upphandlingsdirektiven uppställer. Därför föreslog Välfärdsutredningen en ny lag om valfrihetssystem som skulle ersätta LOV och att terminologin och strukturen tydligare skulle anpassas till att det är fråga om nationell lagstiftning och inte en upphandlingslagstiftning.[50] Tilldelning av kontrakt inom ramen för ett valfrihetssystem omfattas alltså inte av upphandlingsdirektivens defini-

[50] SOU 2016:78, Välfärdsutredningen, s. 583.

tion av offentlig upphandling, men omfattas av de allmänna upphandlingsrättsliga principerna.

Utredningen bedömer att förståelsen av de olika sätten att anskaffa funktioner för elektronisk identitetskontroll skulle underlättas om lagstiftaren valde att betona att det i eLOV är fråga om nationell lagstiftning. På samma sätt som föreslagits för LOV behöver terminologin i eLOV ses över, bl.a. kallas den myndighet som tillhandahåller valfrihetssystem för den upphandlande myndigheten. En sådan begreppsanvändning kan leda tanken fel.

Utredningen vill dessutom uppmärksamma frågan om förslaget att digitaliseringsmyndigheten ska anordna valfrihetssystem i fråga om funktioner för elektronisk identifiering och att offentliga myndigheter ska ansluta sig till detta medför att upphandling enligt LOU är utesluten för elektronisk identitetskontroll.

Oavsett om en offentlig myndighet upphandlar enligt LOU eller anordnar ett valfrihetssystem så syftar själva anskaffningen till att lösa frågan hur aktören ska gå till väga för att köpa den beskrivna funktionen. Av EU-domstolens praxis följer att ett auktorisationsförfarande inte omfattas av upphandlingsregelverket om det innebär att avtal ingås med alla leverantörer som önskar leverera de berörda varorna/tjänsterna på de villkor som angetts och något annat urval inte görs.[51] I förarbetena till eLOV uttalade regeringen att det inte borde finnas hinder för myndigheter som inrättat valfrihetssystem att upphandla tjänster för elektronisk identifiering på annat sätt eller tilläggstjänster för specifika behov. Mot den bakgrunden bedömer utredningen att förslaget om obligatorisk anslutning till valfrihetssystem för offentliga myndigheter inte torde utesluta att en upphandling av samma typ av funktion också skulle vara möjlig att genomföra enligt reglerna i LOU.

De nu förda resonemangen tyder ändå på att det är otydligt hur eLOV ska tolkas i förhållande till upphandlingslagstiftningen. Sådan otydlighet inverkar på samtliga inblandade aktörer och bidrar till att området blir svårt att omfamna. Utredningen föreslår därför att regeringen låter göra en rättslig översyn av eLOV. I det sammanhanget är det också lämpligt att bedöma om alla valfrihetssystem kan samlas i en och samma lag.

[51] Falk Pharma, C-410/14.

14 En infrastruktur för elektronisk identifiering

14.1 Dagens reglering

Det finns i dag två författningar som reglerar elektronisk identifiering; lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering (eLOV) och instruktionen för E-legitimationsnämnden.[1] E-legitimationsnämnden inrättades den 1 januari 2011. eLOV trädde i kraft 2013. Utredningen har tidigare beskrivit eLOV och de valfrihetssystem som E-legitimationsnämnden har anordnat.

Utredningen om bildande av en E-legitimationsnämnd föreslog i sitt betänkande,[2] utöver eLOV och instruktion för E-legitimationsnämnden, också en förordning om infrastruktur för Svensk e-legitimation. Denna förordning infördes aldrig.

E-legitimationsnämnden ska enligt sin instruktion stödja och samordna elektronisk identifiering och underskrift i den offentliga förvaltningens e-tjänster.[3] Efter överenskommelse med upphandlande myndigheter ska E-legitimationsnämnden tillhandahålla och administrera valfrihetssystem samt upprätta och driva en nationell webbplats för annonsering av valfrihetssystem.[4] Nämnden har även uppdrag inom området elektronisk identifiering enligt eIDAS-förordningen och ansvarar bl.a. för den svenska eIDAS-noden.[5]

[1] Det finns också andra myndigheter som har uppdrag inom området. Post- och telestyrelsen har tillsynsansvar för e-underskrifter och andra betrodda tjänster enligt eIDAS-förordningen och erbjuder vägledning inom samma område, förordningen (2007:951) med instruktion för Post- och telestyrelsen.
[2] SOU 2010:104, E-legitimationsnämnden och Svens e-legitimation.
[3] Förordningen (2010:1497) med instruktion för E-legitimationsnämnden.
[4] 4 § eLOV.
[5] 1 b § förordningen (2010:1497) med instruktion för E-legitimationsnämnden.

E-legitimationsnämndens instruktion ger nämnden ett brett mandat att stödja och samordna elektronisk identifiering och underskrift i den offentliga förvaltningens e-tjänster. E-legitimationsnämnden beslutade 2015 om följande vision och mål för sitt arbete.[6]

Visionen är att:

– Svensk e-legitimation gör det enkelt och säkert för medborgare och anställda att använda e-tjänster i offentlig förvaltning och privat sektor,
– Svensk e-legitimation har ett högt förtroende och är utvecklingsbar.

Målen är:

– att bidra till utveckling och användning av flera e-tjänster i samhället,
– flera utfärdare av svensk e-legitimation,
– att villkoren är transparenta, förutsägbara och kostnadseffektiva,
– att övergången från dagens lösning till svensk e-legitimation är smidig.

På senare år har E-legitimationsnämnden beskrivit om följande mål för sitt arbete:[7]

– Alla ska kunna få tillgång till säkra e-legitimationer som är enkla att använda.
– Det ska vara enkelt och säkert för digitala tjänster att inkludera e-legitimation och e-underskrift.
– Det ska vara kostnadseffektivt för offentlig sektor med e-legitimation och e-underskrift.

[6] Årsberättelse för 2015 E-legitimationsnämnden, 2016-02-22, dnr 131-101941-16/9516.
[7] E-legitimationsnämndens rapport ”Fortsatt försörjning av tjänster för e-legitimering och e-underskrift”, 2016-10-15, dnr 131645711-15/9513.

E-legitimationsnämnden saknar föreskriftsrätt men har med stöd av 4 § myndighetsförordningen meddelat föreskrifter för sin verksamhet. Av föreskrifterna[8] framgår följande.

> I dessa föreskrifter menas med *infrastrukturen för Svensk e-legitimation*: den infrastruktur för elektronisk identifiering som E-legitimationsnämnden styr och förvaltar, och *reglerna för Svensk e-legitimation*: de regler för Svensk e-legitimation som E-legitimationsnämnden förvaltar.

Det saknas författningar som närmare anger vad som ska tas fram inom ramen för exempelvis E-legitimationsnämndens uppgift att stödja och samordna e-legitimering och elektronisk underskrift i den offentliga förvaltningen e-tjänster.

E-legitimationsnämnden tar i dag fram ett tillitsramverk och tekniska specifikationer, baserade på internationella standarder. E-legitimationsnämnden granskar elektroniska identitetshandlingar och tilldelar sådana elektroniska identitetshandlingar som överensstämmer med tillitsramverket kvalitetsmärket Svensk e-legitimation. Ingen av dessa uppgifter framgår uttryckligen av instruktionen. Det är emellertid svårt att utifrån författningsregleringen förstå hur de olika uppgifterna förhåller sig till varandra. Exempelvis är det otydligt vilken roll kvalitetsmärket har för marknadens aktörer.

Utredningen bedömer att när det gäller elektronisk identifiering finns det ett stort behov av regelverk. Detta gäller inte bara tekniska regelverk, som beskriver hur system ska överföra budskap till varandra och som är en absolut förutsättning för digital kommunikation, utan också en författningsreglering som beskriver ansvar och uppgifter samt organisatoriska frågor. Utredningen bedömer vidare att det är viktigt med en sammanhållen syn på vad det offentliga åtagandet omfattar.

14.2 Många initiativ, men vart är vi på väg?

Utredningen bedömer:
att det finns många pågående initiativ som utan tydlig styrning riskerar att bli kontraproduktiva.

[8] E-legitimationsnämndens föreskrifter IFS 2014:1.

Det finns många pågående initiativ när det gäller elektroniska identitetshandlingar i samhället. De privata aktörerna, med BankID i täten, har tagit ett stort ansvar för att säkra att den svenska befolkningen har tillgång till elektroniska identitetshandlingar som kan användas i hela den offentliga förvaltningen. Utredningen kan konstatera att vissa initiativ är samordnade medan andra ger intryck av att vara ovetande om varandra. Den bild som presenteras nedan har föranlett utredningens slutsats att det finns behov av att peka ut vilka delar som ska vara föremål för det offentliga åtagandet.

14.2.1 Kvalitetsmärket Svensk e-legitimation

Svensk e-legitimation är ett kvalitetsmärke för e-legitimationer. Utredningen använder i detta avsnitt begreppet e-legitimation eftersom kvalitetsmärket i dag heter Svensk e-legitimation. Angående begreppet Svensk e-legitimation se kapitel 10 och kapitel 14.3.5. Kvalitetsmärket visar att en e-legitimation är kontrollerad och godkänd av E-legitimationsnämnden. E-legitimationen prövas mot ett nationellt tillitsramverk som baserar sig på internationell standard. Tanken är att en e-legitimation med kvalitetsmärket Svensk e-legitimation ska gå att lita på för offentliga och privata aktörer med e-tjänster som kräver elektronisk identifiering. Även användare kan känna sig trygga med att en e-legitimation märkt Svensk e-legitimation är en säker identitetshandling.

Den utfärdare som vill få kvalitetsmärket på sin e-legitimation får ansöka om att bli granskad av E-legitimationsnämnden. En central del i E-legitimationsnämndens granskning är att fastställa att en e-legitimation håller den tillitsnivå, dvs. den grad av säkerhet och tillförlitlighet, som e-legitimationen utlovar.

I E-legitimationsnämndens tillitsramverk beskrivs vilka krav som ställs på en e-legitimation från tillitsnivå 2 och uppåt. Granskningen omfattar inte bara den tekniska arkitekturen, utan även utfärdarens finansiella stabilitet, informationssäkerhetsarbete och intern kontroll, process för identifiering av personer som ansöker om att få en e-legitimation samt framställande och tillhandahållande av e-legitimationer. Ett grundläggande krav är att ingen individ ska kunna tillverka en e-legitimation på egen hand hos utfärdaren.

I dag finns det två godkända kvalitetsgranskade elektroniska identitetshandlingar, Huddinge kommun på tillitsnivå 3 och AB Svenska

Pass på tillitsnivå 4. Den elektroniska identitetshandling som Huddinge kommun har tagit fram är avsedd att tillmötesgå behov av att utfärda elektroniska identitetshandlingar till tjänstemännen i kommunen. Den elektroniska identitetshandling som AB Svenska Pass tillhandahåller har Skatteverket upphandlat och den finns på de identitetskort för folkbokförda i Sverige som Skatteverket utfärdar. Den elektroniska identitetshandlingen fungerar dock inte ännu i alla myndigheters e-tjänster.[9]

14.2.2 Mer om elektroniska identitetshandlingar på den svenska marknaden

BankID

BankID är den mest förekommande lösningen för elektronisk identifiering i Sverige.[10] BankID finns som tre olika lösningar; mobilt BankID, BankID på fil och BankID på kort.

Mobilt BankID innebär att användaren har sin elektroniska identitetshandling i en mobiltelefon eller surfplatta. För att kunna hämta och använda mobilt BankID krävs att användaren har installerat BankID-appen. BankID *på fil* är en elektronisk identitetshandling i en dator. För att kunna hämta och använda BankID på fil krävs att användaren har installerat BankID-programmet. BankID *på kort* är en elektronisk identitetshandling som är lagrad på ett s.k. smartkort.[11] Förutom kortet och BankID-programmet krävs även att man har en kortläsare.

Det finns i dag elva banker som utfärdar BankID.[12] Vilka lösningar som de olika bankerna erbjuder sina kunder skiljer sig åt mellan bankerna.

Danske Bank, Nordea och Swedbank utfärdar alla tre BankID-lösningar, alltså BankID på fil, på kort och mobilt BankID.

Handelsbanken och SEB utfärdar BankID på kort och Mobilt BankID.

---

[9] www.skatteverket.se, 2017-12-09.
[10] 90 procent av befolkningen i åldrarna 20–40 år har minst ett BankID, med Mobilt BankID som dominerande bärare, www.bankid.com, 2017-12-09.
[11] Ett smartkort är ett kort som är försett med ett chip på vilket elektronisk information kan lagras.
[12] Danske Bank, Nordea, Swedbank, Handelsbanken, SEB, Ica Banken, Ålandsbanken, Ikano Bank, Länsförsäkringar, Skandia och Sparbanken, www.bankid.com, 2017-12-08.

Ica Banken och Ålandsbanken utfärdar endast mobilt BankID medan Ikano Bank endast utfärdar BankID på fil.

Länsförsäkringar, Skandia och Sparbanken syd utfärdar BankID på fil och mobilt BankID.[13]

Bankerna stöds av företaget Finansiell ID-teknik BID AB (i det följande Finansiell ID-teknik). Finansiell ID-teknik bildades 2002. Innan företaget bildades hade de stora bankerna i Sverige inlett ett arbete i ett bankkonsortium. Syftet med det arbetet var att ta fram en generell infrastruktur för elektroniska identitetshandlingar, som skulle uppfylla krav från myndigheter och banker och kunna accepteras av allmänhet och företag.[14]

AB Svenska Pass

Skatteverkets identitetskort för folkbokförda i Sverige innehåller en elektronisk identitetshandling som från och med september 2017 utfärdas av AB Svenska Pass.

Telia

Telia utfärdar också elektronisk identitetshandling som kan användas av individer för elektronisk identifiering mot bl.a. e-tjänster.[15] Fram till hösten 2017 var det Telias elektroniska identitetshandling som fanns på Skatteverkets identitetskort för folkbokförda i Sverige.

Freja eID

Företaget Verisec utfärdar en elektronisk identitetshandling som heter Freja eID.[16] Enligt uppgift från E-legitimationsnämndens kansli har Freja eID ansökt om att bli granskade av E-legitimationsnämnden och granskningen pågår.

[13] www.bankid.com, 2017-12-08.
[14] www.bankid.com, 2017-12-08.
[15] www.telia.se, 2017-12-09.
[16] www.verisec.com/sv/autentisering/frejaeid/, 2017-12-09.

Fler pågående aktiviteter

Utöver det som beskrivits i det föregående kan utredningen konstatera att följande aktiviteter identifierats under utredningens arbete.

- Försäkringskassan kommer under 2018 att lansera mobila e-legitimationer till offentliganställda kopplat till Myndighets CA (MCA) för användning i tjänsten.
- Försäkringskassan och Inera AB arbetar med att ta fram en ny gemensam funktion för elektroniska identitetshandlingar i tjänsten; E-identitet För Offentlig Sektor (EFOS).
- Projektet SE-leg, som drivs av SUNET.

14.3 Lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling

Utredningen bedömer:
att det arbete som E-legitimationsnämnden gjort för att ta fram tillitsramverk och tekniska specifikationer, liksom kvalitetsmärkning av elektroniska identitetshandlingar, är sådant som bör lyftas upp och författningsregleras samt
att det finns andra framtida funktioner som också bör författningsregleras.

Utredningen föreslår:
att funktionerna ska regleras i lag och att den myndighet som regeringen bestämmer ska ansvara för att dessa funktioner förvaltas och utvecklas.

Förslaget genomförs genom lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

Tekniken utvecklas hela tiden, liksom sättet att använda sig av de tekniska hjälpmedel som finns. En utmaning vid författningsreglering är därför att hålla författningstexter så teknikneutrala som möjligt. Utredningen bedömer att det är viktigt att inte låsa författningstexten

vid en viss teknik, samtidigt som det är viktigt att författningsreglera sådana funktioner som ska vara ett offentligt åtagande. Utgångspunkter för utredningens förslag är att de ska vara tillåtande, gränssättande och skapa förutsättningar för utveckling, men också ramar för vad som gäller för de olika inblandade aktörerna.

Uppgifter i lag, inte i instruktion

Utredningen har tidigare konstaterat att flera av de uppgifter som E-legitimationsnämnden i dag utför, inte framgår uttryckligen av nämndens instruktion. Utredningen bedömer att förekomsten av tillitsramverk och tekniska specifikationer borgar för transparens i förhållande till aktörerna på marknaden. Det bör därför framgå av lag att dessa funktioner ska finnas, liksom att det är ett statligt ansvar att tillhandahålla dem. Utredningen bedömer därför att det arbete som E-legitimationsnämnden utfört för att ta fram tillitsramverk och tekniska specifikationer, liksom kvalitetsmärkning av elektroniska identitetshandlingar, bör författningsregleras.

Vilka funktioner

Utredningen har ovan bedömt att lagen huvudsakligen ska peka ut vilka funktioner som staten bör ta ansvar för att tillhandahålla, samt vem som ska ansvara för dessa. De funktioner som utredningen bedömer att lagen ska omfatta är tillitsramverket och tekniska specifikationer för elektroniska identitetshandlingar, kvalitetsmärket Svensk elektronisk identitetshandling, ett register med utfärdare av elektroniska identitetshandlingar som har kvalitetsmärket samt en funktion med valbara elektroniska identitetshandlingar.

Ansvar för att utveckla och förvalta funktionerna

Av direktiven till organisationskommittén framgår att regeringen avser att föra över E-legitimationsnämndens verksamhet till den nya myndigheten för digitalisering av den offentliga sektorn.[17] Detta över-

[17] Dir. 2017:117.

ensstämmer med det förslag som utredningen tidigare lämnat. Vad utredningen här föreslår innebär ingen förändring av myndighetsuppdraget.

14.3.1 Begrepp

Utredningen bedömer:
att begrepp som används för att beskriva elektronisk identifiering och vilka aktörer som är inblandade måste vara enhetliga.

Utredningen föreslår:
att det i lagen förs in en begreppslista.

Det förekommer många olika begrepp i sammanhang med elektronisk identifiering. Det är också många olika yrkeskategorier som ska tolka och förstå de begrepp som avses. Med en begreppslista i lag menar utredningen att det skapas en större tydlighet för samtliga inblandade aktörer. De begrepp som utredningen bedömer ska ingå i lagen, med begreppsförklaringar är:

1. *användare:* den som har en elektronisk identitetshandling,
2. *elektronisk identitetshandling:* en värdehandling som en användare kan använda för att identifiera sig elektroniskt,
3. *fysisk bärare:* en fysisk identitetshandling, en koddosa eller liknande,
4. *mobil bärare:* exempelvis en smarttelefon eller en surfplatta,
5. *förlitande aktör:* den som behöver verifiera en användares uppgifter vid identifiering mot en e-tjänst,
6. *utfärdare:* den som utfärdar en elektronisk identitetshandling till en användare,
7. *tillitsramverk:* ett graderat ramverk för tillförlitlighet i utfärdade elektroniska identitetshandlingar,
8. *tillitsnivå:* en nivå inom tillitsramverket,
9. *tekniska specifikationer:* tekniska krav som ställs på en elektronisk identifiering,

10. *modell för dialogruta med valbara elektroniska identitetshandlingar:* gruppering av elektroniska identitetshandlingar som har kvalitetsmärket Svensk elektronisk identitetshandling och som presenterar dessa i en dialogruta för användaren när denne ska identifiera sig elektroniskt.

14.3.2 Tillitsramverk

Utredningen bedömer:
att ett tillitsramverk som är gemensamt för offentliga och privata aktörer skapar förutsättningar för säkra och tillförlitliga elektroniska identitetshandlingar.

Utredningen föreslår:
att det i lag anges att det ska finnas ett tillitsramverk samt
att digitaliseringsmyndigheten ges i uppgift att förvalta och utveckla tillitsramverket.

En elektronisk identitetshandling ska vara utformad, skyddas och användas enligt en viss tillitsnivå. Utfärdare av elektroniska identitetshandlingar ska tillämpa sådana regler och rutiner att det utifrån tillämplig tillitsnivå finns fog för att lita på de elektroniska identitetshandlingar som tillhandahålls. E-legitimationsnämnden tar i dag fram ett tillitsramverk för elektroniska identitetshandlingar. Tillitsramverket och de tekniska specifikationerna utformas med beaktande av internationellt framtagna standarder. Det bör ankomma på digitaliseringsmyndigheten att säkerställa att det finns ett tillitsramverk samt att detta är följsamt med de standarder och utvecklingen i övrigt samt de hot och risker som kan uppkomma på området. Utredningen bedömer att förekomsten av ett tillitsramverk ska regleras i lag. Den närmare utformningen av tillitsramverket, dvs. utvecklingen och förvaltningen av tillitsramverket ska lämnas till digitaliseringsmyndigheten.

14.3.3 Tekniska specifikationer

Utredningen föreslår:
att det i lag ska anges att det ska finnas tekniska specifikationer för elektronisk identitetskontroll, dvs. identitetsintyg kopplade till användning av elektroniska identitetshandlingar, samt
att digitaliseringsmyndigheten ges i uppdrag att utveckla och förvalta sådana tekniska specifikationer.

Elektronisk identitetskontroll kräver att utfärdare av elektroniska identitetshandlingar och förlitande aktörer samverkar. Ju enhetligare sätt att angripa elektronisk identitetskontroll på, desto högre grad av effektivitet skapas. Utredningen bedömer att det är lämpligt att en myndighet ansvarar för att ta fram tekniska specifikationer som gäller för elektronisk identitetskontroll på marknaden. Detta i syfte att underlätta för samtliga aktörer, alltså för såväl utfärdare som förlitande aktörer.

Liksom för tillitsramverket ska de tekniska specifikationer som tas fram vara följsamma mot väletablerade standarder och utvecklingen i övrigt samt de hot och risker som kan uppkomma på området. De tekniska specifikationerna ska också utformas på så sätt att regler om regler om personuppgiftshantering beaktas.

Utredningen bedömer att förekomsten av tekniska specifikationer ska regleras i lag. Den närmare utformningen av de tekniska specifikationerna, dvs. förvaltningen och utvecklingen av dem ska lämnas till digitaliseringsmyndigheten.

14.3.4 Kvalitetsmärket Svensk elektronisk identitetshandling

Utredningen bedömer:
att individer måste ges bättre möjligheter att kunna avgöra vilka elektroniska identitetshandlingar som är säkra och tillförlitliga,
att en kvalitetsmärkning av elektroniska identitetshandlingar kan bidra till att individer lättare kan välja bland flera utfärdare.

Utredningen föreslår:
att staten ska ansvara för att granska elektroniska identitetshandlingar mot tillitsramverket och elektronisk identitetskontroll mot de tekniska specifikationerna.
att det i lag anges att det ska finnas ett kvalitetsmärke för elektroniska identitetshandlingar som heter Svensk elektronisk identitetshandling,
att digitaliseringsmyndigheten ges i uppgift att kvalitetsgranska elektroniska, samt
att digitaliseringsmyndigheten ges i uppgift att marknadsföra kvalitetsmärket.

Kvalitetsmärket heter i dag Svensk e-legitimation. Utredningen har som tidigare beskrivits valt att använda begreppet elektronisk identitetshandling. Eftersom utredningen konsekvent förhåller sig till begreppet elektronisk identitetshandling i beskrivningen av förslagen, ska ett kvalitetsmärke inte heta Svensk e-legitimation. Utredningen föreslår att kvalitetsmärket ska heta Svensk elektronisk identitetshandling.

Utredningen har tidigare beskrivit att det finns en spretighet på marknaden för elektroniska identitetshandlingar. Vissa elektroniska identitetshandlingar, de som AB Svenska Pass och Huddinge kommun, utfärdar är kvalitetsmärkta. Andra, som BankID, är inte kvalitetsmärkta men har trots det en mycket hög andel användare.

Det är få utfärdare av elektroniska identitetshandlingar som låter sig granskas av E-legitimationsnämnden. Det beror sannolikt på en rad saker.

En anledning är att individer ännu inte frågar efter kvalitetsmärkta elektroniska identitetshandlingar. Kvalitetsmärket är sannolikt inte känt bland allmänheten, och vanan att använda sig av etablerade lösningar för elektronisk identifiering innefattar inte sådana elektroniska identitetshandlingar som är kvalitetsmärkta. BankID har som ovan beskrivits inte låtit sig granskas av E-legitimationsnämnden. Eftersom det redan finns en vana hos den svenska befolkningen att identifiera sig elektroniskt och anskaffa elektroniska identitetshandlingar som saknar kvalitetsmärket måste befolkningen uppmärksammas på vad kvalitetsmärkningen innefattar. Det måste skapas incitament hos individer att fråga efter elektroniska identitetshandlingar som har kvalitetsmärket.

En annan anledning är, enligt utredningen, att en granskning i sig inte leder till att den elektroniska identitetshandlingen kan användas hos statliga myndigheter, kommuner och landsting eller på den privata marknaden. Det finns ingen direkt koppling mellan att få kvalitetsmärket och att få sälja sin funktion till en viss målgrupp. En utfärdare av elektroniska identitetshandlingar kan alltså låta bli att låta sig granskas och kan ändå sälja sina funktioner för elektronisk identifiering till offentliga myndigheter, såväl inom ramen för valfrihetssystem enligt eLOV, som inom ramen för upphandlingsförfaranden enligt LOU.

Vad som nu beskrivits föranleder utredningen att dra slutsatsen att kvalitetsmärket i dag saknar status, både hos individer men också hos utfärdare av elektroniska identitetshandlingar. Slutsatsen kan föranleda olika åtgärder. Det första är givetvis ett ifrågasättande om det alls ska finnas något kvalitetsmärke för elektroniska identitetshandlingar i Sverige. Såsom regelverket ser ut i dag menar utredningen att det finns goda skäl att överväga det alternativet. Utredningen bedömer emellertid att det finns anledning att behålla och stärka kvalitetsmärket. Skälen till det är följande.

En elektronisk identitetshandling är en värdehandling. Den används för att visa en individs identitet elektroniskt, utan att individen behöver visa upp sin person. Hela det digitala samhället bygger på att inblandade aktörer kan lita på att individer är de som de utger sig för att vara elektroniskt. En elektronisk identitetshandling kan ses som en elektronisk urkund om den har en utställarangivelse som kan kontrolleras på ett tillförlitligt sätt.[18]

Mot den bakgrunden är det viktigt att de elektroniska identitetshandlingar som utfärdare tillhandahåller är säkra och tillförlitliga. Det är också viktigt att individer vet vilka elektroniska identitetshandlingar, och vilka utfärdare, som de kan lita på. Detsamma gäller för förlitande aktörer. Kvalitetsmärket kan tjäna sådana syften.

[18] Jfr 14 kap. 1 § brottsbalken (1962:700): En elektronisk handling som upprättats till bevis eller annars är av betydelse som bevis och som har en utställarangivelse som kan kontrolleras på ett tillförlitligt sätt. Härmed avses enligt propositionen att angivelsen ska ha en inte obetydlig grad av säkerhet, vilket i nuvarande skede i it-utvecklingen anges innebära att den elektroniska underskriften uppfyller kraven på kvalificerade eller avancerade signaturer i lagen (2000:832) om kvalificerade elektroniska signaturer (prop. 2012/13:74 s. 45). Lagen om kvalificerade elektroniska signaturer upphävdes den 1 juli 2016 och ersattes av lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, se prop. 2015/16:72.

Utredningen anser därför att kvalitetsmärket tjänar ett angeläget syfte i det digitala samhället, och i synnerhet för den digitala offentliga förvaltningen. Därför föreslår utredningen att kvalitetsmärket och uppgiften att utfärda detta författningsregleras i den nu föreslagna lagen.

Ansökan

Utredningen föreslår att digitaliseringsmyndigheten ska granska elektroniska identitetshandlingar. Granskningen ska göras mot såväl tillitsramverket som de tekniska specifikationerna. En elektronisk identitetshandling som motsvarar de krav som ställs får som tillägg till sitt eget namn använda kvalitetsmärket Svensk elektronisk identitetshandling.

Det är i dag E-legitimationsnämnden som efter ansökan prövar elektroniska identitetshandlingar mot tillitsramverket. Det framgår inte av E-legitimationsnämndens instruktion att nämnden har denna uppgift. Utredningen bedömer att det är lämpligt att det i den föreslagna lagen också regleras att ansökan om att få kvalitetsmärket ska göras hos den myndighet som regeringen bestämmer. På så sätt regleras inte bara att det ska finnas ett kvalitetsmärke, utan också att det finns en statlig myndighet som har ansvar för att tilldela elektroniska identitetshandlingar detta.

Utredningen menar att prövningen ska göras mot tillitsramverket vilket innebär att elektroniska identitetshandlingar på samtliga tillitsnivåer som tillitsramverket omfattar kan få kvalitetsmärket. Utredningen föreslår att prövningen också ska göras mot de tekniska specifikationer som tas fram. Det blir en skillnad i förhållande till i dag när prövningen endast görs mot tillitstramverket. Utredningen menar emellertid att det på detta sätt blir tydligare för såväl leverantörer som förlitande aktörer vilken teknik som ska användas för de identitetsintyg som skickas på begäran av den förlitande aktören. Utredningen anser att det borde leda till en bättre förutsebarhet på marknaden för samtliga inblandade aktörer.

14.3.5 Register med utfärdare av elektroniska identitetshandlingar och förlitande aktörer

Utredningen föreslår:
att det i lagen anges att det ska finnas ett register med uppgift om utfärdare av elektroniska identitetshandlingar med kvalitetsmärket Svensk elektronisk identitetshandling och förlitande aktörer som är anslutna till valfrihetssystem enligt lagen om valfrihetssystem i fråga om funktion för elektronisk identitetskontroll,
att digitaliseringsmyndigheten ges i uppgift att förvalta och utveckla ett sådant register, samt
att den närmare regleringen av vilka uppgifter som ska finnas i registret måste tas fram i samband med utvecklingen av registret.

Utredningen bedömer att det behövs ett register med de utfärdare av elektroniska identitetshandlingar som har kvalitetsmärket Svensk elektronisk identitetshandling och de förlitande aktörer som är anslutna till valfrihetssystem enligt eLOV. Ett sådant register kan bestå bl.a. av uppgifter om de anslutna aktörernas elektroniska adresser. Utredningen föreslår att digitaliseringsmyndigheten ska ges i uppgift att ta fram och förvalta ett sådant register. Registrets utformning, vilka uppgifter som behöver behandlas, vem som ska ges åtkomst till uppgifterna och hur åtkomsten ska regleras är frågor som bör ingå i uppgiften. Utgångspunkten bör vara att personuppgifter inte ska behandlas i registret. Undantag från den huvudregeln kan behöva göras för de som är ombud för aktörerna i registret. En annan utgångspunkt för registret bör vara att det inte ska innehålla information om den kommunikation som förekommer mellan användare och förlitande aktörer.

Utredningen lämnar inget förslag till reglering av personuppgiftsansvaret när det gäller detta register eftersom det förslag utredningen lämnar avser ett kommande register. Utredningen vill emellertid framhålla vikten av att ett register av detta slag förhåller sig till dataskyddsförordningen.[19] Det måste alltså parallellt med utvecklingen av registret tas fram ett förslag om hur eventuella personuppgifter i det ska behandlas.

[19] Förordning (EU) 2016/679 om skydd för enskilda personer med avseende på behov av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

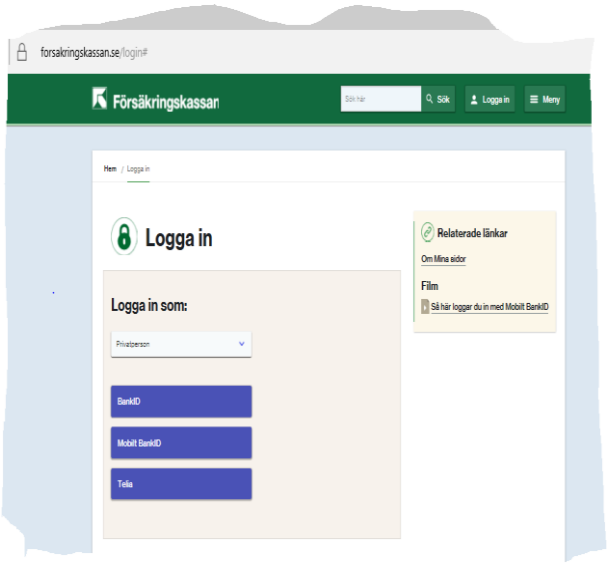
14.3.6 Modell för dialogrutor med valbara elektroniska identitetshandlingar

Utredningen bedömer:
att en individs användarupplevelse vid elektronisk identifiering ska vara densamma, oavsett vilken offentlig myndighet som individen vill identifiera sig elektroniskt mot.
att det av användarupplevelsen ska framgå att individen *identifierar sig* för åtkomst till en e-tjänst.

Utredningen föreslår:
att det i lag anges att det ska finnas en modell för hur dialogrutor för valbara elektroniska identitetshandlingar ska se ut, samt
att digitaliseringsmyndigheten ges i uppgift att utveckla och förvalta modellen.

När individer använder e-tjänster hos olika myndigheter möts de av olika dialogrutor för att välja elektronisk identitetshandling. Hos Skatteverket och Försäkringskassan ser det ut på följande sätt:

Figur 14.1 Skärmdump från Försäkringskassans inloggningssida



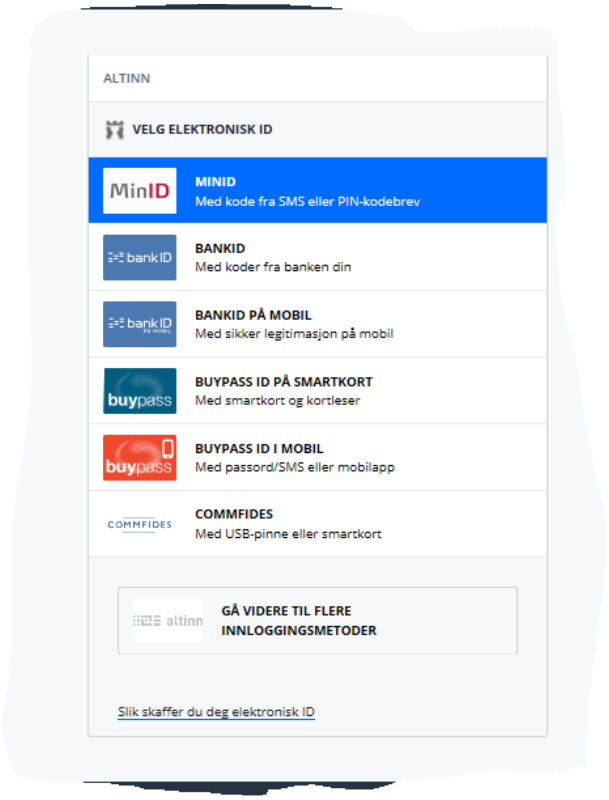
Källa: www.forsakringskassan,se

Figur 14.2 Skärmdump från Skatteverkets inloggningssida

Källa: www.skatteverket.se

Anledningen till att det ser olika ut är att varje myndighet själv bestämmer hur denna dialogruta ska se ut. Dessutom kan de olika alternativen för identifiering också skilja sig åt mellan myndigheterna eftersom det i dagsläget inte är samordnat vilka funktioner för elektronisk identifiering, alltså vilka elektroniska identitetshandlingar, som myndigheterna ska använda sig av. I Norge ser det ut som följer när en individ ska identifiera sig i e-tjänster i den offentliga förvaltningen.

Figur 14.3 Skärmdump från inloggningssida Altinn i Norge



Källa: www.altinn.no

Individer ska känna igen sig oavsett offentlig myndighet

Utredningen lämnar förslag om att alla offentliga myndigheter ska erkänna den statliga elektroniska identitetshandlingen, liksom att de ska ansluta sig till de valfrihetssystem som digitaliseringsmyndigheten anordnar. Därmed skapas förutsättningar för att offentliga myndigheter kommer att erbjuda individer samma valmöjligheter för elektronisk identifiering. De alternativ för elektronisk identifiering som därmed skapas bör erbjudas individer på ett för offentliga myndigheter ensat sätt. Utredningen bedömer att det är lämpligt att individer som ska använda sig av e-tjänster hos offentliga myndigheter får samma användarupplevelse, dvs. att de känner igen den dialogruta de möts av vid identifieringsmomentet och att samtliga valbara elektroniska identitetshandlingar visas för användaren på samma sätt. I denna dialogruta

för valbara elektroniska identitetshandlingar ska såväl den statliga elektroniska identitetshandlingen finnas som alternativet ”foreign eID” dvs. utländsk elektronisk identitetshandling. Det alternativet ska väljas av de användare som har en elektronisk identitetshandling som är anmäld för gränsöverskridande identifiering enligt eIDAS-förordningen.[20] Därtill bedömer utredningen att alla de elektroniska identitetshandlingar som finns inom valfrihetssystem ska visas i dialogrutan.

Utredningen föreslår därför att digitaliseringsmyndigheten ska ta fram en modell för hur en dialogruta för valbara elektroniska identitetshandlingar[21] ska se ut. Denna modell ska sedan kunna användas av offentliga myndigheter för att ta fram egna dialogrutor som ger förutsättningar för att individer får samma användarupplevelse oavsett vilken offentlig myndighet det handlar om. Det blir alltså digitaliseringsmyndighetens uppgift att ta fram modellen för dialogrutan, medan respektive offentlig myndighet ska ansvara för att tillhandahålla sin en dialogruta. Utredningen bedömer att det kan vara lämpligt att digitaliseringsmyndigheten verkar för att mindre offentliga myndigheter samverkar om framtagandet av dialogrutan.

Information om att en individ identifierar sig elektroniskt

Utredningen bedömer också att de dialogrutor för valbara elektroniska identitetshandlingar som tillhandahålls utifrån modellen ska innehålla information om att individen *identifierar sig* för att få komma åt en e-tjänst. Det är enligt utredningen viktigt att göra det tydligt för användare att de vid elektronisk identifiering faktiskt använder sig av en elektronisk identitetshandling. Som många dialogrutor är utformade i dag, inleds förfarandet med att användaren ska *logga in*.[22] För användaren kan det innebära en otydlighet om användaren inte förstår att han eller hon använder sig av en elektronisk värdehandling. Därför är det enligt utredningen viktigt att offentliga myndigheters dialogruta för valbara elektroniska identitetshandlingar innehåller information

[20] Dessa användare behöver en egen gemensam dialogruta där de får välja land och därefter dirigeras via den svenska noden för bekräftelse av identiteten.
[21] Tidigare kallad anvisningstjänst.
[22] https://computersweden.idg.se/2.2683/1.693238/e-id-varning?queryText=legitimering, 2017-11-27.

om att användaren *identifierar sig* genom att använda någon av de alternativa elektroniska identitetshandlingar som visas.

14.3.7 Skyldighet att använda dialogruta för valbara elektroniska identitetshandlingar

Utredningen föreslår:
att offentliga myndigheter som kräver att användare av e-tjänster ska identifiera sig elektroniskt ska tillhandahålla en dialogruta för valbara elektroniska identitetshandlingar utifrån den modell för ändamålet som digitaliseringsmyndigheten tar fram,
att regeringen får besluta om undantag för en offentlig myndighet att använda den modell för hur dialogrutor för valbara elektroniska identitetshandlingar ska se ut, om det finns särskilda skäl.

Modellen ska användas …

Utredningen bedömer att det är viktigt ur ett användarperspektiv att individer får samma upplevelse av dialogen att välja elektronisk identitetshandling oavsett vilken offentlig myndighet de vänder sig till. Utredningen har övervägt på vilket sätt offentliga myndigheter ska styras till att ensa användarupplevelsen av valbara elektroniska identitetshandlingar. Härvid har utredningen övervägt att reglera detta genom föreskriftsrätt eller lagstiftning. För att det ska få genomslag på alla offentliga myndigheter har utredningen kommit fram till att lagformen är den mest ändamålsenliga. Den betonar att det är fråga om att säkerställa att alla individer som ska identifiera sig mot offentliga myndigheter möts av samma dialogruta, i vilken de elektroniska identitetshandlingar som finns inom ett valfrihetssystem presenteras, liksom den statliga elektroniska identitetshandlingen.

Utredningen har vidare övervägt hur en bestämmelse för offentliga myndigheter ska utformas. Härvid kan konstateras att en bestämmelse kan skilja sig åt beroende på om det avser en statlig myndighet, en kommun eller ett landsting. Exempelvis skulle det kunna regleras att statliga myndigheter *ska* använda modellen, medan kommuner och landsting *får* använda den. En sådan utformning påminner då om det sätt som utredningen föreslår att statliga myndigheter, kommuner

och landsting ska respektive får ansluta sig till infrastrukturen för Mina meddelanden. Bestämmelsen skulle också kunna utformas utifrån hur stor volym en statlig myndighet, en kommun eller ett landsting står för när det gäller elektronisk identifiering. Det är då tänkbart att utforma regelverket på så sätt att stora offentliga myndigheter *ska* använda modellen, medan små *får* använda den.

En dialogruta för valbara elektroniska identitetshandlingar är någonting som alla offentliga myndigheter med e-tjänster måste ha. Med beaktande av utredningens förslag att offentliga myndigheter ska ansluta sig till valfrihetssystem som digitaliseringsmyndigheten tillhandahåller finner utredningen att det är lämpligt att utforma styrningen av de offentliga myndigheterna på samma sätt när det gäller användningen av modellen för utformning av dialogruta för valbara elektroniska identitetshandlingar. Utredningen anser att individers användarupplevelse ska vara densamma oavsett vilken offentlig myndighet som han eller hon identifierar sig mot.

… om det inte finns särskilda skäl

Många offentliga myndigheter är i dag bundna av avtal för tjänster för elektronisk identifiering. Dessa avtal har slutits på olika sätt, vid olika tidpunkter och med olika lång bindningstid. Det gör att offentliga myndigheter kan ha svårt att följa bestämmelsen som utredningen föreslår under den tid som de är bundna av andra avtal. Utredningen bedömer att avtal som hindrar att en offentlig myndighet använder sig av modellen kan vara särskilda skäl.

14.3.8 Ikraftträdande

Utredningen föreslår:
att den föreslagna lagen ska träda i kraft den 1 januari 2020.

Lagen reglerar många av de uppgifter som E-legitimationsnämnden utför i dag samt nya uppgifter som utredningen har bedömt nödvändiga. Utredningen föreslår att lagen ska träda i kraft den 1 januari 2020. Därmed skulle den författningsreglering som utredningen föreslår för elektroniska identitetshandlingar och elektronisk identifiering träda i kraft vid samma tidpunkt.

15 Arbetstagare, student, ställföreträdare – och elektronisk identifiering

15.1 Identitetshandling i tjänsten eller behörighetskontroller?

Individer behöver identifiera sig i många sammanhang. I vissa fall är det tillräckligt att identifiera sig, dvs. visa vem man är. I andra fall måste man visa vem man är i en viss kontext, exempelvis att man är anställd hos en viss arbetsgivare. I de fallen uppkommer ofta fråga om en åtgärd som en individ vidtar är i tjänsten eller som privatperson. Att en individ förekommer i en viss kontext är heller inte unikt för relationen arbetstagare och arbetsgivare. Personer som studerar har en relation till sin skola, liksom personer som agerar som ombud[1] eller ställföreträdare[2] har en relation till sin uppdragsgivare.

I samtliga nämnda fall är det intressant att bedöma vem som ska ha information om detta; individen, den som ska kontrollera identiteten eller den som utfärdar en identitetshandling.

Kontext innebär en relation mellan en individ och något annat; en organisation, ett företag eller en annan person. I stället för kontext kan man beskriva det som att individen intar olika *roller*. I utredningen ingår främst att lämna förslag som avser elektroniska identitetshandlingar i tjänsten.

[1] Med ombud menar utredningen exempelvis den som uppträder som rättegångsombud eller agerar på fullmakt för en individ.
[2] Med ställföreträdare menar utredningen här exempelvis den som för talan för en person som saknar processhabilitet (t.ex. en förvaltare) eller den som tecknar en juridisk persons firma.

15.2 Processen för identifiering när en individ har en roll eller ställning

Utredningen har i tidigare kapitel beskrivit hur den elektroniska identifieringsprocessen ser ut gentemot en e-tjänst. Kortfattat innebär identifieringsprocessen då att användaren väljer vilken elektronisk identitetshandling som han eller hon vill använda för att identifiera sig för inloggning. Den förlitande aktören (alltså den som tillhandahåller e-tjänsten) ställer en fråga till utfärdaren av den elektroniska identitetshandlingen om användarens identitet och får ett s.k. identitetsintyg tillbaka. Identitetsintyget innehåller uppgifter om användarens identitet. I dag innehåller identitetsintygen oftast personnummer och namn. Identitetsintygen innehåller inte uppgift om användarens (individens) roll eller ställning.

Inom E-delegationen etablerades en princip för organisationstillit i syfte att effektivisera arbetet med informationsutbyte mellan offentliga aktörer. Principen bygger på att det vid informationsutbyte inom ramen för myndigheternas samverkans- och serviceskyldighet räcker att kontrollera att den andra parten är den myndighet som den uppger sig vara, eftersom en myndighet vanligtvis kan lita på att en handläggare som agerar för en annan myndighets räkning är behörig att företräda myndigheten. Principen bygger på förvaltningslagens regler om myndigheternas samverkansskyldighet samt att varje myndighet själv ansvarar för sin interna kontroll.[3] Ett exempel på organisationstillit är den system-till-system-lösning som finns inom rättsväsendets informationsförsörjning, RIF. I RIF skickas information direkt mellan myndigheternas verksamhetsstöd. Någon särskild identifieringslösning har därför inte bedömts nödvändig eftersom utbytena bygger på att varje mottagande myndighet litar på att den information som förmedlas kommer från en behörig tjänsteman hos den avsändande myndigheten.[4] Det är i den avsändande myndighetens eget stöd som tjänstemännens behörigheter kontrolleras. Den mot-

[3] eSam:s rapport En effektiv informationsförsörjning, s. 63.

[4] Ett exempel på hur lagstiftningen kan sägas ha följt principen om organisationstillit är 45 kap. 4 § rättegångsbalken. Av bestämmelsen följer att en stämningsansökan som huvudregel ska vara egenhändigt undertecknad. En stämningsansökan som ges in elektroniskt ska emellertid vara undertecknad med en sådan elektronisk underskrift som avses i artikel 3 i eIDAS-förordningen eller överföras på ett sätt som uppfyller motsvarande grad av säkerhet. Det sista ledet i bestämmelsen menar utredningen utgör en författningsreglerad organisationstillit.

tagande myndigheten behöver därför inte göra några särskilda kontroller av avsändande tjänsteman.

15.3 Vad är behörighets- och attributstjänster?

15.3.1 E-legitimationsnämnden och Svensk e-legitimation

I betänkandet E-legitimationsnämnden och Svensk e-legitimation beskrev utredningen om bildande av en E-legitimationsnämnd att attributsintyg var elektroniska intyg som lämnade uppgift om behörighet, uppdrag, roll eller andra egenskaper som i traditionell miljö lämnas genom att visa upp en legitimation eller ge in registreringsbevis, fullmakter eller liknande handlingar. Utredningen om bildande av en E-legitimationsnämnd anförde också följande:

> Genom attributsintyg ska myndigheters och företags e-tjänster smidigt kunna förses med ytterligare information om användare som legitimerar sig. Attribut kan vara ett eller flera och kan innehålla vilken information som helst, inom rimliga gränser – och de paketeras ”på samma sätt” som i ett identitetsintyg, dvs. i ett standardiserat format kallat SAML 2.0.[5]

Utredningen om bildande av en E-legitimationsnämnd beskrev vidare att det från juridiska utgångspunkter kunde tas olika perspektiv på hur information om en individ skulle inhämtas eller bifogas en identifiering. Det anfördes att olika lösningar kan komma att väljas utifrån olika praktiska situationer (vilka regler som gäller för personuppgiftshantering etc.). Dessa lösningar bör i praktiken begränsas till vissa typfall som lämpligen kan beskrivas från den praktiska situationen. Om man utgick från individen kunde attributsintyg innehålla information om i vilken form individen är behörig att företräda ett visst företag eller har någon annan egenskap. I de fallen är det upp till den förlitande aktören att utvärdera informationen för att bedöma frågan om behörighet. Om man i stället tog utgångspunkt i ett företag kunde det finnas behov av att bedöma om en viss individ är behörig och genom kompletterande sökningar hos exempelvis Bolagsverket för att inhämta registreringsbevis.[6]

[5] SOU 2010:104, E-legitimationsnämnden och Svensk e-legitimation, s. 38.
[6] SOU 2010:104, E-legitimationsnämnden och Svensk e-legitimation, s. 39.

15.3.2 eSam

eSam har i sin rapport En effektiv informationsförsörjning beskrivit följande om identitetshantering och behörighetshantering.

> Områden som identitetshantering och behörighetshantering blir därmed centrala och behöver en gemensam utformning för hur det ska fungera såväl mellan offentliga aktörer som mellan offentliga aktörer, privatpersoner och företag. Privatpersoner kan agera i olika roller mot det offentliga; t.ex. som ordförande i en samfällighet, firmatecknare i ett bolag eller som privatperson. Privatpersoner kan även agera som ombud i olika former för andra privatpersoner, vilket även behöver kunna hanteras digitalt. Informationsförsörjningen behöver generellt ha stöd för att urskilja i vilken roll en enskild person har kontakt med det offentliga och vilka förutsättningar som föreligger i den specifika rollen.[7]

eSam anför vidare i samma rapport att det behöver tydliggöras om en gemensam attributstjänst för hantering av roller i relation till behörigheter kan vara en effektiv och ändamålsenlig lösning.

15.4 Identifiering i en e-tjänst eller annan identifieringslösning?

Utredningen om bildande av en E-legitimationsnämnd beskrev attributstjänster som tog sikte på fler roller än den som arbetstagare. Beskrivningarna omfattade också ombuds- och ställföreträdarrelationer. Detsamma gäller eSams angreppssätt i rapporten En effektiv informationsförsörjning.

Utredningen bedömer att den beskrivning av attributstjänster som Utredningen om bildande av en E-legitimationsnämnd gjorde huvudsakligen utgick från att identifieringen skulle göras mot en e-tjänst. Det beskrivs att identitetskontrollen resulterar i ett identitetsintyg, som kan förses med attributsintyg av olika slag.[8] Implementeringen av utredningen om bildande av en E-legitimationsnämnds tankar har emellertid inte blivit på det sätt som beskrivits. Utredningen har erfarit att det i stället har blivit fråga om en standarduppsättning i identitetsintygen som består av namn och personnummer.

[7] eSam, En effektiv informationsförsörjning s. 32.
[8] SOU 2010:104, E-legitimationsnämnden och Svensk e-legitimation, s. 38 ff.

Ovan har utredningen beskrivit att det inte är alla elektroniska identifieringar som ska göras mot e-tjänster och att detta särskilt gäller sådana elektroniska identifieringar som utförs i tjänsten.

15.5 Viktigt att utgå från praktiska fall, men dessa är inte generiska

Utredningen instämmer i den bedömning som Utredningen om bildande av en E-legitimationsnämnd gjorde, dvs. att man i analysen av attributs- och behörighetstjänster måste utgå från olika praktiska fall. Utredningen konstaterar att processer för förmedling och inhämtande av uppgifter med bäring på olika roller, främst de som avser ombud eller ställföreträdarskap, kan skilja sig åt mellan olika offentliga myndigheter. Vid en jämförelse mellan förvaltningslagens och rättegångsbalkens bestämmelser framgår följande. Av förvaltningslagen följer att myndigheter vid handläggning av ärenden ska beakta möjligheten att själv inhämta upplysningar och yttranden från andra myndigheter, om sådana behövs.[9] Av rättegångsbalken följer att parters första inlaga ska innehålla uppgifter som både visar domstolens behörighet samt kan tjäna som underlag för delgivning.[10] Part som vill ställa ett ombud för sig ska lämna ombudet fullmakt. Fullmakten ska visas upp i original när ombudet första gången för talan i målet.[11] När det gäller förvaltningslagen innebär bestämmelsen att myndigheten själv ska inhämta uppgifter, medan rättegångsbalken föreskriver att parten ska förse domstolen med uppgifterna.[12] De refererade bestämmelserna beskriver inte samma situation, men angreppssätten är enligt utredningen intressanta på så sätt att det finns processregler som medför att ansvaret för att förse myndigheter med uppgifter kan skilja sig åt mellan myndigheter. I bland måste myndigheten aktivt hämta och eftersöka uppgifter om en individs roll, andra gånger måste individer förse myndigheter med dessa uppgifter.

[9] 7 § förvaltningslagen (1986:223). Motsvarande bestämmelse finns också i 8 § andra stycket i den nya förvaltningslagen (2017:900) som träder i kraft den 1 juli 2018.
[10] 33 kap. rättegångsbalken (1942:740).
[11] 12 kap. rättegångsbalken (1942:740.
[12] Det ska dock påpekas att många domstolar också inhämtar sådana uppgifter från centrala register, om inte annat för att kontrollera att uppgifterna stämmer. Motsvarande bestämmelse som i FL saknas dock i RB.

15.6 Något om behörighetshantering

Utredningen kan vidare konstatera att frågan om behörigheter är komplex. Behörigheter kan bedömas utifrån olika perspektiv och behörighet handlar i bland också om befogenhet. En individ – tjänsteman eller ombud – kan vara behörig att vidta vissa åtgärder i tjänsten eller inom ramen för sitt uppdrag. I de fallen bestäms behörigheten av arbetsgivaren eller huvudmannen, som också är den som bäst kan förmedla information om behörigheten till andra. En sådan förmedling kan göras genom en behörighetstjänst. Behörighet kan också bestämmas hos mottagaren och handlar då främst om vilken information en utomstående kan få åtkomst till.

15.7 Pågående initiativ

När det gäller behovet av att kunna identifiera individer i en kontext med elektroniska medel finns det flera pågående arbeten. Vissa initiativ gäller utfärdande av elektroniska identitetshandlingar. Andra gäller att skapa identitetsfederationer. De pågående initiativen innefattar inte endast elektronisk identifiering i tjänsten, utan också elektronisk identifiering i skolans värld och i högskolesektorn.

15.7.1 Elektroniska identitetshandlingar i en kontext

Myndighets CA

Försäkringskassan har arbetat med it-tjänsten Myndighets CA[13] (MCA), som började utvecklas i och med att Servicekontoren öppnades år 2007. Med den lösning som MCA innebär kan en arbetstagare signera exempelvis word- och PDF-dokument eller e-postmeddelanden. Det är också möjligt att med MCA kryptera meddelanden samt att ställa ut s.k. servercertifikat för att säkerställa en maskins äkthet i den egna domänen eller på internet. I dagsläget används tjänsten av servicekontoren, Statens servicecenter, Pensionsmyndigheten, Försäkringskassan, Skatteverket och Kronofogdemyndigheten. Det är För-

[13] CA står för *Certificate Authority*, dvs. en certifikatutfärdare, www.forsakringskassan.se/myndigheter/e-tjanster/myndighets-ca, 2017-12-05.

säkringskassan som ansvarar för drift, förvaltning och vidareutveckling av lösningen, i samverkan med anslutna myndigheter.[14]

Enligt uppgifter från Försäkringskassan[15] är kostnaderna för MCA fördelade på en utvecklingskostnad och en driftskostnad. Dessa prognostiseras för varje år. Den totala summan för 2017 är 185 kronor per användare, och av det beloppet fördelar sig 150 kronor på driftskostnader och 35 kronor på nyutveckling. Beloppen är föremål för revidering och att de sätts utifrån hur många som använder dem.

SITHS

Inera AB[16] har tagit fram SITHS-kortet för personer som är anställda eller uppdragstagare inom landsting, kommuner och privata vårdgivare. Kortet är personligt och används tillsammans med en personlig PIN-kod.[17] Med SITHS-kortet kan arbetstagaren/uppdragstagaren identifiera sig för inloggning i datorer, olika system och e-tjänster, framför allt inom vården men också hos myndigheter. Det är vidare möjligt att signera e-postmeddelanden, avtal, fakturor, journalhandlingar och recept med SITHS-kortet. Kortet kan dessutom användas vid inpassering och utskrifter. Kortet är både en fysisk och en elektronisk identitetshandling.[18]

E-identitet för offentlig sektor – samverkan mellan Försäkringskassan och Inera AB

Inera AB[19] och Försäkringskassan har sedan februari 2016 på eget initiativ drivit ett samverkansprojekt som handlar om tjänsten E-identitet för offentlig sektor. Avsikten med samverkansprojektet är att ersätta både SITHS och Försäkringskassans MCA. E-identitet för offentlig sektor ska lanseras den 3 april 2018. E-identitet för offentlig

[14] www.forsakringskassan.se/myndigheter/e-tjanster/myndighets-ca, 2017-12-05.
[15] Telefonmöte den 27 september 2017 mellan utredningen och Försäkringskassan.
[16] Inera ägs av SKL Företag, landsting, regioner och kommuner. Genom att erbjuda kompetens inom digitalisering stödjer Inera ägarnas verksamhetsutveckling. Inera koordinerar och utvecklar gemensamma digitala lösningar till nytta för invånare, medarbetare och beslutsfattare.
[17] Dvs. att en persons identitet kontrolleras med tvåfaktorsautentisering.
[18] www.inera.se/tjanster/identifieringstjanst-siths/, 2017-12-05.
[19] Inera ägs i dag av SKL Företag AB samt landsting och regioner. Under 2017 har nästan samtliga kommuner i Sverige valt att köpa aktier i Inera AB och därmed också bli delägare.

sektor innebär att identifieringslösningen kan användas tillsammans med annan infrastruktur och s.k. lokala *identity providers* (IdP:er) så länge den lokala lösningen följer referensarkitekturen.[20]

Huddinge kommun

Huddinge kommun utfärdar elektroniska identitetshandlingar till sina anställda, som kan användas i tjänsten för samverkan med myndigheter och medborgare. Deras lösning har granskats och godkänts av E-legitimationsnämnden på tillitsnivå 3 och utfärdas med kvalitetsmärket Svensk e-legitimation.

15.7.2 Identitetsfederationer

En identitetsfederation syftar till att undvika att förlitande aktör måste sluta bilaterala avtal med varje utfärdare av en elektronisk identitetshandling. Syftet med identitetsfederationen är alltså att en aktör utses som ansvarig för federationen, och att varje aktör som vill ansluta sig till federationen måste följa ett uppställt regelverk – såväl tekniskt som tillitsbaserat – samt åtar sig att genomgå prövning och granskning med avseende på säkerhet och uppfyllelse av uppställda regelverk.

Sambi

Sambi[21] stödjer rollbaserad åtkomst till e-tjänster. Det görs genom att det är användarorganisationen som ansvarar för hanteringen av deras användares roller och behörigheter, medan tjänsteleverantörerna ansvarar för att ge tillgång till tjänsten enligt den behörighet som användaren givits av användarorganisationen.

En viktig poäng med Sambi är att känsliga uppgifter som användarnamn och lösenord inte behöver skickas över internet. De lagras inte heller hos tjänsteleverantören. Inloggningen sker hos användarorganisationen som förser tjänsten med relevant information för be-

[20] www.inera.se/aktuellt/projekt/e-identitet-for-offentlig-sektor/, 2017-12-05.
[21] Sambi är ett samarbete mellan eHälsomyndigheten, Inera och IIS (Internetstiftelsen i Sverige).

slut om åtkomst. Sambi är ett samarbete mellan eHälsomyndigheten, Inera och Internetstiftelsen i Sverige.

SWAMID

SWAMID är en identitetsfederation som omfattar de flesta lärosäten, forskningsinstitut och andra myndigheter som är relaterade till svensk forsknings- och utbildningssektor. SWAMID drivs av SUNET.[22] SWAMID innehåller uppgifter om både individen och vilken roll denne har, vilket oftast är student eller anställd.

Skolfederationen

Skolfederationen har en standardiserad inloggningslösning för att förenkla konto- och lösenordshanteringen för såväl användarna på skolsidan, som för leverantörer av olika läromedel, tjänster och system. Med Skolfederation kan eleverna använda en enda inloggning, *single sign-on*, för att komma åt tjänster i skolan samt alla de digitala resurser som skolan abonnerar på online (till exempel läromedel, referensverk eller schemaläggning). Den här lösningen bygger på en internationell öppen standard. Skolfederation har tagits fram under ledning av SIS, Swedish Standards Institute, och drivs av Internetstiftelsen i Sverige.[23]

15.8 Skilj på tjänsteutövning och privata ärenden

Utredningen bedömer:
Arbetstagare ska inte använda sina privata elektroniska identitetshandlingar i tjänsten. Det är arbetsgivares ansvar att säkerställa att arbetstagare kan identifiera sig elektroniskt i tjänsten.

Utredningen har i föregående avsnitt beskrivit att det finns olika sätt för arbetsgivare att lösa elektronisk identifiering för arbetstagare inom sin organisation och i relation till andra. Sättet som det löses på

[22] www.sunet.se/swamid/, 2017-12-06.
[23] www.skolfederation.se/om/, 2017-12-06.

är en teknisk fråga. Tekniken bör emellertid följa de strukturer som finns i fråga om ansvar för att arbetstagare har de medel som behövs för att utföra sin tjänst.

På de allra flesta arbetsplatser finns det digitala verksamhetsstöd. Arbetstagare kan behöva identifiera sig elektroniskt mot dessa, men också mot andra organisationers e-tjänster och i vissa fall andra organisationers verksamhetsstöd. Utredningen anser att arbetsgivare som ställer krav på elektronisk identifiering för att en individ ska kunna utföra sina arbetsuppgifter också ska förse individen med det medel som krävs för att göra detta. En elektronisk identitetshandling som arbetstagare använder i tjänsten är alltså att betrakta som ett verktyg för tjänsten.

15.8.1 Den statliga elektroniska identitetshandlingen är bara för privat bruk …

Utredningen föreslår att alla statliga myndigheter, kommuner och landsting ska godta identifiering med den statliga elektroniska identitetshandlingen. Detta kan tolkas på så sätt att den statliga elektroniska identitetshandlingen kan användas av individer också för att identifiera sig i tjänsten. Utredningen menar emellertid att den statliga elektroniska identitetshandlingen inte ska användas av individer i tjänsten, med det undantag som redovisas i det följande.

Om en arbetsgivare kräver att en anställd använder privat utrustning i arbetet måste detta framkomma av anställningsavtalet. Annars gäller principen att arbetsgivaren tillhandahåller den utrustning arbetet kräver. Vad gäller it-utrustning måste även arbetsgivarens personuppgiftsansvar vägas in. Om personuppgifter behandlas i tjänsten på en privat utrustning så har arbetsgivaren personuppgiftsansvaret och är därför skyldighet att kontrollera utrustningen i fråga. Detta kan innebära att arbetsgivaren får del av den anställdes privata information. Det torde därför vara mindre lämpligt att arbetsgivare kräver att anställda ska använda elektronisk identitetshandling på en privat mobiltelefon. Vid användning av privat elektronisk identitetshandling på kort uppstår inte samma komplikation. Däremot finns en annan omständighet att ta i beaktande.

Den statliga elektroniska identitetshandlingen kan tillhandahållas antingen genom upphandling eller genom att en myndighet utvecklar den själv. I fallet upphandling kan det innebära att den leverantör staten

väljer får en dominerande ställning även på marknaden för identitetshandlingar i tjänsten. Om den elektroniska identitetshandlingen levereras av en myndighet innebär det i stället att staten konkurrerar med leverantörer på denna marknad.

I de flesta fall torde arbetsgivare vilja att det fysiska kort som den elektroniska identitetshandlingen finns på även optiskt förmedlar den behörighet arbetstagaren har, t.ex. genom företagsnamn, avdelning osv. Arbetstagarens behörighet kan nämligen behöva bedömas i sådana sammanhang där kortet inte kan läsas elektroniskt.

Sammantaget innebär detta att det inte är lämpligt att arbetstagare använder samma elektroniska identitetshandling i tjänsten som de använder privat. En arbetsgivare som kräver att en anställd – i sin tjänsteutövning – ska identifiera sig elektroniskt gentemot det egna verksamhetsstödet eller i e-tjänster hos andra aktörer måste enligt utredningens bedömning tillhandahålla den anställde en särskild identifieringslösning.

15.8.2 … men kan användas som underlag för arbetsgivaren att skapa en annan elektronisk identitetshandling

Som arbetsgivare behöver man i många fall kontrollera identiteten hos sina anställda, åtminstone i samband med att de anställs. I de fall arbetsgivaren kontrollerar identiteten på en arbetstagare görs det genom att individen visar upp en fysisk identitetshandling. I bland måste arbetsgivaren också göra säkerhetskontroller på individen. De fysiska identitetshandlingar som staten utfärdar har alltså en betydelse i den identitetskontroll som arbetsgivare gör av sina arbetstagare. Nu är det oftast så att anställningsförfaranden innefattar personliga besök hos arbetsgivaren, men utredningen bedömer att den statliga elektroniska identitetshandlingen på sikt kan användas på motsvarande sätt.

15.9 Organisering och ansvarsfördelning

Utredningen föreslår:
att regeringen ger digitaliseringsmyndigheten i uppdrag att närmare bedöma om E-identitet för offentlig sektor skulle kunna användas i hela den offentliga förvaltningen.

Utredningen bedömer att det är viktigt med samordning av elektronisk identifiering i tjänsten. De lösningar som tas fram ska fungera såväl inom den egna organisationen som i relation till andra aktörer. Det som Försäkringskassan och Inera AB tar fram inom ramen för E-identitet för offentlig sektor kan komma att utvecklas till en funktion som kan användas i hela den offentliga förvaltningen. Det är möjligt att den med tiden blir att bedöma som en förvaltningsgemensam digital funktion. Eftersom arbete alltjämt pågår och en lansering av E-identitet för offentlig sektor inte är planerad förrän våren 2018 bedömer utredningen att det är bäst att avvakta den fortsatta utvecklingen av arbetet. Utredningen föreslår därför att regeringen ger digitaliseringsmyndigheten i uppdrag att närmare bedöma om E-identitet i offentlig sektor kan användas i hela den offentliga förvaltningen, dvs. om arbetet utvecklas till att vara en förvaltningsgemensam digital funktion.

16 eIDAS – syfte och innebörd

Enligt utredningens direktiv ska de rättsliga, ekonomiska och verksamhetsmässiga konsekvenserna för svenska offentliga myndigheter av att erkänna anmälda europeiska elektroniska identitetshandlingar och elektroniska underskrifter i nationella e-tjänster utredas. Det inbegriper bland annat att lämna förslag på hur processen för tilldelning av samordningsnummer till utländska medborgare på distans kan möjliggöras och automatiseras, hur personuppgiftsansvaret bör fördelas samt dess omfattning. Dessutom ska utredningen även utreda behoven av och förutsättningarna för anmälan av svenska elektroniska identitetshandlingar enligt eIDAS-förordningen. Här ingår bland annat att ta ställning till ett eventuellt offentligt åtagande, ekonomiska och rättsliga risker, ersättningsmodell till privata utfärdare av elektroniska identitetshandlingar samt om pseudonym bör användas. Slutligen ska utredningen i denna del även översiktligt kartlägga vilka svenska tjänster som kan komma att omfattas av eIDAS-förordningens krav på betrodda tjänster och den offentliga förvaltningens förväntade framtida behov av sådana tjänster. I följande kapitel (16–20) behandlar utredningen de förutsättningar, bedömningar och förslag som har att göra med eIDAS-förordningen och dess följder.

16.1 Skälen till eIDAS-förordningen

I skälen till eIDAS-förordningen[1] (1–77) anges anledningarna till att förordningen skapades och de syften som eftersträvades när förordningstexten formulerades.

[1] Europaparlamentets och Rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

Skälen till förordningen är inte tvingande reglering och ska därför inte blandas samman med förordningens artiklar som följer efter skälen. För förståelsen av eIDAS-förordningen återges nedan ändå några av de skäl som ledde fram till förordningens lydelse.

Förtroende för nätmiljön (skäl 1–2)

Medlemsstaterna vill genom förordningen bygga upp förtroendet för nätmiljön för att främja den ekonomiska och sociala utvecklingen. Bristande förtroende, särskilt på grund av upplevd brist på rättssäkerhet, anses göra att konsumenter, företag och offentliga myndigheter tvekar att utföra transaktioner på elektronisk väg och att använda nya tjänster. Genom att i förordningen tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter vill medlemsstaterna öka förtroendet för elektroniska transaktioner på den inre marknaden. Därigenom ska effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel öka i unionen.

Ömsesidigt erkännande av elektronisk identifiering (skäl 9 och 12)

Det konstateras att medborgare i de flesta fall inte kan använda sin elektroniska identifiering för att autentisera sig[2] i en annan medlemsstat därför att de nationella systemen för elektronisk identifiering i deras land inte är erkända i andra medlemsstater. Detta elektroniska hinder utestänger enligt skälen tillhandahållare av e-tjänster från möjligheten att fullt ut utnyttja fördelarna med den inre marknaden. Ömsesidigt erkända medel för elektronisk identifiering bör underlätta tillhandahållandet av en rad olika tjänster över gränserna på den inre marknaden och ge företagen möjlighet att verka över gränserna utan att stöta på en mängd hinder i sina kontakter med offentliga myndigheter.

[2] Autentisering innebär en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form.

Medlemsstaternas självbestämmande (skäl 12–13)

Förordningen syftar inte till att ingripa i fråga om elektroniska identitetshanteringssystem och tillhörande infrastrukturer som inrättats i medlemsstaterna. Syftet är att se till att säker elektronisk identifiering och autentisering för åtkomst till gränsöverskridande nättjänster som erbjuds av medlemsstaterna är möjlig.

Medlemsstaterna bör fortsättningsvis ha rätt att för elektronisk identifiering använda eller införa medel för åtkomst till nättjänster. De bör ha möjlighet att själva bestämma om de vill engagera den privata sektorn i tillhandahållandet av dessa medel. De bör inte vara skyldiga att anmäla sina system för elektronisk identifiering till kommissionen. Det ankommer på medlemsstaterna att välja om de till kommissionen vill anmäla alla, några eller inga av de elektroniska identifieringssystem som används på nationell nivå för att få åtkomst till åtminstone offentliga nättjänster eller särskilda nättjänster.

Principer och gränser för ömsesidigt erkännande (skäl 14)

Förordningen bör innehålla villkor för vilka medel för elektronisk identifiering som måste erkännas och hur systemen för elektronisk identifiering bör anmälas. Dessa villkor syftar till att hjälpa medlemsstaterna att bygga upp det förtroende som krävs för varandras system för elektronisk identifiering. Principen om ömsesidigt erkännande bör gälla om den anmälande medlemsstatens system för elektronisk identifiering uppfyller villkoren för anmälan och om anmälan har offentliggjorts. Principen om ömsesidigt erkännande bör dock endast avse autentisering för en nättjänst. Åtkomsten till nättjänsten och dess slutliga leverans till användaren bör vara nära kopplad till rätten att ta emot sådana tjänster enligt villkoren i nationell lagstiftning.

Skadeståndsansvar (skäl 18)

I förordningen bör det föreskrivas skadeståndsansvar för den anmälande medlemsstaten, den aktör som utfärdar medlet för elektronisk identifiering och den aktör som har hand om autentiseringsförfarandet vid underlåtenhet att uppfylla relevanta skyldigheter enligt förordningen. Förordningen bör dock tillämpas i enlighet med nationella

bestämmelser om skadeståndsansvar. Den ska därför inte påverka tillämpningen av nationella bestämmelser om t.ex. definition av skada eller relevanta tillämpliga förfaranderegler exempelvis om bevisbörda.

Säkerhet och samarbete (skäl 19–20)

Säkerheten i system för elektronisk identifiering är enligt skälen avgörande för ett tillförlitligt gränsöverskridande ömsesidigt erkännande av medel för elektronisk identifiering. Mot denna bakgrund bör medlemsstaterna samarbeta med avseende på säkerheten och interoperabiliteten i systemen för elektronisk identifiering på unionsnivå.

Medlemsstaternas samarbete bör underlätta den tekniska interoperabiliteten för de anmälda systemen för elektronisk identifiering i syfte att främja en hög nivå av förtroende och en säkerhetsnivå som är anpassad till risknivån. Ett utbyte av information och bästa praxis mellan medlemsstaterna med sikte på ömsesidigt erkännande bör bidra till detta samarbete.

Betrodda tjänster (skäl 21–67)

Liksom när det gäller artiklarna handlar en stor del av skälen till förordningen om betrodda tjänster. Någon allmän skyldighet att använda dem eller att installera en accesspunkt för alla befintliga betrodda tjänster bör enligt skälen inte skapas. I synnerhet bör förordningen inte gälla tillhandahållande av tjänster som endast används inom slutna system mellan en avgränsad uppsättning deltagare, och som inte påverkar tredje man. Endast betrodda tjänster som tillhandahålls för allmänheten och som påverkar tredje man behöver uppfylla förordningens krav.

På grund av den snabba tekniska utvecklingen bör förordningen omfatta en strategi som är öppen för innovation. Förordningen bör även vara teknikneutral.

I övrigt behandlar skälen bl.a. tillsynsorgan, skadeståndsansvar och säkerhetsfrågor när det gäller betrodda tjänster.

16.2 Allmänna bestämmelser

Förordningens första kapitel behandlar syfte, tillämpningsområde och definitioner. I artikel 1 anges att i syfte att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster fastställs i förordningen

a) de villkor på vilka medlemsstaterna erkänner medel för elektronisk identifiering av fysiska och juridiska personer som omfattas av ett anmäl system för elektronisk identifiering hos en annan medlemsstat,

b) regler för betrodda tjänster, i synnerhet elektroniska transaktioner, och

c) en rättslig ram för elektroniska underskrifter, elektroniska stämplar, elektronisk tidsstämpling, elektroniska dokument, elektroniska tjänster för rekommenderade leveranser och certifikattjänster för autentisering av webbplatser.

I artikel 2 följer en beskrivning av förordningens tillämpningsområde och artikel 3 innehåller definitioner av 41 centrala begrepp som används i förordningstexten och i genomförandeakterna. Artikel 4 beskriver inremarknadsprincipen som bl.a. innebär att produkter och betrodda tjänster som överensstämmer med förordningen ska omfattas av fri rörlighet på den inre marknaden. Av artikel 5 följer att personuppgifter ska behandlas i enlighet med dataskyddsdirektivet.[3] Dessutom ska användningen av pseudonymer vid elektroniska transaktioner inte förbjudas.

16.3 Elektronisk identifiering

Förordningens andra kapitel behandlar elektronisk identifiering och inleds med artikel 6 om ömsesidigt erkännande. Enligt första punkten har offentliga organ (myndigheter) skyldighet att erkänna andra

[3] Direktiv 95/46/EG. Dataskyddsdirektivet kommer den 25 maj 2018 ersättas av Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

medlemsstaters elektroniska identitetshandlingar för gränsöverskridande autentisering i e-tjänster som kräver elektronisk identifiering och autentisering för nationell åtkomst, förutsatt att

a) den elektroniska identitetshandlingen är utfärdad inom ramen för ett system för elektronisk identifiering som ingår i kommissionens förteckning enligt artikel 9,

b) tillitsnivån för den elektroniska identitetshandlingen motsvarar en tillitsnivå som är lika hög eller högre än den tillitsnivå som den offentliga myndigheten i fråga kräver för åtkomst till den aktuella e-tjänsten, förutsatt att tillitsnivån för den elektroniska identitetshandlingen motsvarar tillitsnivån väsentlig eller hög,

c) den offentliga myndigheten i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.

Det innebär alltså en skyldighet för offentlig sektor att erkänna andra anmälda elektroniska identitetshandlingar för gränsöverskridande autentisering om tillitsnivån på den utländska notifierade elektroniska identitetshandlingen är minst nivå väsentlig och minst samma eller högre än vad som krävs nationellt, och det nationellt krävs minst tillitsnivå väsentlig.[4]

Enligt andra punkten får en offentlig myndighet erkänna en elektronisk identitetshandling som ingår i kommissionens förteckning och som motsvarar tillitsnivå låg. Det är alltså valfritt för den offentliga myndigheten.

Artikel 7 beskriver vad som krävs för att ett system för elektronisk identifiering ska kunna anmälas enligt artikel 9.1. Bland annat följande villkor ska vara uppfyllda:

a) Den elektroniska identitetshandlingen ska vara utfärdad

   i) av den anmälande medlemsstaten,

   ii) på uppdrag av den anmälande medlemsstaten, eller

   iii) oberoende av den anmälande medlemsstaten och erkännas av den medlemsstaten.

[4] Tillitsnivå väsentlig har bedömts motsvara svensk tillitsnivå 3, se avsnitt 12.7 om svenska tillitsnivåer.

Anmälan av privata utfärdare av elektroniska identitetshandlingar är alltså tillåtet om den elektroniska identitetshandlingen är godkänd i den anmälande medlemsstaten.

b) Den elektroniska identitetshandlingen ska kunna användas för att få åtkomst till åtminstone en tjänst som tillhandahålls av en offentlig myndighet och som kräver elektronisk identifiering i den anmälande medlemsstaten.

c) Den elektroniska identitetshandlingen ska uppfylla kraven för åtminstone en av de tillitsnivåer som anges i den genomförandeakt som avses i artikel 8.3.

Därefter regleras fördelning av ansvar mellan anmälande medlemsstat och den aktör som utfärdar elektroniska identitetshandlingar när det gäller personidentifieringsuppgifter och tilldelning av elektroniska identitetshandlingar. Den anmälande medlemsstaten ska se till att en autentiseringstjänst erbjuds samtliga förlitande aktörer. Tjänsten får förenas med särskilda villkor för den privata sektorn och ska vara kostnadsfri för förlitande aktörer i den offentliga sektorn.

I artikel 8 beskrivs systemet med tillitsnivåer för elektroniska identitetshandlingar. Tillitsnivåerna låg, väsentlig eller hög ska specificeras för anmälda elektroniska identitetshandlingar. Vad varje tillitsnivå innebär förtydligas i en genomförandeförordning.[5]

Artikel 9 handlar om hur elektroniska identitetshandlingar anmäls till kommissionen för att kunna inkluderas i förteckningen av elektroniska identitetshandlingar som ska erkännas i medlemsstaternas offentliga e-tjänster. Anmälan ska bland annat innehålla en beskrivning av den elektroniska identitetshandlingen inbegripet dess tillitsnivåer och av utfärdaren eller utfärdarna av den elektroniska identitetshandlingen. Anmälan ska även innehålla uppgift om det tillämpliga systemet för tillsyn och information om systemet för skadeståndsansvar när det gäller både utfärdare och den aktör som handhar autentiseringsförfarande. Dessutom ska den eller de offentliga myndigheter som ansvarar för den elektroniska identitetshandlingen anges samt

[5] Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

information om den eller de enheter som hanterar registreringen av de unika personuppgifterna. I övrigt krävs också bl.a. uppgift om system för tillfälligt upphävande eller återkallelse av den anmälda elektroniska identitetshandlingen.

En medlemsstat får själv lämna in begäran till kommissionen om att ta bort en elektronisk identitetshandling från förteckningen. Fler definitioner av hur anmälan och avanmälan ska gå till finns i ett genomförandebeslut.[6]

Artikel 10 behandlar säkerhetsincidenter och vilka åtgärder som ska vidtas om en anmäld elektronisk identitetshandling utsätts för intrång eller delvis äventyras på ett sätt som påverkar tillförlitligheten i systemets gränsöverskridande autentisering. Den anmälande medlemsstaten ska då utan dröjsmål tillfälligt upphäva eller återkalla denna gränsöverskridande autentisering eller de berörda utsatta delarna och informera andra medlemsstater och kommissionen. När incidenten har åtgärdats kan den gränsöverskridande autentiseringen återinföras och de andra medlemsstaterna ska informeras om det. Om problemet inte har åtgärdats efter tre månader ska den elektroniska identitetshandlingen dras tillbaka.

I artikel 11 berörs frågor om skadeståndsansvar. I princip bär varje aktör skadeståndsansvar för det man ansvarar för. Den anmälande medlemsstaten har skadeståndsansvar för skada som åsamkats genom dess underlåtenhet att uppfylla sina skyldigheter enligt artikel 7. Den aktör som utfärdat den elektroniska identitetshandlingen har skadeståndsansvar för skada som åsamkats genom underlåtenhet att uppfylla sina skyldigheter enligt artikel 7. Den aktör som handhar autentiseringsförfarandet har skadeståndsansvar för skada som åsamkats genom underlåtenhet att säkerställa korrekt handhavande av autentisering enligt artikel 7.

Ovanstående regler ska enligt artikel 11.4 tillämpas i enlighet med nationella regler om skadeståndsansvar. Det är dock inte specificerat vilka nationella regler som avses. Det kan vara reglerna i den medlemsstat som ansvarar för den elektroniska identitetshandlingen eller i den eller de medlemsstater där incident har uppstått.

[6] Kommissionens genomförandebeslut (EU) 2015/1984 av den 3 november 2015 om förutsättningar, format och förfaranden för anmälan enligt artikel 9.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Artikel 12 behandlar samarbete och interoperabilitet. Anmälda elektroniska identitetshandlingar ska följa ett interoperabilitetsramverk som ska uppfylla vissa kriterier. Det ska vara teknikneutralt, följa europeiska och internationella standarder och främja integritetsskydd samt säkerställa persondataskydd.

Vidare anges i artikel 12 att medlemsstaterna ska samarbeta när det gäller säkerhet, tillitsnivåer och interoperabilitet. De ska utbyta erfarenheter inom områden som berör sakkunnighetsbedömningar, minimikrav på teknik för interoperabilitet och minimikrav på attribut.

Vidare definitioner när det gäller interoperabilitet och samarbete finns i en genomförandeförordning.[7]

Genomförandeförordningen innehåller regler om bland annat tekniska minimikrav rörande tillitsnivåer och kartläggning av nationella tillitsnivåer för anmälda medel för elektronisk identifiering som utfärdats inom ramen för anmälda system för elektronisk identifiering, tekniska minimikrav på interoperabilitet, minimuppsättningen av personidentifieringsuppgifter som är unika för en fysisk eller juridisk person, gemensamma standarder för operativ säkerhet och bestämmelser för tvistlösning.

16.4 Betrodda tjänster

Förordningens kapitel III om betrodda tjänster omfattar 32 artiklar indelade i åtta avsnitt. Nedan följer en översiktlig beskrivning av reglernas innebörd.

16.4.1 Allmänna bestämmelser

Artikel 13 behandlar skadeståndsansvar och bevisbörda när det gäller betrodda tjänster. Även här ansvarar varje aktör för åsamkad skada.

Kvalificerade tillhandahållare av betrodda tjänster har bevisbörda för att visa att skadan uppstått utan avsikt eller oaktsamhet hos den kvalificerade tillhandahållaren. Däremot är det den som gör gällande

[7] Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

skada som har bevisbördan för avsikt eller oaktsamhet hos en icke-kvalificerad tillhandahållare av betrodda tjänster.

Reglerna ska tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar men inte heller när det gäller betrodda tjänster specificerar förordningen vilken medlemsstats nationella bestämmelser som ska gälla.

De allmänna bestämmelserna innehåller även artiklar som behandlar vissa internationella aspekter, tillgänglighet för personer med funktionshinder och sanktioner.

16.4.2 Tillsyn

I artikel 17 finns regler om tillsynsorgan. Medlemsstaterna ska utse ett tillsynsorgan. Tillsynsorganet ska utöva tillsyn över kvalificerade tillhandahållare av betrodda tjänster och även vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster om tillsynsorganet tar del av påståenden att dessa inte uppfyller förordningens krav. Artikelns lydelse specificerar vilka uppgifter som ingår i tillsynen. I Sverige är Post- och telestyrelsen (PTS) utsedd till tillsynsorgan.

Tillsynsorganen ska enligt artikel 18 samarbeta och ge varandra bistånd men har också möjlighet att under vissa förutsättningar vägra sådant bistånd.

Artikel 19 innehåller regler om säkerhetskrav på tillhandahållare av betrodda tjänster. Enligt första punkten ska kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster vidta lämpliga tekniska och organisatoriska åtgärder för att hantera säkerhetsriskerna hos de betrodda tjänster som de tillhandahåller. Åtgärderna ska säkerställa att säkerhetsnivån står i proportion till graden av risk.

Enligt 19.2 ska kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster, utan otillbörligt dröjsmål och under alla omständigheter inom 24 timmar efter upptäckt, underrätta tillsynsorganet och i förekommande fall andra relevanta organ, såsom det behöriga nationella organet för informationssäkerhet eller dataskyddsmyndigheten, om alla säkerhetsincidenter och integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller på de personuppgifter som ingår i denna.

När det är troligt att säkerhetsincidenten eller integritetsförlusten kommer att ha negativ inverkan på en fysisk eller juridisk person till vilken den betrodda tjänsten har tillhandahållits, ska tillhandahållaren av betrodda tjänster utan onödigt dröjsmål även underrätta den fysiska eller juridiska personen om säkerhetsincidenten eller integritetsförlusten.

Tillsynsorganet har vid sådana säkerhetsincidenter eller integritetsförluster i uppgift att, om det är lämpligt, informera övriga medlemsstater, allmänheten samt Europeiska byrån för nät- och informationssäkerhet (Enisa).

16.4.3 Kvalificerade betrodda tjänster

Kraven på kvalificerade betrodda tjänster är högre än på icke kvalificerade betrodda tjänster. Därför är det i högre grad specificerat vad som gäller för kvalificerade betrodda tjänster. I förordningens artikel 20 regleras hur tillsyn av kvalificerade betrodda tjänster ska gå till. Minst en gång vartannat år och på egen bekostnad ska kvalificerade tillhandahållare av betrodda tjänster granskas. Tillsynsorganet får dessutom när som helst utföra granskning. Om den kvalificerade tillhandahållaren underlåter att åtgärda något som tillsynsorganet har påpekat kan tillsynsorganet komma att återkalla tjänstens status som kvalificerad.

Artikel 21 innehåller krav för att sätta igång en kvalificerad betrodd tjänst. Detta ska anmälas till tillsynsorganet som, om tillhandahållaren uppfyller förordningens krav, ska bevilja status som kvalificerad och föra upp tillhandahållaren på förteckningen över kvalificerade tillhandahållare.

Varje medlemsstat ska enligt artikel 22 upprätta, underhålla och offentliggöra förteckningar med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som den ansvarar för, tillsammans med uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller. Detta görs i Sverige på PTS webbplats.

Kvalificerade tillhandahållare av betrodda tjänster får enligt artikel 23 använda sig av EU-förtroendemärket för att på ett enkelt, igenkännligt och tydligt sätt ange de kvalificerade betrodda tjänster som de tillhandahåller.

Figur 16.1 EU-förtroendemärket

Kommissionens genomförandeförordning (EU) 2015/806 av den 22 maj 2015 om fastställande av specifikationer för utformningen av EU-förtroendemärket för kvalificerade betrodda tjänster, bilaga I och II.

I artikel 24 behandlas kraven på kvalificerade tillhandahållare av betrodda tjänster. Tillhandahållaren ska, när den utfärdar ett kvalificerat certifikat för en betrodd tjänst, på lämpligt sätt och i enlighet med nationell rätt kontrollera identiteten och i förekommande fall eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet utfärdas. Detta kan göras genom fysisk närvaro, elektronisk identitetshandling med tillitsnivå väsentlig eller hög, certifikat för kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel, eller slutligen med hjälp av andra identifieringsmetoder som erkänns på nationell nivå och som erbjuder garantier som är likvärdiga med fysisk närvaro. Likvärdiga garantier ska då bekräftas av ett organ för bedömning av överensstämmelse.

Övriga krav inkluderar bland annat informationsplikt, kunskap hos personal och underleverantörer, ekonomiska medel eller försäkring för att täcka risk för ansvar vid skador, säkerhet, tillförlitlig lagring av uppgifter, plan för verksamhetens upphörande samt att säkerställa laglig behandling av personuppgifter.

16.4.4 Elektroniska underskrifter

Rättslig verkan av elektroniska underskrifter beskrivs i artikel 25. En elektronisk underskrift får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att underskriften har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska underskrifter.

En kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift och erkännas som en kvalificerad elektronisk underskrift i samtliga medlemsstater.

I artikel 26 återfinns de krav som ställs på en avancerad elektronisk underskrift. Den ska vara knuten till undertecknaren, undertecknaren ska kunna identifieras genom den, den ska vara skapad så att undertecknaren med hög grad av tillförlitlighet kan använda den uteslutande under sin egen kontroll och slutligen ska efterföljande ändringar av de undertecknade uppgifterna kunna upptäckas.

Elektroniska underskrifter i offentliga tjänster är enligt artikel 27 föremål för ömsesidigt erkännande på motsvarande nivå. Medlemsstaterna ska för gränsöverskridande användning av nättjänster som erbjuds av ett offentligt organ inte kräva en elektronisk underskrift med en högre säkerhetsnivå än den som gäller för kvalificerade elektroniska underskrifter.

Vissa regler när det gäller kvalificerade certifikat för elektroniska underskrifter finns i artikel 28 men kraven de ska uppfylla finns i bilaga I till förordningen. Där specificeras vad certifikaten ska innehålla. En liknande konstruktion har valts när det gäller anordningar för skapande av kvalificerade elektroniska underskrifter i artikel 29–30 och bilaga II.

Kommissionen ska enligt artikel 31 offentliggöra en förteckning över certifierade anordningar för skapande av kvalificerade elektroniska underskrifter.

Giltigheten för en kvalificerad elektronisk underskrift kan bekräftas genom validering. Artikel 32 innehåller krav för sådan validering och artikel 33 reglerar kvalificerade valideringstjänster för kvalificerade elektroniska underskrifter.

I artikel 34 finns en regel om vem som får tillhandahålla en kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter.

16.4.5 Elektroniska stämplar

Elektroniska stämplars rättsliga verkan beskrivs i artikel 35. Den får inte förvägras rättslig verkan enbart på grund av att den har elektronisk form. En kvalificerad elektronisk stämpel ska omfattas av en presumtion om integritet hos de uppgifter som den är kopplad till och om att uppgifterna har korrekt ursprung. En kvalificerad elektronisk

stämpel som är baserad på ett kvalificerat certifikat som har utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk stämpel i alla andra medlemsstater.

En elektronisk stämpel ska uppfylla krav enligt artikel 36. Den ska vara knuten uteslutande till skaparen av stämpeln. Skaparen av stämpeln ska kunna identifieras. Stämpeln ska vara skapad så att den kan användas med hög grad av tillförlitlighet. Den ska vara kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Elektroniska stämplar i offentliga tjänster är enligt artikel 37 föremål för ömsesidigt erkännande på motsvarande nivå. Medlemsstaterna ska för gränsöverskridande användning av nättjänster som erbjuds av ett offentligt organ inte kräva en elektronisk stämpel med en högre säkerhetsnivå än den som gäller för den kvalificerade elektroniska stämpeln.

Vissa regler när det gäller kvalificerade certifikat för elektroniska stämplar finns i artikel 38 men kraven de ska uppfylla finns i bilaga III till förordningen. Där specificeras vad certifikaten ska innehålla.

När det gäller kvalificerade anordningar för skapande av elektroniska stämplar samt validering och bevarande av kvalificerade elektroniska stämplar hänvisas i artikel 39–40 till motsvarande bestämmelser för kvalificerade elektroniska underskrifter i artikel 29–34.

16.4.6 Elektroniska tidsstämplingar

Elektroniska tidsstämplingars rättsliga verkan beskrivs i artikel 41. Även när det gäller elektroniska tidstämplingar får de inte förvägras rättslig verkan enbart på grund av att den har elektronisk form. En kvalificerad elektronisk tidsstämpling ska omfattas av en presumtion av korrekthet och erkännas som en kvalificerad elektronisk tidsstämpling i alla medlemsstater.

Artikel 42 innehåller förordningens krav på en kvalificerad elektronisk tidsstämpling. Den ska binda datumet och tiden till uppgifter så att möjligheten att uppgifterna ändras utan att det går att upptäcka rimligtvis kan uteslutas. Den ska vara grundad på en korrekt tidskälla som är kopplad till samordnad universaltid. Den ska vara undertecknad med hjälp av en avancerad elektronisk underskrift eller för-

seglad med en avancerad elektronisk stämpel från den kvalificerade tillhandahållaren av betrodda tjänster eller genom en likvärdig metod.

16.4.7 Elektroniska tjänster för rekommenderade leveranser

Rättslig verkan av elektroniska tjänster för rekommenderade leveranser beskrivs i artikel 43. Uppgifter som sänds och tas emot genom en elektronisk tjänst för rekommenderade leveranser får inte förvägras rättslig verkan enbart på grund av att de har elektronisk form. Uppgifter som sänds och tas emot genom en kvalificerad elektronisk tjänst för rekommenderade leveranser ska omfattas av en presumtion om uppgifternas integritet, om uppgifternas avsändande av den identifierade avsändaren, uppgifternas mottagande av den identifierade adressaten samt om riktigheten i det datum och den tidpunkt för avsändande och mottagande som anges i den kvalificerade elektroniska tjänsten för rekommenderade leveranser.

Artikel 44 innehåller förordningens krav på kvalificerade elektroniska tjänster för rekommenderade leveranser. Kraven innebär bland annat följande. De kvalificerade elektroniska tjänsterna för rekommenderade leveranser ska tillhandahållas av en eller flera kvalificerade tillhandahållare av betrodda tjänster. De ska med hög grad av tillförlitlighet säkerställa avsändarens identitet. De ska säkerställa adressatens identitet innan uppgifterna levereras. Kvalificerade betrodda tjänster ska användas för att säkerställa avsändande, mottagande och tidpunkt på ett sätt som utesluter möjligheten att uppgifterna ändras utan att det går att upptäcka.

16.4.8 Autentisering av webbplatser

Krav på kvalificerade certifikat för autentisering av webbplatser finns enligt artikel 45 i bilaga IV. Där specificeras vad certifikaten ska innehålla.

16.5 Elektroniska dokument

Ett elektroniskt dokument får enligt artikel 46 inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form.

16.6 Genomförandeakter

Utöver förordningen finns det genomförandeakter som ger kommissionen befogenhet att på ett flexibelt och snabbt sätt kunna komplettera vissa detaljerade aspekter av förordningen. Genomförandebefogenheter bör även tilldelas kommissionen för att säkerställa enhetliga villkor för genomförandet av förordningen. Detta anges i skäl 70–71 till förordningen.

Enligt flera artiklar ska kommissionen inom viss tid anta genomförandeakter för att förtydliga och specificera vissa uppgifter men på många andra ställen i förordningen ges kommissionen möjlighet att anta genomförandeakter.

Nedan följer en förteckning av de genomförandeakter som i skrivande stund har antagits.

Kommissionens genomförandebeslut (EU) 2015/296 av den 24 februari 2015 om inrättande av förfaranden för samarbete mellan medlemsstaterna om elektronisk identifiering i enlighet med artikel 12.7 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

Genomförandebeslutet handlar om förfaranden för att underlätta samarbetet mellan medlemsstaterna, vilket är nödvändigt för att säkerställa interoperabiliteten och säkerheten i system för elektronisk identifiering som medlemsstaterna avser att anmäla eller har anmält till kommissionen. Förfarandena avser särskilt utbyte av information, erfarenheter och god praxis om system för elektronisk identifiering samt undersökning av den relevanta utvecklingen inom sektorn för elektronisk identifiering, sakkunnighetsbedömning av system för elektronisk identifiering och samarbete genom ett särskilt samarbetsnätverk.

Kommissionens genomförandeförordning (EU) 2015/806 av den 22 maj 2015 om fastställande av specifikationer för utformningen av EU-förtroendemärket för kvalificerade betrodda tjänster

Genomförandeförordningen behandlar EU-förtroendemärket för kvalificerade betrodda tjänster och bilagan till förordningen visar hur det ser ut.

Kommissionens genomförandebeslut (EU) 2015/1506 av den 8 september 2015 om fastställande av specifikationer rörande format för avancerade elektroniska underskrifter och avancerade elektroniska stämplar i enlighet med artiklarna 27.5 och 37.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

Genomförandebeslutet innehåller tekniska specifikationer för att underlätta ömsesidigt erkännande mellan medlemsstaterna när det gäller avancerade elektroniska underskrifter och avancerade elektroniska stämplar. I beslutets bilaga finns en förteckning över de tekniska specifikationerna.

Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

Genomförandeförordningen innehåller regler om bland annat tekniska minimikrav rörande tillitsnivåer och kartläggning av nationella tillitsnivåer för anmälda medel för elektronisk identifiering som utfärdats inom ramen för anmälda system för elektronisk identifiering, tekniska minimikrav på interoperabilitet, minimuppsättningen av personidentifieringsuppgifter som är unika för en fysisk eller juridisk person, gemensamma standarder för operativ säkerhet och bestämmelser för tvistlösning.

I genomförandeförordningen finns krav, regler och definitioner för noder.

I bilagan till genomförandeförordningen listas minimiuppsättningen av personidentifieringsuppgifter som är unika för en fysisk eller en juridisk person. En minimiuppsättning av uppgifter för en fysisk person ska innehålla följande obligatoriska attribut: nuvarande efternamn, nuvarande förnamn, födelsedatum samt en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständig i tid. En minimiuppsättning för en fysisk person kan dessutom innehålla ett eller flera av följande ytterligare attribut: förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön.

En minimiuppsättning av uppgifter för en juridisk person ska innehålla följande obligatoriska attribut: nuvarande juridiska namn och en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständig i tid. En minimiuppsättning av uppgifter för en juridisk person kan dessutom innehålla ett eller flera ytterligare attribut, t.ex. nuvarande adress, momsregistreringsnummer, skatteregistreringsnummer m.m.

Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

Genomförandeförordningen beskriver specifikationer och övrigt för tillitsnivåerna låg, väsentlig och hög för medel för elektronisk identifiering utfärdade inom ett anmält system för elektronisk identifiering.

I bilagan till förordningen finns specificerat vad som krävs för att uppnå respektive tillitsnivå vid olika skeden i processerna för inskrivning, hantering av medel för elektronisk identifiering, autentisering, hantering och organisation.

Kommissionens genomförandebeslut (EU) 2015/1505 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och format rörande förteckningar över betrodda tjänsteleverantörer i enlighet med artikel 22.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

Enligt genomförandebeslutet ska medlemsstaterna upprätta, offentliggöra och underhålla förteckningar över betrodda tjänsteleverantörer med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som står under medlemsstaternas tillsyn, liksom uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller. Dessa förteckningar ska uppfylla de tekniska specifikationer som anges i bilaga I till genomförandebeslutet.

Kommissionens genomförandebeslut (EU) 2015/1984 av den 3 november 2015 om förutsättningar, format och förfaranden för anmälan enligt artikel 9.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

I genomförandebeslutet finns bestämmelser om hur medlemsstaterna ska gå till väga för att anmäla ett system för elektroniska identitetshandlingar till kommissionen. Anmälan ska göras på engelska och det ska ske elektroniskt genom det formulär som finns i bilagan till genomförandebeslutet.

Kommissionens genomförandebeslut (EU) 2016/650 av den 25 april 2016 om fastställande av standarder för säkerhetsbedömning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar enligt artiklarna 30.3 och 39.2 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

I bilagan till genomförandebeslutet förtecknas de standarder för säkerhetsbedömning av informationsteknikprodukter som gäller för certifiering av kvalificerade anordningar för skapande av elektroniska underskrifter eller kvalificerade anordningar för skapande av elektroniska stämplar i de fall de uppgifter som genereras för skapande av elektroniska underskrifter eller av elektroniska stämplar bevaras i en helt, men inte nödvändigtvis uteslutande, användarskött miljö.

16.7 Fonden för ett sammanlänkat Europa – CEF

Förordningen 1316/2013[8] reglerar Fonden för ett sammanlänkat Europa (Connecting Europe Facility – CEF). Enligt artikel 1 ska fonden fastställa villkor, metoder och förfaranden för tillhandahållande av finansiellt stöd från unionen till transeuropeiska nät i syfte att främja projekt av gemensamt intresse inom sektorerna för transport-, telekommunikations- och energi infrastruktur och utnyttja potentiella synergieffekter mellan dessa sektorer. En del av fondens program är CEF Digital som arbetar för att möjliggöra en digital inre marknad. CEF Digital beskriver fem centrala byggstenar som tillsammans utgör basen för att uppnå en sådan marknad:[9]

- eDelivery som är en digital meddelandetjänst,
- eID som är elektroniska identitetshandlingar,
- eInvoicing som är elektronisk fakturering,

[8] Europaparlamentets och Rådets förordning (EU) nr 1316/2013 av den 11 december 2013 om inrättande av Fonden för ett sammanlänkat Europa, om ändring av förordning (EU) nr 913/2010 och om upphävande av förordningarna (EG) nr 680/2007 och (EG) nr 67/2010.
[9] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home, 2017-11-07.

- eSignature som är elektroniska underskrifter,
- eTranslation som är digital översättning.

På webbplatsen för byggstenen eID finns information om hur frågor om gränsöverskridande identifiering och den digitala marknaden drivs inom EU. Webbplatsen ger ett europeiskt perspektiv på hur systemet är tänkt att fungera.[10]

På webbplatsen förklaras vilka aktörer som är inblandade i olika skeden, fördelarna eIDAS-förordningen kan medföra, medlemsstaternas arbete och kontaktpunkter, hur man kan ansöka om finansiering och exempel på användningsområden. Vidare finns länkar till olika samarbetsnätverk, instruktioner till tillhandahållare av e-tjänster om hur de kan förbereda sig och till utvecklare av noder samt relevant lagstiftning.

[10] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID, 2017-11-07.

17 Europeiska elektroniska identitetshandlingar i svenska e-tjänster

17.1 Beskrivning av processen

När en användare identifierar sig i en e-tjänst med hjälp av en elektronisk identitetshandling startar en process för att avgöra om användaren ska ges tillträde till tjänsten eller inte. För att släppa in användaren i e-tjänsten kan tillhandahållaren av e-tjänsten kräva bekräftelse på att individen som identifierar sig verkligen är den som den utger sig för att vara. Elektroniska identitetshandlingar kan ge sådan bekräftelse genom ett identitetsintyg. Identitetsintyget innehåller vissa attribut (uppgifter om användaren), t.ex. personnummer. Detta har även beskrivits av utredningen i tidigare kapitel.

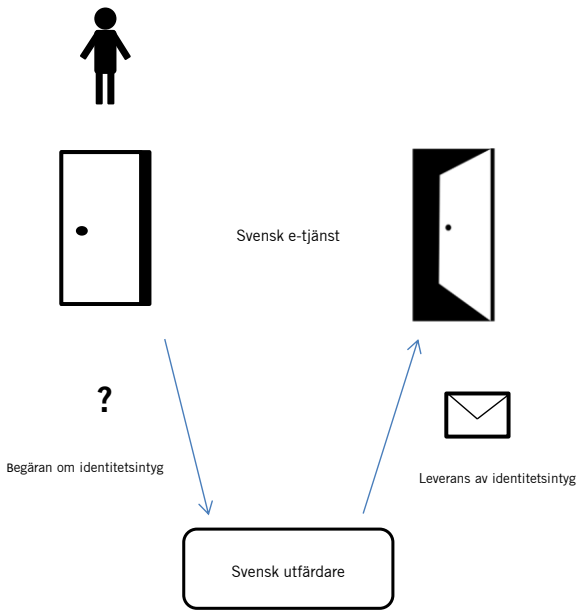
Beskrivningen av processen nedan ger en förenklad bild av vad som händer när en användare identifierar sig i en e-tjänst. Avsikten är att visa skillnaderna mellan att en användare identifierar sig med en svensk eller en utländsk elektronisk identitetshandling.

17.1.1 Identifiering med svensk elektronisk identitetshandling

När en användare identifierar sig i en svensk e-tjänst med en svensk elektronisk identitetshandling skickas en begäran om identitetsintyg från tillhandahållaren av e-tjänsten (förlitande aktör) till utfärdaren av den elektroniska identitetshandlingen. Utfärdaren bekräftar identiteten genom att ansvara för att ett identitetsintyg levereras till den förlitande aktören och användaren kan därefter släppas in i e-tjänsten. Ofta köper utfärdaren av den elektroniska identitetshandlingen identitetsintyg från en underleverantör. I praktiken levereras alltså

identitetsintyget då av någon annan än utfärdaren av den elektroniska identitetshandlingen.

Figur 17.1 Individ identifierar sig med svensk elektronisk identitetshandling



17.1.2 Identifiering med utländsk elektronisk identitetshandling

När en användare identifierar sig i en svensk e-tjänst med en utländsk elektronisk identitetshandling kommer processen att se lite annorlunda ut. Användaren får ange att han eller hon vill identifiera sig med en utländsk elektronisk identitetshandling och i vilket land den är utfärdad. Begäran om identitetsintyg skickas via den svenska noden som dirigerar begäran vidare till det valda landets nod. Det valda landets nod skickar begäran om identitetsintyg till den utfärdare som har utfärdat den elektroniska identitetshandlingen i det aktuella landet. Identitetsintyget ska innehålla användarens nuvarande förnamn, nuvarande efternamn, födelsedatum och landets unika iden-

titetsbeteckning. Det kan också innehålla några ytterligare attribut.[1] Identitetsintyget levereras tillbaka från utfärdaren via den utländska noden till den svenska noden. Den svenska noden kan antingen leverera identitetsintyget direkt till tillhandahållaren av e-tjänsten eller göra en slagning mot ett framtida kopplingsregister och därefter eventuellt leverera ett berikat identitetsintyg till tillhandahållaren av e-tjänsten. Identitetsintyget är då berikat med användarens svenska person- eller samordningsnummer.

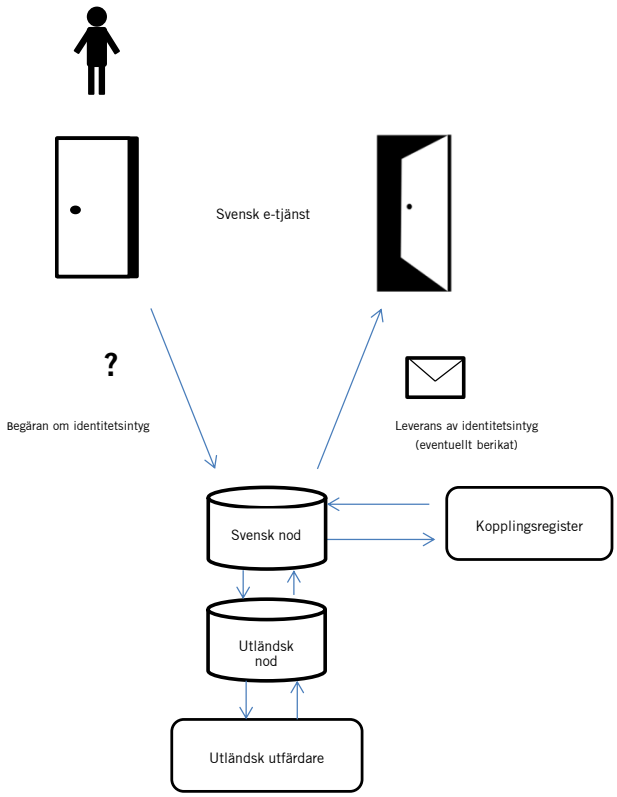
För att få tillgång till svenska offentliga myndigheters e-tjänster krävs i många fall att användaren har ett svenskt person- eller samordningsnummer. De användare som har behov av att använda svenska offentliga myndigheters e-tjänster har troligtvis redan någon relation till Sverige. Därför har de kanske även ett svenskt person- eller samordningsnummer. Det är av intresse för de förlitande aktörerna att veta att de har att göra med en person som har en viss identitet i Sverige. För att uppnå högsta möjliga nivå av säkerhet i kopplingarna mellan utländska elektroniska identitetshandlingar och svenska person- och samordningsnummer och för att de offentliga myndigheternas tillämpning ska bli enhetlig har Skatteverket föreslagit att det ska finnas ett centralt kopplingsregister.[2]

Om någon försöker identifiera sig med en utländsk elektronisk identitetshandling som inte är godkänd enligt eIDAS-förordningen kommer den utländska nod som frågan om identitetsintyg levereras till inte att kunna besvara frågan eller bekräfta identiteten. De offentliga myndigheterna som tillhandahåller e-tjänster behöver därmed inte själva känna till eller kontrollera vilka utländska elektroniska identitetshandlingar som är godkända. Om de inte får tillbaka ett identitetsintyg som bekräftar identiteten på användaren ska användaren inte släppas in i e-tjänsten.

[1] Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

[2] Skatteverkets promemoria från den 24 oktober 2016, Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer, dnr 131 184020-16/113.

Figur 17.2 Individ identifierar sig med utländsk elektronisk identitetshandling



17.1.3 Skatteverkets rapport, centralt kopplingsregister eller inte?

Konsekvenserna för de svenska offentliga myndigheterna av skyldigheten att erkänna utländska elektroniska identitetshandlingar i sina e-tjänster kan komma att variera beroende på om det skapas ett centralt kopplingsregister eller inte.

Enligt Skatteverkets förslag om kopplingsregister ska den svenska noden förmedla till den offentliga myndigheten om koppling finns eller inte. De offentliga myndigheterna måste kunna lita på att det är samma person bakom den utländska elektroniska identitetshandlingen som bakom det svenska person- eller samordningsnumret. Annars blir kopplingsregistret inte användbart. För att få en koppling registrerad

ska det därför krävas samma grad av säkerhet som vid utfärdandet av en fysisk identitetshandling. Det innebär enligt Skatteverket att koppling kan registreras först efter noggrann kontroll som kan genomföras på tre sätt.

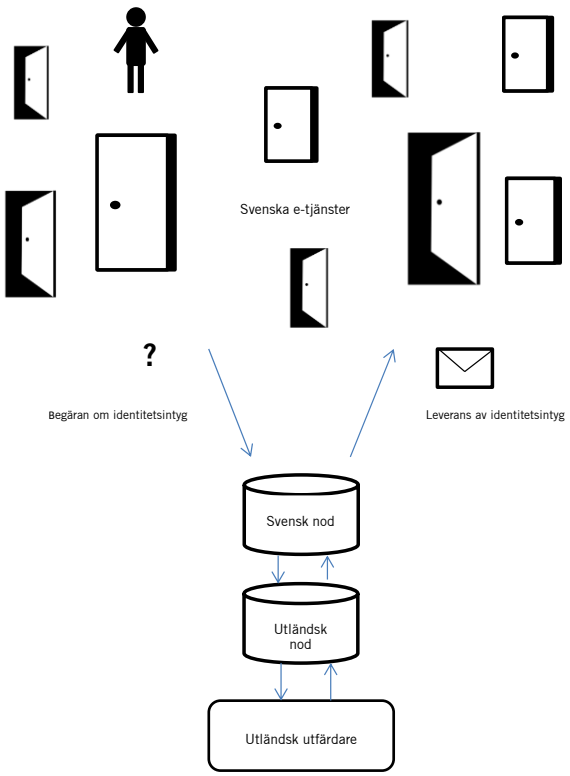
För att få till stånd en elektronisk lösning kan Sverige i bilaterala avtal komma överens med främst de andra nordiska länderna om att den elektroniska identitetshandlingen ska innehålla personnummer eller motsvarande som kan jämföras med redan registrerade uppgifter i folkbokföringsdatabasen. Ett alternativt sätt som också ger en elektronisk lösning är att användaren först identifierar sig med en redan registrerad elektronisk identitetshandling och därefter kopplar ytterligare en elektronisk identitetshandling till sitt personnummer eller styrkta samordningsnummer. För de användare som inte kan få en koppling registrerad elektroniskt finns slutligen alternativet att användaren inställer sig fysiskt för identifiering hos en registrerande offentlig myndighet.

Om det inte finns ett centralt kopplingsregister kommer varje offentlig myndighet att själv behöva ha en beredskap för att göra motsvarande kopplingar. Det varierar mellan de offentliga myndigheterna hur stora säkerhetskrav de har, hur mycket de använder sig av e-tjänster och hur stora flöden av identifiering med utländska elektroniska identitetshandlingar som beräknas strömma in. Enligt Skatteverkets analys kommer det dock att finnas stora behov av ett kopplingsregister hos vissa större offentliga myndigheter.

En stor risk med att inte tillhandahålla ett centralt kopplingsregister är att de offentliga myndigheterna kan göra olika bedömningar av om koppling mellan en utländsk elektronisk identitetshandling och ett svenskt person- eller samordningsnummer ska göras. Användaren kan då släppas in i vissa e-tjänster men inte i andra trots att e-tjänsterna har samma nivå på säkerhetskrav och användaren identifierar sig med samma utländska elektroniska identitetshandling på alla ställen.

Det finns också risk för att varje offentlig myndighet då behöver en egen registerförfattning för att hålla ett eget register när flödet av identifieringar med utländska elektroniska identitetshandlingar ökar.

Figur 17.3 Vad händer om kopplingsregister saknas?



17.1.4 Personuppgiftsbehandling i processen

I all användning av elektroniska identitetshandlingar förekommer behandling av personuppgifter. I och med ikraftträdandet av dataskyddsförordningen[3] ställs nya krav på alla aktörer som utför behandling av personuppgifter. Offentliga myndigheter som har e-tjänster där man hanterar elektroniska identitetshandlingar behöver se över sin beredskap ur den här aspekten. Det gäller även andra aktörer som medverkar i processen vid identifiering med elektroniska identitetshand-

[3] Europaparlamentet och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

lingar, såsom utfärdare av elektroniska identitetshandlingar och utfärdare av identitetsintyg.

För att ta ställning till vilken aktör som ska ha personuppgiftsansvar behöver redas ut vilka parter som är aktuella, vilka personuppgifter som behandlas, och vem som kan uppfylla kraven som följer med personuppgiftsansvar.

Skatteverket har i sin rapport om kopplingsregister föreslagit att Skatteverket ska vara personuppgiftsansvarig för behandlingar av personuppgifter i kopplingsregistret. Skatteverket har också föreslagit att E-legitimationsnämnden[4] ska vara personuppgiftsansvarig för den personuppgiftsbehandling som utförs när noden kontrollerar om en användare förekommer i kopplingsregistret. Utredningen låter dessa förslag ligga som utgångspunkter i fördelningen av personuppgiftsansvar mellan aktörerna. I kommande avsnitt hanteras därför inte personuppgiftsansvar när det gäller kopplingsregistret.

17.2 Konsekvenser för de svenska offentliga myndigheterna av att erkänna europeiska elektroniska identitetshandlingar och underskrifter i sina e-tjänster

17.2.1 E-legitimationsnämndens enkäter om myndigheternas beredskap

E-legitimationsnämnden har under åren 2015, 2016 och 2017 gått ut med en enkät till alla statliga myndigheter, kommuner och landsting för att mäta behov av elektroniska identitetshandlingar och i viss mån även betrodda tjänster.[5] Syftet har också varit att skapa en tydligare bild av hur statliga myndigheter, kommuner och landsting ligger till i arbetet med att förbereda sig för eIDAS-förordningens krav, samla in deras frågeställningar och behov samt även sprida kunskap till dem som har svarat på enkäterna.

[4] Här förutsätter utredningen att det i praktiken blir den nya digitaliseringsmyndigheten som väntas ta över E-legitimationsnämndens verksamhet fr.o.m. den 1 september 2018 som får personuppgiftsansvar i detta led.

[5] www.elegnamnden.se/omoss/enkater, 2017-10-27, E-legitimationsnämndens enkätundersökning för 2017. Enkäten skickades ut till alla 500 registraturer och i juli 2017 hade 146 svar inkommit, varav hälften av svaren var från kommunal sektor och hälften från statliga myndigheter.

Av de svar som har kommit in 2017 drar E-legitimationsnämnden bl.a. följande slutsatser. Den offentliga sektorns transaktionsvolym för elektroniska identifiering och underskrifter går från 148 miljoner 2016 till 178 miljoner 2017. Hos 58 procent av de statliga myndigheterna, kommunerna och landstingen finns e-tjänster där man identifierar sig med hjälp av elektroniska identitetshandlingar men det är åtta myndigheter som står för 98 procent av transaktionerna.

I 40 procent av de offentliga myndigheterna finns e-tjänster där användaren skriver under med elektronisk underskrift men det är fem av de offentliga myndigheterna som står för 98 procent av transaktionerna. Av de berörda har 30 procent skaffat fristående underskrifttjänst. Endast 20 procent av de berörda känner till eIDAS-förordningens krav om erkännande av utländska elektroniska underskrifter.

Enkätsvaren visar också att det finns behov av kvalificerade elektroniska underskrifter, samt behov av elektroniska stämplar och tidsstämplingar.

De tio organisationer som har störst transaktionsvolymer när det gäller elektronisk identifiering och elektroniska underskrifter är Skatteverket, Försäkringskassan, 1177.se, Arbetsförmedlingen, Centrala studiestödsnämnden, Stockholms stad, Pensionsmyndigheten, Bolagsverket, Jönköpings kommun och Sundsvalls kommun.

De eIDAS-relaterade frågorna visar att ungefär tre fjärdedelar av de berörda svarande myndigheterna känner till eIDAS-förordningen och det är få som har påbörjat arbetet med att förbereda för att kunna erkänna utländska elektroniska identitetshandlingar och underskrifter i sina e-tjänster. Endast 40 procent av de berörda svarande offentliga myndigheterna planerar att hinna i tid med förberedelsearbetet till tredje kvartalet 2018.

Som exempel på möjliga framtida användningsområden för europeiska elektroniska identitetshandlingar anges:

- Ansökan om kontaktfamilj, familjehem, språkvän,
- Ansökan om stipendium,
- Beställa betyg,
- Ansökan om arbetstillstånd,
- Inrapportering till Finansinspektionen,
- Utländska jägare,

- Ansöka om elektronisk identitetshandling inom högskolesektorn,
- Tillstånd om att få ställa ut container och annat begagnande av offentlig plats,
- Ansöka om tillstånd för skolverksamhet,
- Intresseanmälningar av olika slag,
- Lämna synpunkter, göra felanmälan,
- Boka lokal.

De offentliga myndigheter som har svarat på frågor om framtida tänkbara transaktionsvolymer av utländska e-legitimeringar bedömer att dessa kommer att öka stort under de närmaste åren.

17.2.2 Vad säger de offentliga myndigheterna själva?

Utredningen har under utredningstiden träffat företrädare för offentliga myndigheter av olika slag och storlek för att få en uppfattning om vad de själva ser för konsekvenser av eIDAS-förordningens krav. Utredningen har även i oktober 2017 skickat ut en enkät till ett tjugotal offentliga myndigheter som har påbörjat sitt förberedelsearbete. Av svaren framkommer bl.a. följande.

Konsekvenserna av eIDAS-förordningen varierar beroende på de offentliga myndigheternas verksamhet, storlek och digitaliseringsgrad men också på hur de organiserar sin anpassning. Det finns flera exempel på kommuner som har gått samman, tio–tolv stycken, i geografisk närhet och med liknande storlek och förutsättningar i övrigt, och i gemensamma upphandlingar köpt elektronisk identifiering. Denna form av samarbete bedöms av de inblandade fungera mycket bra och underlättar både kostnads- och kompetensmässigt.

En direkt konsekvens för de tillfrågade offentliga myndigheterna är behovet av att anpassa sina berörda e-tjänster. Det kräver insatser av befintliga resurser som t.ex. kravanalytiker, experter och utvecklare samt inom informationssäkerhet och juridik.

Flera offentliga myndigheter efterfrågar besked om huruvida regeringen avser att gå vidare med utvecklingen av ett centralt kopplingsregister eller Skatteverkets förslag om kopplingsregister. Konsekven-

serna för dessa offentliga myndigheter varierar mycket beroende av om det kommer att finnas en gemensam lösning eller inte.

Konsekvenserna av eIDAS-förordningen medför ökade behov av nationell samordning mellan offentliga myndigheter gällande fler områden, t.ex. gemensam arkitektur, federativa modeller för åtkomst och behörighetsstyrning.

Även harmonisering av viss lagstiftning inom EU bedöms nödvändig, t.ex. dataskyddsförordningen[6] möjliggör en samsyn gällande personuppgiftshanteringen i alla medlemsländer. Det inbegriper frågor om lagring av personuppgifter för utländska användare som använder svenska e-tjänster och om utländska användare ska kunna titta på information som är lagrad i svenska register.

I flera avseenden är konsekvenserna svåra att överblicka eftersom det är oklart vilken hållning regeringen kommer att inta till vilken nivå av service svenska offentliga myndigheter ska hålla. Det gäller t.ex. språkliga anpassningar av e-tjänster och information till utländska användare som inte bedöms kunna släppas in i den offentliga myndighetens e-tjänster.

Konsekvenserna beskrivs också medföra möjligheter till förbättring. Offentliga myndigheter kan med hjälp av eIDAS-förordningen ytterligare öka och förenkla utvecklingen av interoperabla e-tjänster, både självbetjänande och helt automatiserade. Det ger även möjlighet att utveckla e-tjänster som är interoperabla internt inom Sverige och externt i och mot EU. Ur ett verksamhetsperspektiv medför eIDAS-förordningen möjligheter att både billigare och effektivare hantera användare som inte har någon form av svensk elektronisk identitetshandling. Indirekt ger det möjlighet att utveckla e-tjänster som för användaren blir mer självbetjänande och enklare eftersom de offentliga myndigheterna kan bygga användarcentrerade tjänsteportaler. Användaren kan hitta allt från olika leverantörer i en och samma e-tjänst. Detta bygger på att tjänsteleverantörerna har interoperabla funktioner. Digitalisering och automatisering bedöms även frigöra personella resurser hos de offentliga myndigheterna och personalens processspecifika kompetens kan koncentreras till andra delar i en verksamhetsprocess. En konsekvens av förordningen kan bli att de offentliga

[6] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

myndigheterna gemensamt levererar e-tjänster till användare där användaren står i centrum och inte de offentliga myndigheterna själva.

Möjlighet till fler e-tjänster kan höja säkerheten avseende vem som äger transaktionen i tjänster som i dag inte har möjlighet att hantera EU-medborgare som inte har svensk elektronisk identitetshandling. Det påpekas även att fler e-tjänster kan innebära en förhöjd risk för bedrägligt beteende gentemot olika offentliga myndigheter, såväl systematiskt som engångsföreteelser.

De offentliga myndigheterna identifierar särskilt en potential för gränsöverskridande e-tjänster i norra Sverige mellan Sverige och Finland, mellan Danmark och Sverige i Skåneregionen, turister i Stockholm samt svenska pensionärer som bor i södra Europa.

17.3 Omfattningen av kravet på erkännande

När det gäller bedömningar av hur förordningstexten ska tolkas är det svårt att förutspå den rättsliga utvecklingen. Utredningen kan analysera vissa frågor, göra avvägningar av alternativa tolkningssätt och även lämna rekommendationer för hur utredningen anser att offentliga myndigheter bör förbereda sig och agera när användare vill identifiera sig i deras e-tjänster med en utländsk elektronisk identitetshandling. Utredningen kan däremot inte med säkerhet veta hur EU-domstolen kommer att agera i eventuella framtida tvister om hur förordningstexten ska tolkas. Utredningen kan därför inte uttala sig om hur förordningstexten ska tolkas i specifika fall utan på ett mer generellt plan uppskatta de rimliga konsekvenserna av förordningens lydelse.

17.3.1 Vem ska erkänna den elektroniska identitetshandlingen?

Utredningen bedömer:
att varje offentlig myndighet som tillhandahåller en e-tjänst får avgöra om en elektronisk identitetshandling ska erkännas eller inte.

I artikel 6 i eIDAS-förordningen står det att medel för elektronisk identifiering som utfärdats i en annan medlemsstat under vissa för-

hållanden ska erkännas i den första medlemsstaten för gränsöverskridande autentisering för att få åtkomst till en nättjänst. Det specificeras inte vem som har skyldighet att erkänna den elektroniska identitetshandlingen. Det kan vara medlemsstaten i fråga eller varje myndighet i medlemsstaten.

Det finns inte någon central funktion för erkännande i Sverige. Det har enligt utredningens vetskap inte heller lyfts några förslag om en sådan funktion. I praktiken blir det därför varje e-tjänst eller offentlig myndighet bakom e-tjänsten som kommer att ställas inför ställningstagandet att erkänna den elektroniska identitetshandlingen eller inte. Eftersom det är tydligt specificerat vilka elektroniska identitetshandlingar som ska erkännas blir det inget svårt ställningstagande att göra.

Om de offentliga myndigheterna i Sverige är dåligt förberedda när användare med europeiska elektroniska identitetshandlingar vill identifiera sig är det möjligt att EU-kommissionen på något sätt anmodar Sverige att se till att de offentliga myndigheterna kan erkänna europeiska elektroniska identitetshandlingar.

17.3.2 När krävs det att utländska elektroniska identitetshandlingar ska erkännas?

Utredningen bedömer:
att utländska godkända elektroniska identitetshandlingar ska erkännas när det enligt svensk rätt eller den offentliga myndighetens administrativa förfaranden krävs en elektronisk identitetshandling för att få åtkomst till en e-tjänst som tillhandahålls av den offentliga myndigheten.

Enligt artikel 6 om ömsesidigt erkännande ska utländska godkända elektroniska identitetshandlingar erkännas när det enligt nationell rätt eller nationella administrativa förfaranden *krävs* elektronisk identitetshandling för att få åtkomst till en e-tjänst som tillhandahålls av ett offentligt organ.

Om det finns nationella författningskrav på att elektronisk identitetshandling ska användas för att få åtkomst till e-tjänsten ska alltså även utländska elektroniska identitetshandlingar erkännas. Dessutom måste de offentliga myndigheterna avgöra när det ska krävas

elektronisk identitetshandling för att få åtkomst till en e-tjänst. Nationella administrativa förfaranden är inget formaliserat begrepp utan borde enligt utredningens mening innebära att varje offentlig myndighet analyserar behovet av säkerhet vid identitetskontroll av användaren. I e-tjänster som inte har höga säkerhetsbehov kan man använda sig av andra inloggningsmetoder såsom användarnamn och lösenord. Vid inloggning till sådana e-tjänster krävs inte elektronisk identitetshandling och följden borde således bli att det inte heller uppstår något krav på att erkänna utländska elektroniska identitetshandlingar i sådana e-tjänster.

Det finns exempel på e-tjänster hos offentliga myndigheter där det är valfritt för användaren att identifiera sig med elektronisk identitetshandling eller logga in med användarnamn och lösenord. Inte heller i dessa fall bör det enligt utredningens mening uppstå ett krav på erkännande av utländska elektroniska identitetshandlingar eftersom det inte *krävs* elektronisk identitetshandling för att få åtkomst till e-tjänsten i fråga.

17.3.3 Vad innebär erkännandet?

Utredningen bedömer:
att målsättningen bör vara att erkännande av utländska elektroniska identitetshandlingar i svenska offentlig myndigheters e-tjänster innebär att – utan att göra avsteg från säkerhetsmässiga hänsynstaganden – ge användaren tillgång till de e-tjänster hon eller han har behov av.
att erkännandet ska avse identifieringen men inte den slutliga åtkomsten till e-tjänsten.
att om användaren inte ges tillträde till e-tjänsten ska ett erkännande ändå alltid innebära att den offentliga myndigheten hälsar användaren välkommen och informerar om vad som gör att användaren inte kan ges tillträde och vad som krävs för att kunna ges tillträde. Användaren bör också alltid kunna hänvisas till analog service med sitt ärende.

Det finns olika uppfattningar i medlemsstaterna om vad det ömsesidiga erkännandet innebär. Att erkänna en elektronisk identitetshandling kan innebära att användaren hälsas välkommen till den

offentliga myndighetens e-tjänst men att där inte finns något i övrigt som användaren kan nyttja. Att erkänna en elektronisk identitetshandling kan också innebära att ge användaren full rätt att utnyttja alla e-tjänster som den offentliga myndigheten erbjuder mot krav på identifiering med elektronisk identitetshandling.

Utredningen anser att målsättningen bör vara att erkännande av utländska elektroniska identitetshandlingar i svenska offentliga myndigheters e-tjänster innebär att – utan att göra avsteg från säkerhetsmässiga hänsynstaganden – ge användaren tillgång till de e-tjänster hon eller han har behov av.

I skäl 14 till eIDAS-förordningen anges att principen om ömsesidigt erkännande endast bör avse autentisering för en nättjänst. Åtkomsten till nättjänsten och dess slutliga leverans till användaren bör vara nära kopplad till rätten att ta emot sådana tjänster enligt villkoren i nationell lagstiftning.

En användare med svensk elektronisk identitetshandling har inte användning av alla svenska e-tjänster och får därför inte tillgång till allt trots att den elektroniska identitetshandlingen erkänns av den offentliga myndigheten. Det kan gälla e-tjänster i en kommun som användaren inte har någon koppling till eller specifika e-tjänster enbart för användare som har en relation med en offentlig myndighet av någon särskild anledning. Användaren behöver inte tillgång till Skatteverkets e-tjänster för egenföretagare om hon eller han inte har något eget företag eller Försäkringskassans e-tjänster för föräldrar om hon eller han inte är förälder.

På samma sätt kan offentliga myndigheter begränsa användare med utländska elektroniska identitetshandlingar om det inte finns någon relation som visar att användaren har behov av att använda en e-tjänst. En sådan relation kan visas genom ett svenskt personnummer eller styrkt samordningsnummer.

De offentliga myndigheterna behöver också analysera sin roll och sina e-tjänster när det kommer till säkerhet. Offentliga myndigheter som är utbetalande eller vars e-tjänster är ett led i en kedja som leder till en utbetalning måste naturligtvis vara extra vaksamma. Frågan är här vad skyldigheten att erkänna utländska elektroniska identitetshandlingar innebär i förhållande till den offentliga myndighetens egna säkerhetskrav. Utgångspunkten bör enligt utredningens mening vara att de godkända utländska elektroniska identitetshandlingarna jämställs med de svenska som den offentliga myndigheten redan hanterar.

I svenska offentliga myndigheters e-tjänster med höga säkerhetskrav måste användaren ha ett svenskt personnummer eller styrkt samordningsnummer. Det svenska personnumret bekräftas genom identitetskontrollen via den elektroniska identitetshandlingen. Om användaren med en utländsk elektronisk identitetshandling kan bekräfta ett svenskt personnummer på motsvarande sätt bör användaren kunna nyttja e-tjänsten. För detta behöver en koppling mellan den utländska elektroniska identitetshandlingen och det svenska personnumret göras med mycket hög grad av säkerhet.

I de fall användaren inte har något svenskt personnummer eller inte med tillräcklig säkerhet kan bekräfta det använda personnumret kan kravet på erkännande enligt utredningens mening inte innebära att användaren ska ges tillträde till e-tjänsten.

Kravet på erkännande bör ändå i praktiken leda till att den svenska offentliga myndigheten hälsar användaren välkommen och informerar om vad som gör att användaren inte kan ges tillträde och vad som krävs för att kunna ges tillträde. Användaren bör också i förekommande fall kunna hänvisas till den instans som kan hjälpa till med t.ex. en koppling.

Detta är i praktiken det som brukar benämnas väntrum i eIDAS-sammanhang. Utredningens uppfattning är att det är viktigt att dessa väntrum inte blir återvändsgränder utan att användaren får den information som behövs för att kunna ta ärendet vidare.

Frågan om vad erkännandet innebär har analyserats i olika sammanhang. I Sverige är, enligt utredningens mening, den allmänna uppfattningen att erkännandet ska avse identifieringen men inte den slutliga åtkomsten till e-tjänsten. Det har även beskrivits i eSams vägledning.[7] I de övriga medlemsstaterna förekommer dock andra tolkningar av begreppet erkännande.

[7] eSam:s vägledning, Juridisk vägledning för införande av e-legitimering och e-underskrifter, s. 57 f.

17.3.4 Vad säger de andra medlemsstaterna?

Utredningen har under utredningstiden träffat företrädare för några av de andra medlemsstaterna[8] bland annat för att få en bild av deras uppfattning om hur eIDAS-förordningen ska tolkas och vad de ser för konsekvenser av eIDAS-förordningens krav. Utredningen har även i oktober 2017 skickat ut en enkät till ett tiotal medlemsstater vars system liknar de svenska eller som har kommit långt i sitt förberedelsearbete. Av medlemsstaternas svar framkommer bl.a. följande.

Danmark

Danmark håller på att utveckla en eIDAS-nod som alla offentliga organ kan ansluta till. Den blir en del av den nationella digitala infrastrukturen. Man är också i färd med att analysera hur en central kopplingsfunktion kan byggas upp.

I Danmark avser man att utveckla ett gemensamt centralt väntrum för utländska användare. Detta arbete är dock fortfarande i analysstadiet. Det kan komma att bli två väntrum, ett för privatpersoner och ett för företag. Väntrummet är tänkt för myndigheter som har e-tjänster och som inte vill hantera väntrumsfrågan individuellt.

Det kommer att bero på varje myndighet som har e-tjänster vilka språkanpassningar som ska göras. Vissa affärsorienterade e-tjänster kommer troligtvis att översättas till polska, tyska och andra språk. De flesta kommer troligtvis översättas till engelska.

I Danmark är folkbokföringssystemet förhållandevis likt det svenska med mycket beständiga s.k. CPR-nummer (motsvarighet till personnummer) och E-nummer (motsvarighet till samordningsnummer). Det är ännu inte bestämt om pseudonymer kommer att användas eller inte. Det är heller inte avgjort hur beständigt det danska personidentifieringsnumret kommer att vara. Men det är inte troligt att danskar ska kunna ha mer än ett identitetsnummer.

Danmark kommer inte att anmäla sin nationella elektroniska identitetshandling inom de närmsta åren eftersom man håller på att implementera ett nytt system för elektroniska identitetshandlingar.

[8] När utredningen använder begreppet medlemsstaterna avses även Norge, Island, Lichtenstein och Schweiz som har skrivit avtal om att också få ingå i regelverket.

Finland

I Finland är det obligatoriskt enligt lag att alla offentliga organ använder befolkningsregistrets officiella lösning för elektronisk identifiering. Fr.o.m. september 2018 kommer befolkningsregistret i Finland att skicka utländska användares attribut enligt eIDAS-förordningen till de myndigheter som klarar och behöver ta emot dessa användare.

Finland kommer att ha en speciallösning för de myndigheter som inte hinner förbereda sig i tid genom att använda säker elektronisk post speciellt till de utländska användare som vill ha tillträde till dessa e-tjänster.

Finland avser inte att utveckla någon särskild kopplingslösning till sitt nationella identitetsnummer. Man har i Finland startat ett projekt för att utveckla nästa generations identitetsnummer som ska inkludera biometri för att förebygga identitetsstölder. Finland anser sig inte ha kapacitet att klara en central kopplingsservice, vare sig för utländska användare eller för finska användare som bor utomlands. Koppling får i stället utföras lokalt av varje tillhandahållare av e-tjänst efter deras respektive behov.

Man planerar inte heller något centralt väntrum. Myndigheterna ska agera enligt befintliga regler och förfaranden för att tilldela finska identitetsnummer till icke-medborgare.

Varje myndighet som har e-tjänster får även själv bestämma vilka språk som ska finnas. Alla myndigheters e-tjänster är redan tvåspråkiga och ska finnas på finska och svenska.

Finland kommer inte att använda pseudonym. Man väntar sig att medlemsstaterna behandlar information om identitetsnummer konfidentiellt och i enlighet med dataskyddsförordningen.

Det finska identitetsnumret är mycket beständigt och ändras bara vid t.ex. identitetsstöld eller könsbyte. Det är omöjligt att samma person från Finland har flera identitetsnummer.

Nederländerna

I Nederländerna planerar man att erkänna och ge anmälda utländska elektroniska identitetshandlingar i kombination med att individen har ett holländskt identitetsnummer tillträde till önskade e-tjänster i samma utsträckning som om användaren har en nederländsk elektronisk identitetshandling. Man kommer att erbjuda en pintjänst som

jämför attributen i den utländska elektroniska identitetshandlingen med uppgifter i folkbokföringen. Både minimi- och valfria attribut kommer att jämföras.

I Nederländerna kommer det inte att finnas väntrum. För att få tillgång till en offentlig e-tjänst måste man ha holländskt identitetsnummer (s.k. BSN), tilldelat enligt nederländsk lag. Det innebär att man måste inställa sig fysiskt för identitetskontroll på en myndighet i Nederländerna.

Språkanpassningar diskuteras nu men är ännu inte fastställt vad som ska krävas av respektive myndighet.

Nederländerna kommer att använda sig av pseudonymer. Nederländska personidentifieringsnummer är livslånga i persistens.[9] Det är omöjligt att en individ kan ha flera holländska personidentifieringsnummer.

Norge

Utredningen har fått ta del av en norsk rapport från Skatteetaten där frågan om en central kopplingstjänst och det norska förhållningssättet till eIDAS-förordningens krav finns beskrivna.[10]

En utgångspunkt för det norska anpassningsarbetet är skäl 14 i eIDAS-förorningen enligt vilket kravet om ömsesidigt erkännande bara träffar autentiseringen medan tillträde till e-tjänsterna beror på nationell rätt.

Norge vill utveckla möjligheterna med bilaterala överenskommelser med i första hand de andra nordiska länderna. Man ser dels att det säkerhetsmässigt skulle fungera eftersom de nordiska länderna har liknande system med mycket persistenta identitetsnummer, dels att en stor del av användarbehovet skulle kunna täckas eftersom många av situationerna med gränsöverskridande identifiering kommer att gälla användare som bor i gränstrakter mellan de nordiska länderna.

Det har övervägts om det skulle gå att automatiskt rekvirera s.k. D-nummer (motsvarighet till svenska samordningsnummer) för användare från utvalda samarbetsländer men man har ännu inte kommit

[9] Med persistens avses i detta sammanhang att numret ska vara detsamma så att man kan lita på att individen är densamma, helst under hela sin livstid.
[10] Skatteetatens rapport, eIDAS-innloggning med europeisk e-ID til norske tjenester, Versjon 1.0.

till något ställningstagande. Se utredningens bedömning av denna fråga i Sverige i avsnitt 17.5.

För de användare som inte har en elektronisk identitetshandling från ett land Norge har ingått ett bilateralt avtal med, väntar inledningsvis väntrum.

Tyskland

Den tyska infrastrukturen är decentraliserad. E-tjänsttillhandahållarna sköter var och en sin egen eIDAS-nod.

Man bedömer att tyska och engelska räcker som språk.

I Tyskland används pseudonymer redan nationellt och det är naturligt att göra det också inom vid gränsöverskridande identifiering.

Det finns ingen motsvarighet till personnummer i Tyskland och ingen liknande persistens. Det nationella personidentifieringsnumret kommer därför att ändras varje gång en person byter elektronisk identitetshandling. Man får bara ha en elektronisk identitetshandling åt gången.

Österrike

I Österrike har man erkänt utländska elektroniska identitetshandlingar sedan 2008. Infrastrukturen är därför redan förberedd för eIDAS-förordningens krav. Inkommande utländska användare registreras i ett kompletterande register och tilldelas ett unikt identifieringsnummer. De får också en pinkod för att man ska kunna identifiera samma person igen.

Österrike ser inget skäl att inte ge utländska användare tillgång till e-tjänster eller registrera i det kompletterande registret baserat på erfarenheter från projekten STORK och STORK 2.0. Det har redan visats att det kan ske automatiskt.

En koppling mellan en utländsk elektronisk identitetshandling och en österrikisk identitet som inte är självklar kan behöva manuell behandling. Det kan gälla t.ex. om det finns flera träffar i det kompletterande registret eller vid andra oklarheter.

Den österrikiska noden klarar engelska och tyska. När det gäller e-tjänsterna får myndigheterna bestämma eftersom det inte regleras av eIDAS-förordningen.

Österrike använder redan pseudonymer också nationellt. Det österrikiska identifieringsnumret är livslångt i persistens. Man kan bara ha ett österrikiskt identifieringsnummer.

17.4 Verksamhetsmässiga konsekvenser

Alla offentliga myndigheter som har e-tjänster behöver i god tid se över sina processer och anpassa sin verksamhet efter eIDAS-förordningens krav så att de kan ta emot användare med europeiska elektroniska identitetshandlingar. Svenska offentliga myndigheter består av en mängd vitt skilda verksamheter. Förutom sina olika uppdrag varierar de t.ex. i storlek, kultur, ekonomiska förutsättningar och digital mognad. Av naturliga skäl varierar det därför också hur långt de offentliga myndigheterna har kommit i sina förberedelser.

17.4.1 De offentliga myndigheterna bör agera försiktigt

Utredningen bedömer:
att de offentliga myndigheterna bör avstå från att göra egna kopplingar mellan utländska elektroniska identitetshandlingar och svenska person- och samordningsnummer.

Som tidigare har beskrivits ovan bör medvetenhet om informationssäkerhet prägla de offentliga myndigheternas anpassningar och beredskap. I varje steg av anpassning måste de offentliga myndigheterna analysera eventuella risker och konsekvenser av förändringen.

Utredningen anser att de offentliga myndigheterna bör avstå från att göra egna kopplingar mellan utländska elektroniska identitetshandlingar och svenska person- eller samordningsnummer. De offentliga myndigheterna får uppgifter om användarens för- och efternamn samt födelsedatum i identitetsintyg. Om de även begär att användaren ska ange sitt svenska person- eller samordningsnummer kan den offentliga myndigheten själv göra en jämförelse med uppgifter ur folkbokföringen (via Navet). Därefter kan den offentliga myndigheten bedöma om den vill ge användaren tillträde till e-tjänsten. Om uppgifterna stämmer överens kan det vara lockande att släppa in användaren i e-tjänsten.

Av säkerhetsskäl som har beskrivits av Skatteverket i sin rapport om kopplingsregister[11] och även finns återgivna ovan menar utredningen dock att detta förfarande kan medföra stora risker. Innan det finns en central kopplingstjänst med erforderlig säkerhetsnivå för att koppla samman utländska elektroniska identitetshandlingar med svenska person- och samordningsnummer bör de offentliga myndigheterna inte ge användarna tillträde till de e-tjänster som kräver svenskt person- eller samordningsnummer.

17.4.2 Vad berörda offentliga myndigheter behöver göra

Utredningen bedömer:
att varje statlig myndighet, kommun och landsting som tillhandahåller e-tjänster som kräver elektronisk identifiering behöver förbereda följande steg:

- Planera för e-tjänsternas delar,
- Förbereda meddelande om att den europeiska elektroniska identitetshandlingen är erkänd,
- Påbörja den tekniska integrationen,
- Avgöra vem som får göra vad i e-tjänsten,
- Överväga hur e-tjänsterna ska hantera det europeiska personidentitetsbegreppet,
- Förbereda informationsmeddelande om den svenska offentlighetsprincipen,
- Anpassa e-tjänstens språk, åtminstone så att den erbjuds på engelska,
- Informera berörda om eventuella förändringar.

[11] Skatteverkets promemoria från den 24 oktober 2016, Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer, dnr 131 184020-16/113.

Det finns vägledning från Fonden för ett sammanlänkat Europa i hur de offentliga myndigheterna kan gå tillväga för att förbereda sig för att ta emot europeiska elektroniska identitetshandlingar.[12]

Det de offentliga myndigheterna behöver göra för att förbereda sig har i flera sammanhang beskrivits av E-legitimationsnämnden som har i uppdrag att informera och bistå den offentliga sektorn i frågor om elektroniska identitetshandlingar både i Sverige och inom ramen för eIDAS-förordningen. Nedanstående lista är hämtad bl.a. från E-legitimationsnämndens material.[13] Den kan användas som checklista för berörda offentliga myndigheter.

Planera för e-tjänsternas delar

Varje e-tjänst behöver kunna göra det möjligt att identifiera sig med en europeisk elektronisk identitetshandling. Det ordnas lämpligen genom att lägga till ”Foreign eID” som identifieringsalternativ där det är möjligt för användare att identifiera sig med svenska elektroniska identitetshandlingar.

E-tjänsterna behöver även kunna ställa ut en begäran om identitetsintyg för att skicka via den svenska och den utländska noden till den utländska utfärdaren av den elektroniska identitetshandlingen.

E-tjänsterna behöver därefter kunna ta emot identitetsintyg som skickas tillbaka från den utländska utfärdaren via den utländska och den svenska noden.

Slutligen behöver e-tjänsterna kunna meddela användaren att den elektroniska identitetshandlingen är accepterad (erkänd).

Meddelande om att den elektroniska identitetshandlingen är erkänd

Tillhandahållarna av e-tjänster behöver förbereda ett standardiserat textmeddelande som kan visas upp för användare som identifierar sig (autentiseras) med en eIDAS-erkänd europeisk elektronisk identitetshandling, men där behörighet till e-tjänsten saknas. Ett exempel kan

[12] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Connect+a+public+or+private+online+service+-+Overview, 2017-11-07.
[13] E-legitimationsnämnden, Introduktion till eIDAS, dnr. 131 151182-16/9517, den 19 augusti 2016.

vara om e-tjänsten endast kan hantera användare som har svenska personnummer och ett centralt register för koppling till sådant personnummer saknas vid inloggning i e-tjänsten.

Påbörja den tekniska integrationen

E-tjänsterna (och e-tjänsternas eventuella integrationslager) behöver ta teknisk höjd för eIDAS-förordningen. E-legitimationsnämnden tillhandahåller testmiljöer och kan bistå i anpassningsarbetet.

Avgör vem som får göra vad i e-tjänsten

Tillhandahållare av e-tjänster behöver planera för vilka uppgifter (attribut) som behövs för att kunna avgöra användarens behörighet, och hur uppgifterna ska hämtas in, när användaren identifierar sig med en europeisk elektronisk identitetshandling.

Det är viktigt att de offentliga myndigheterna inte avslutar de analoga möjligheter till service som redan finns. Om användaren inte kan ges tillträde till e-tjänsten bör de offentliga myndigheten informera om hur användaren ska göra för att utföra sina ärenden analogt genom att erbjuda eventuella blanketter och kontaktmöjligheter.

Personidentitetsbegrepp i utländska elektroniska identitetshandlingar

Personidentitetsbegreppet i det utländska identitetsintyget är unikt och pekar på endast en individ. Däremot kan en individ med flera elektroniska identitetshandlingar ha flera olika personidentitetsbegrepp. Många svenska e-tjänster har lagstadgade krav på att användaren ska ha svenskt personnummer eller samordningsnummer. En individ med svenskt samordningsnummer eller personnummer kan ha en utländsk elektronisk identitetshandling.

Tillhandahållare av e-tjänster behöver överväga hur e-tjänsterna ska hantera det utländska personidentitetsbegreppet som kommer med i autentiseringen. Eventuellt kommer det att finnas ett centralt kopplingsregister för att underlätta för tillhandahållarna av e-tjänster att koppla samman det utländska personidentitetsbegreppet med ett

svenskt personnummer eller styrkt samordningsnummer men innan det är på plats anser utredningen att de offentliga myndigheterna bör agera försiktigt, se avsnitt 17.4.1.

Förbered informationsmeddelande om den svenska offentlighetsprincipen

Enligt den svenska offentlighetsprincipen ska alla ha rätt att ta del av allmänna handlingar som inte är sekretessbelagda. Med allmän handling menas varje handling, tryckt eller elektronisk, som är förvarad hos en offentlig myndighet, samt har inkommit till den offentliga myndigheten utifrån eller har upprättats inom den offentliga myndigheten. I Sverige gäller som huvudregel att offentlighet råder för individers identitetsbegrepp, t.ex. personnummer och namn. Det innebär att vem som helst kan begära ut information där det förekommer identitetsbegrepp kopplade till andra individer än de själva.

I många av de andra medlemsstaterna är regleringen annorlunda. Där behandlas identitetsbegrepp med sekretess och användare från dessa länder kanske utgår från att behandlingen är densamma i Sverige. Därför anser utredningen att det innan identifieringsprocessen startar behöver finnas ett kort informationsmeddelande (standardiserat textmeddelande) om offentlighetsprincipen i Sverige i de e-tjänster som ska erkänna europeiska elektroniska identitetshandlingar.

Offentlighetsprincipen gäller naturligtvis redan i motsvarande analoga flöden. De offentliga myndigheterna borde därför även tillhandahålla informationen så att den når de individer som inte använder e-tjänsterna.

Överväg e-tjänstens språk

I eIDAS-förordningen regleras inte vilka språk e-tjänster ska erbjuda. Här behöver tillhandahållarna av e-tjänster analysera hur man bäst kan hjälpa sina användare. Som första steg anser utredningen att man behöver se till att e-tjänster som erbjuds användare med europeiska elektroniska identitetshandlingar finns på engelska.

I artikel 2 i kommissionens genomförandebeslut 2015/296 anges att samarbetsspråket ska vara engelska om inte annat överenskommits med den berörda medlemsstaten. Det handlar där om inrättande

av förfaranden för samarbete mellan medlemsstaterna, men det säger åtminstone något om vad som anses vara förstahandsval av språk mellan medlemsstaterna i eIDAS-sammanhang.

Därefter kan man utgå från de behov som väntas i respektive e-tjänst. Olika tillhandahållare kan vänta sig användare med olika språkfärdigheter.

Informera berörda

Tillhandahållare av e-tjänster behöver planera kommunicering av förändringarna till alla berörda målgrupper.

17.4.3 Hur kan de offentliga myndigheterna erbjuda ännu bättre service?

Utredningen bedömer:
att de offentliga myndigheterna därefter kan vidareutveckla sin service gentemot utländska användare genom att:

- Fortsätta utveckla funktioner,
- Bygga vidare på servicen till de som inte ges tillträde,
- Erbjuda mer information på fler språk.

Efter att de offentliga myndigheterna vidtagit de åtgärder som är nödvändiga enligt det förra avsnittet bör de enligt utredningens mening överväga hur de kan erbjuda ännu bättre service till sina respektive användare. Det kräver individuella analyser genom t.ex. brukarundersökningar av varje verksamhet för att ta ställning till hur den offentliga myndigheten i fråga bäst hjälper de användare som är intresserade av deras e-tjänster.

Fortsätt utveckla funktioner

Med vetskap om vilka utländska användare som identifierar sig i e-tjänsterna och vad de har för behov kommer de offentliga myndigheterna att kunna utveckla sin servicenivå ytterligare. De kommer att kunna göra olika val av nivå för anpassning av funktioner på t.ex. mina sidor samt för olika verktyg och guider som riktas till användarna.

Bygg vidare på servicen till de som inte ges tillträde

Likaså när det gäller användare som inte kan ges tillgång till e-tjänsterna finns det möjlighet, med ökad kunskap om dem, att utveckla servicegraden gentemot dem. Det kan gälla hänvisningar om var de kan vända sig för fortsatt hjälp eller utökat material med blanketter eller liknande tillgängligt direkt på webbplatsen.

Erbjud mer information på fler språk

Efter att ha sett till att tillhandahålla en basnivå av information och e-tjänster på engelska bör offentliga myndigheter göra en djupare analys av språkbehoven i just deras e-tjänster.

Det kan förekomma olika språkbehov beroende av användarens val av språk, användarens val av elektronisk identitetshandling eller vad användaren verkligen vill göra i e-tjänsten. Från vilka länder kommer användarna? Vad har de för språkkunskaper? Vilket språk väljer de själva? Är många av användarna med europeiska elektroniska identitetshandlingar utlandsboende svenskar med goda kunskaper i svenska? För att möta användarnas behov krävs individuella analyser hos varje enskild offentlig myndighet som tillhandahåller e-tjänster.

Både EU-kommissionen och Google erbjuder översättningsverktyg som offentliga myndigheter kan använda för att anpassa sina e-tjänster. Utvecklingen av sådana översättningsverktyg går snabbt och kvalitén förväntas snart nå sådana nivåer att offentliga myndigheter inte behöver använda sig av manuell översättning.

Webbplatsen verksamt.se har låtit konsultföretaget Stelacon analysera språkbehovet för sina e-tjänster. Stelacon har därefter sammanställt tre konkreta rekommendationer på vad som skulle komplettera webbportalen verksamt.se på bästa sätt. Detta så att företagare från

andra EU-länder inte bara skulle förstå det svenska systemet bättre, utan även få tydligare information hur det fungerar att driva företag och sälja tjänster i Sverige. Rekommendationerna utgår från förutsättningarna för verksamt.se men utredningen anser ändå att de kan vara av värde även i andra offentliga myndigheters analyser av sina språkbehov.

Mer information på engelska

Språket är en viktig komponent som företagare för att både kommunicera med kunder och relevanta myndigheter samt ta del av viktig information på ett effektivt sätt. De intervjuade företagarna indikerar att engelska är tillräckligt som språk, men att mer information bör finnas på engelska för att göra mer information tillgänglig. Stelacon rekommenderar att utöka informationsmängden som finns tillgänglig på engelska.

Enkel och orienterande information

Företag efterfrågar information som är lika enkel att förstå som enkel att hitta. Steg för steg-guider tycker företagare är ett bra och vägledande sätt att ta till sig information. Verksamt.se har flera guider av den typen, och en rekommendation är därför att utöka det utbudet, framför allt för processen att skaffa personnummer och bankkonto där många företag har problem.

I tillägg till steg för steg-guider kan olika mallar vara ett bra komplement. Dessa mallar kan hjälpa företagarna när de ska utforma exempelvis fakturor till sina kunder eller sin F-skattsedel.

Bättre marknadsföring av verksamt.se

Sju av de elva intervjuade företagarna känner till webbportalen verksamt.se. Av dessa har fyra använt sig av information på sidan och de är väldigt nöjda. Det finns därmed utrymme att både öka kännedomen om verksamt.se och öka användningen av webbplatsen.

Stelacon rekommenderar därför en utförlig marknadsföringsstrategi för den engelska versionen av verksamt.se.[14]

17.4.4 Regeringen ska utse färdledande offentliga myndigheter

Utredningen föreslår:
att regeringen utser ett antal färdledande offentliga myndigheter som i sitt agerande kan hjälpa andra offentliga myndigheter att anpassa sig till eIDAS-förordningens krav och möjligheter.

För att skapa ytterligare vägledning till de offentliga myndigheterna föreslår utredningen att regeringen ska utse ett antal färdledande offentliga myndigheter som kan visa vägen och bistå andra liknande offentliga myndigheter med kunskap och erfarenhetsutbyte.

Det är viktigt att de offentliga myndigheterna representerar olika verksamhetssektorer och är av olika storlek. De färdledande offentliga myndigheterna behöver alla ha uppnått en viss mognad i digitaliseringsfrågor och dessutom ha kompetens och möjligheter att dela med sig av erfarenheter och expertis.

De färdledande offentliga myndigheterna behöver utgöras av minst en större statlig myndighet med mycket medborgarkontakt och väl utvecklade e-tjänster, någon statlig myndighet med lite mindre flöden t.ex. en länsstyrelse, ett landsting, en större kommun och en mindre.

De offentliga myndigheter som utses bör samverka om att ta fram material och stöd. Digitaliseringsmyndigheten kan också vara behjälplig i detta arbete.

[14] Behovsanalys för engelskspråkiga sidorna på verksamt.se, en studie av Stelacon efter uppdrag från Tillväxtverket.

17.5 Bör processen för tilldelning av samordningsnummer till utländska medborgare på distans automatiseras?

Utredningen bedömer:
att för att uppnå ökad grad av automatisering i processen för tilldelning av samordningsnummer måste kraven på säker identitetskontroll av de enskilda individerna sänkas eller så behöver samordningsnummersystemet ses över.

Enligt utredningens direktiv[15] ska utredaren analysera och lämna förslag på hur processen för tilldelning av samordningsnummer till utländska medborgare på distans genom elektroniska identitetshandlingar kan möjliggöras och automatiseras.

För att kunna ta ställning i denna fråga behövs först en genomgång av vad samordningsnummer är, dess syfte och hur de har utvecklats sedan de infördes.

17.5.1 Vad är samordningsnummer?

Samordningsnumret är konstruerat som ett personnummer men med sifferkombinationer som inte kan förekomma i ett personnummer på så sätt att siffrorna för dag adderas med 60. Motsvarigheten till personnumrets födelsenummer benämns i samordningsnumret individnummer. Kontrollsiffran beräknas med samma metod som beträffande personnumret. En man född den 3 oktober 1970 med individnummer 239 får följande samordningsnummer: 701063-2391.

På motsvarande sätt som personnumren är samordningsnumren unika såtillvida att två identiska samordningsnummer inte förekommer. Om en individ med ett samordningsnummer senare blir folkbokförd ersätts samordningsnumret med ett personnummer.[16]

I folkbokföringsförordningen[17] finns bestämmelser om tilldelning av personnummer och samordningsnummer. Skatteverket får tilldela samordningsnummer på begäran av en statlig myndighet eller

[15] Dir. 2016:39.
[16] Prop. 2008/09:111 s. 27 f.
[17] SFS 1991:749, FOF.

en utbildningsanordnare som har tillstånd att utfärda vissa examina[18] och som i sin verksamhet behöver ett samordningsnummer för en individ för att undvika personförväxling eller för att utbyta information om individen med andra offentliga myndigheter eller organisationer. Skatteverket kan också på eget initiativ tilldela samordningsnummer för registrering i beskattningsdatabasen.[19]

Samordningsnummer får tilldelas en individ om det inte råder osäkerhet om dennes identitet. I vissa fall kan dock samordningsnummer tilldelas ändå, bl.a. om det behövs för vissa registreringar inom rättsväsendet, för registrering i beskattningsdatabasen eller för registrering i Migrationsverkets verksamhetsregister när det gäller individer som omfattas av lagen[20] om mottagande av asylsökande m.fl.[21] Det är den statliga myndighet eller det organ som begär att en individ ska tilldelas samordningsnummer som ska bedöma om identiteten kan anses fastställd. Skatteverket får meddela närmare föreskrifter om de krav som ska ställas på identifieringen av en individ som ska tilldelas ett samordningsnummer.

En begäran om samordningsnummer ska innehålla uppgift om vilka handlingar som legat till grund för identifieringen och Skatteverket får begära att dessa handlingar lämnas in till Skatteverket.[22] Den statliga myndighet som begär ett samordningsnummer ska ange om det råder osäkerhet om någon uppgift som lämnas om individen.[23]

17.5.2 Skälen för att samordningsnummer infördes

För varje folkbokförd individ fastställs enligt 18 § folkbokföringslagen[24] ett personnummer som identitetsbeteckning. En individ som inte är eller har varit folkbokförd får efter begäran från en statlig myndighet tilldelas ett särskilt nummer, samordningsnummer.

Syftet med folkbokföringen har beskrivits i förarbetena till reglerna om samordningsnummer. Folkbokföringens kanske viktigaste uppgift är att för olika samhällsfunktioner tillhandahålla basuppgifter

[18] Utfärdare enligt lagen (1993:792) om tillstånd att utfärda examina.
[19] 5 § FOF.
[20] SFS 1994:137.
[21] 5 a § FOF.
[22] Detta gäller dock inte då samordningsnummer ska tilldelas en person som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall.
[23] 6 § FOF.
[24] SFS 1991:481.

om befolkningen i landet. För att det ska kunna fungera på ett korrekt och fullständigt sätt måste personnummer användas. Ett personnummer som har fastställts efter identitetskontroll motverkar förväxling av individer och öppnar möjlighet för en säker överföring av tillförlitliga personuppgifter mellan olika användare. Bland annat mot den bakgrunden är det, enligt förarbetena, naturligt att personnummer används inom folkbokföringen.

Bestämmelser om samordningsnummer infördes den 1 januari 2000 eftersom personnummer då reserverades för individer som är folkbokförda i Sverige. Tidigare tilldelades personnummer även till de individer som inte var folkbokförda. Den som rekvirerade personnummer för individer som inte var folkbokförda skulle ange om identiteten hade styrkts med pass eller annan handling. Det ankom alltså på den rekvirerande myndigheten att göra identitetskontrollen.

Som skäl för införandet av samordningsnummer anfördes bland annat att ett system med enhetliga personbeteckningar kan behövas även utanför folkbokföringen. Tilldelningen av personnummer utan koppling till folkbokföring grundades på att flera statliga myndigheter ansåg sig behöva ett gemensamt samordningsbegrepp för bl.a. kommunikation sinsemellan. Registreringen av personuppgifter omfattade ett mycket stort antal individer. Den berörde också viktiga områden, både för individen och samhället. Främst för att olika individer inte skulle förväxlas med varandra hade de statliga myndigheterna ett behov av att använda personnummer eller annan unik personbeteckning för registrerade individer.[25]

Enligt förarbetena var det otvivelaktigt så att personnumret kunde uppfattas som en sorts inträdesbiljett till samhället. Man ansåg att det kunde ifrågasättas om individer som inte var folkbokförda skulle ha den inträdesbiljett som personnumret innebär. Det kunde också uppfattas som stötande att brottslingar och brottsmisstänkta tilldelades personnummer. Dessa tillhörde också en kategori av individer vars identitet ofta är svår att fastställa. Det var dock inte bara vid registrering inom rättsväsendet som det kunde finnas identifieringssvårigheter. Även för skatteområdet var underlaget för kontroll av en individs identitet i många fall bristfälligt vid tilldelning av personnummer.

[25] Prop. 1997/98:9 s. 77 f.

Det konstaterades att om identitetskontrollen är otillräcklig kan följden bli att en individ tilldelas mer än ett personnummer. Det leder i sin tur till att individen kan uppträda under flera identiteter och förekomma med skilda nummer i olika register. Därmed försvåras personkontrollen exempelvis vid inresa från utlandet, polisiära ingripanden, lagföring och straffverkställighet. Om en individ har ”dubbla identiteter” finns det också risk för att han eller hon kan uppbära dubbla bidragsförmåner samt undandra sig förpliktelser av olika slag. Regeringen ansåg att tilldelningen av personnummer måste grundas på en identitetskontroll som uppfyller höga anspråk på säkerhet för att tilltron till personnumret som identifikationsbegrepp skulle upprätthållas.[26]

Det diskuterades vad ett nytt personidentitetsbegrepp skulle kallas och anfördes att av de beteckningar som föreslagits framstod samordningsnummer som bäst. Beteckningen är dock inte främst till för att utvisa en individs identitet varför beteckningen identitetsnummer kan vara missvisande. Registreringsnummer är inte heller bättre. Regeringen föreslog därför att det särskilda numret skulle benämnas samordningsnummer.

Tilldelningen av samordningsnummer skulle i första hand användas för de ändamål för vilka personnummer inte tilldelades. Regeringen såg inga hinder mot att låta även andra statliga myndigheter och verksamhetsområden använda samordningsnummer men det anfördes samtidigt att en utvidgad tilldelning av samordningsnummer endast borde medges om det aktuella verksamhetsområdet behövde numret antingen för att undvika personförväxling eller för uppgiftsutbyte med andra myndigheter.[27]

När det gäller identifieringskravet anfördes bl.a. följande.[28]

> Det är i likhet med vad som gäller för tilldelning av personnummer viktigt att en persons identitet är klarlagd när samordningsnummer tilldelas. I dag görs kontrollen av en persons identitet i stor utsträckning av den myndighet som rekvirerar personnummer för en person som inte är folkbokförd. Identitetskontrollen bör enligt regeringens mening även fortsättningsvis ligga utanför folkbokföringen. Det är alltså den rekvirerande myndigheten som har att fullgöra den kontrollen och så långt det är möjligt söka fastställa identiteten. Rekvisitionen av samordningsnummer bör alltid innehålla uppgift om underlaget (pass, körkort, kon-

[26] Prop. 1997/98:9 s. 78 f.
[27] Prop. 1997/98:9 s. 80.
[28] Prop. 1997/98:9 s. 82 f.

> takter med utländska instanser m.m.) för myndighetens identitetskontroll. Rekvirerande myndighets bedömning av personens identitet och lämnade uppgifter skall också anges. För flertalet myndigheter som kommer att rekvirera samordningsnummer torde det inte heller innebära några problem att en persons identitet skall vara fastställd. För polismyndigheterna och skattemyndigheterna kan det dock innebära vissa komplikationer.

Man fick enligt regeringens mening godta att en individs identitet kunde vara oklar när det gäller tilldelning av samordningsnummer för registrering inom rättsväsendets register och i skatteregister. Samtidigt måste de rekvirerande statliga myndigheterna sträva efter att i största möjliga utsträckning fastställa den enskildes identitet.

Det anfördes vidare att när fråga uppkommer om att tilldela samordningsnummer för persongrupper som inte tidigare hade tilldelats personnummer borde kravet på säker identifiering särskilt uppmärksammas. Regelmässigt borde identitets- och uppgiftskontrollen ligga hos den statliga myndighet som rekvirerar samordningsnumret.[29]

17.5.3 Utvecklingen av samordningsnummer

Knappt tio år efter att samordningsnummer infördes i Sverige stod samma principer kvar när det bl.a. övervägdes om samordningsnummer skulle bytas ut mot något annat. Regeringen anförde då att i likhet med vad som gäller för personnummer är det viktigt att en individs identitet är klarlagd när han eller hon får ett samordningsnummer. Individens identitet ska därför som huvudregel vara fastställd även för att denne ska kunna tilldelas ett samordningsnummer.

När det gäller individer som ska registreras i beskattningsdatabasen och inom rättsväsendet görs dock undantag från kravet att identiteten ska vara fastställd. Omkring 60 procent av de samordningsnummer som tilldelas under ett år tilldelas individer tillhörande dessa grupper.[30]

Person- och samordningsnumren är personbeteckningar vars syften huvudsakligen är att undvika personförväxling och att underlätta informationsutbyten om individer. Inga rättsverkningar är direkt knutna till att en individ har en personbeteckning. För att olika be-

[29] Prop. 1997/98:9 s. 83 f.
[30] Prop. 2008/09:111 s. 27.

stämmelser ska vara tillämpliga kan det däremot krävas att individen har en viss anknytning till landet. Ofta krävs folkbokföring, det vill säga att individen är bosatt i landet i folkbokföringslagens mening, eller bosatt i landet enligt någon annan definition av bosättning. Det gäller exempelvis för flera socialförsäkringsförmåner. Den som är folkbokförd betraktas normalt som bosatt i landet enligt de definitioner av bosättning som finns och behöver därför oftast inte styrka sin bosättning på något annat sätt. Alla som är eller har varit folkbokförda har ett personnummer.

I folkbokföringsdatabasen registreras ett stort antal uppgifter om individer som folkbokförs och därmed också får ett personnummer. Det finns också en skyldighet för individer och myndigheter att lämna uppgifter om nya eller ändrade förhållanden. Uppgifterna ska normalt vara styrkta för att Skatteverket ska registrera dem. Det är således möjligt för andra aktörer att kontrollera olika uppgifter om individer som är registrerade i databasen. Även individer som inte längre är folkbokförda i landet anmäler i stor utsträckning ändrade uppgifter till Skatteverket, exempelvis om barn som föds i utlandet och om ändrat civilstånd.

Det är däremot få uppgifter som registreras om individer med samordningsnummer, många gånger är uppgifterna inte heller styrkta. Möjligheterna att kontrollera uppgifter om dessa individer är därför mycket mindre. I och med att en stor andel av de individer som får ett samordningsnummer har en mycket svag anknytning till Sverige har de typiskt sett inte heller något intresse av att anmäla ändringar i de registrerade uppgifterna. Personnumret används inom i stort sett alla samhällssektorer. Samordningsnumret är mer okänt och inte lika vedertaget som personbeteckning. I it-stöd finns också hinder som innebär att de inte kan hantera personnummer där siffrorna för dagen överstiger 31.

Det anförs vidare att det huvudsakliga syftet med samordningsnumret även i fortsättningen bör vara att tillgodose de statliga myndigheternas behov av ett enhetligt nummer för att undvika personförväxling och för att utbyta information med andra myndigheter och organisationer om individer som vistas tillfälligt här i landet eller som har rätt till olika förmåner utan att vistas här. Härutöver måste även beaktas samordningsnumrens funktion ur individens perspektiv. Det finns individer med samordningsnummer som vistas i Sverige under en inte helt kortvarig tid och bland dessa finns det individer med ett

starkt behov av att ha en fungerande identitetsbeteckning för att kunna sköta sina vardagliga liv.[31]

17.5.4 Tilldelning av samordningsnummer

Processen för tilldelning av samordningsnummer går alltså till så att Skatteverket tilldelar samordningsnummer på begäran av någon av de statliga myndigheter som räknas upp i 5 § folkbokföringsförordningen[32] för vissa där angivna ändamål.

För att kunna rekvirera samordningsnummer måste den statliga myndigheten i fråga ha rätt att behandla uppgiften om samordningsnummer, antingen med stöd av en särskild registerförfattning eller med stöd av dataskyddsförordningen.[33] Kommuner och landsting samt andra företag och organisationer än utbildningsanordnare, exempelvis banker eller försäkringsbolag, ingår inte i kretsen som kan begära tilldelning av ett samordningsnummer. Individen har inte heller själv rätt att begära ett samordningsnummer.

Skatteverket samordnar hanteringen av samordningsnummer. Samtliga tilldelade samordningsnummer ingår i folkbokföringsdatabasen. Uppgifter tas inte bort eller gallras. Det ger möjlighet att kontrollera om individen tidigare har tilldelats ett nummer och minskar risken för dubbla identiteter. Innan ett samordningsnummer tilldelas en individ kontrollerar Skatteverket att individen inte genom tidigare bosättning i landet eller av annan anledning har tilldelats personnummer eller samordningsnummer.

Av Skatteverkets meddelande, Skatteverkets information om begäran om tilldelning av samordningsnummer,[34] framgår bl.a. att det måste ställas höga krav på identitetskontrollen vid tilldelning av samordningsnummer. Detta främst med anledning av att en begäran om samordningsnummer kan komma från flera håll och med hänsyn till spridningen av numren i samhället genom SPAR.[35] Under förutsätt-

[31] Prop. 2008/09:111 s. 29 f.
[32] SFS 1991:749.
[33] Innan maj 2018 med stöd av personuppgiftslagen, SFS 1998:204.
[34] SKV M 2010:3.
[35] Statens personadressregister, SPAR, är ett offentligt register som omfattar alla personer som är folkbokförda i Sverige, både svenska och utländska medborgare. I registret ingår även personer som erhållit samordningsnummer och vars identitet är fastställd. Uppgifterna i SPAR uppdateras varje dygn med uppgifter från folkbokföringsregistret. Syftet med SPAR är att lämna ut uppgifter elektroniskt under förutsättning att mottagaren uppfyller vissa villkor.

ning att underlaget är korrekt och fullständigt kommer det inte att finnas mer än ett nummer för individen. Brister i identitetskontrollen kan däremot få till följd att en och samma individ kan få flera samordningsnummer. Det är den rekvirerande statliga myndigheten som har ansvar för att identiteten är kontrollerad. I Skatteverkets meddelande anges vilka uppgifter som krävs för att en individs identitet ska anses vara fastställd och vilka handlingar som ska bifogas. I meddelandet ges också rekommendationer om vad den rekvirerande statliga myndigheten bör beakta vid fastställande av identiteten. Bland annat ska handlingen som ligger till grund för bedömningen visas upp i original eller vidimerad kopia, att denna är utfärdad av en myndighet och innehåller uppgift om en i hemlandet etablerad och registrerad identitet. Handlingen får inte heller vara av alltför enkel beskaffenhet eller lätt att förfalska. Det finns inte något krav på att kontrollen av identiteten ska göras genom ett personligt möte mellan den rekvirerande statliga myndigheten och den som ska tilldelas ett samordningsnummer.

17.5.5 Samordningsnumrens syfte

Samordningsnummer har införts och utvecklats för att myndigheter inom sina respektive verksamheter och sinsemellan ska kunna hantera individer som inte är folkbokförda i Sverige. Myndigheterna behöver veta att det är samma individ som avses oavsett i vilket ärende individen har kontakt med myndigheten. De statliga myndigheter som har rätt att rekvirera samordningsnummer kan också behöva kommunicera med varandra när det gäller dessa individer. Systemet är utformat utifrån de statliga myndigheternas perspektiv och avsikten med samordningsnummer har från början varit att tillgodose de statliga myndigheternas behov, inte individernas.

Det finns därför i dagsläget inte möjlighet för kommuner, landsting, företag eller individer att rekvirera samordningsnummer.

Eftersom det är den rekvirerande statliga myndighetens behov av samordningsnummer som styr tilldelningen är det också den rekvirerande statliga myndigheten som ansvarar för identifieringen av individen. Det är avgörande att identifieringen genomförs med hög kvalitet och att de samordningsnummer som tilldelas, i så hög grad som möjligt, är styrkta. Som systemet är uppbyggt nu måste varje ny aktör

som tillåts rekvirera samordningsnummer också kunna ansvara för identifieringen.

Det har uppmärksammats bl.a. av Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden att samordningsnummer kan användas i bedrägligt syfte. Av utredningens kartläggning framgår t.ex. att flera statliga myndigheter uppmärksammat att falska uppgifter lämnas i syfte att få samordningsnummer som i sin tur kan leda till utbetalningar från välfärdssystemen. [36] Att en individ har tilldelats ett samordningsnummer innebär inte att denne tillförsäkras några rättigheter i sig. Däremot kan det finnas ett behov av samordningsnummer för handläggning av förmåner som ska betalas ut till en individ som inte är folkbokförd i landet men där förutsättningarna för ersättningen i övrigt är uppfyllda.[37]

17.5.6 Automatisering av processen

Utredningen har i uppdrag att analysera hur processen för tilldelning av samordningsnummer till utländska medborgare på distans genom elektronisk identifiering kan möjliggöras och automatiseras. Beroende av hur man ser på begreppet automatisering kan det redan hävdas att processen är automatiserad. Den kan åtminstone skötas elektroniskt i flera delar.

Processen inleds genom kontakt mellan en utländsk användare och en svensk statlig myndighet. Om användaren har ett svenskt personnummer eller styrkt samordningsnummer kan den statliga myndigheten få vetskap om en relation finns sedan tidigare. Om användaren är i färd med att etablera en relation och den statliga myndigheten anser det behövligt kan den statliga myndigheten rekvirera ett samordningsnummer från Skatteverket. Den statliga myndigheten ansvarar då för att identifiera användaren och Skatteverket bedömer om individen kan tilldelas ett styrkt eller ostyrkt samordningsnummer. Som tidigare beskrivits finns det inte något krav på ett personligt möte för identitetskontrollen mellan den rekvirerande statliga myndigheten och den som ska tilldelas ett samordningsnummer. Den

[36] SOU 2017:37 Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra, s. 248.
[37] SOU 2017:37 Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra, s. 293.

statliga myndigheten kan begära in kopior av identitetshandlingar från den enskilda individen och därefter, baserat på elektroniska kontakter och vad som förekommit i övrigt, vara nöjd med identitetskontrollen och rekvirera ett samordningsnummer.

Skatteverket har utvecklat en e-tjänst för att rekvirera samordningsnummer där den rekvirerande statliga myndigheten skickar in rekvisition och uppvisade handlingar elektroniskt till Skatteverket. Vid användningen av e-tjänsten ska en kopia av underlaget som styrkt identiteten skickas in elektroniskt. Stora statliga myndigheter som rekvirerar många samordningsnummer rekommenderas att använda e-tjänsten för att slippa postgång och kunna ge snabbare service.

Den identitetskontroll som beskrivs ovan är inte av den kvalitet som önskas för att samhällsfunktionerna ska kunna lita på att samordningsnummersystemet fungerar som det ska. Det påverkar också folkbokföringens förmåga att upprätthålla god registerkvalitet. Det får till följd att ett styrkt samordningsnummer inte är av samma kvalitet som ett personnummer. Kraven på identitetskontrollen behöver därför snarare skärpas än att processen ska skyndas på genom ökad automatisering.

Om samordningsnummersystemet ska kunna stramas upp i önskad grad och samtidigt hålla ett högre tempo behöver systemet ses över och eventuellt göras om till något annat än vad det är i dag. Detta har uppmärksammats både av regeringen, Skatteverket och övriga rekvirerande statliga myndigheter. Skatteverket har lämnat flera förslag om regelförändringar för att öka registerkvaliteten.[38]

Under sommaren 2017 fick Skatteverket ytterligare ett uppdrag från regeringen för att förbättra kunskapen och informationen om samordningsnummer. I uppdraget ingår också att analysera hur samordningsnummer används i e-tjänster och om det finns behov av informationsinsatser.

När det gäller tilldelning av samordningsnummer ska Skatteverket även utreda om det är lämpligt att ge fler aktörer än för närvarande möjlighet att begära tilldelning av samordningsnummer och i så fall lämna förslag om detta. Som framgår ovan gäller att kommuner, landsting, arbetsgivare, banker och pensionsinstitut inte har möjlighet att

[38] Skatteverkets promemoria Samordningsnummer och utländska fastighetsägare – en översyn från den 18 augusti 2014, dnr. 131 430148-14/113 samt Skatteverkets promemoria Samordningsnummer till asylsökande från den 25 april 2016, dnr. 131 176575-16/113.

begära tilldelning av samordningsnummer enligt dagens regler. Uppdraget omfattar även att utreda om EU- och EES-medborgare själva ska kunna begära samordningsnummer för sin egen del.[39]

17.5.7 Framtida utveckling av person- och samordningsnummer

Det finns vissa problem med person- och samordningsnummersystemen som de är konstruerade i dagsläget.

Ett välkänt bekymmer är att nummerserierna tar slut. Det har redan inträffat när det gäller vissa datum och författningsändringar har genomförts för att kunna medge att individer tilldelas person- eller samordningsnummer som anger ett annat datum än det datum individen faktiskt är född. Folkbokföringsutredningen lämnade 2008 ett delbetänkande[40] där det bedömdes att det var nödvändigt att ändra personnumrets konstruktion för att komma till rätta med bristen på tillgängliga personnummer. Utredningen gick igenom ett antal tänkbara alternativ för hur konstruktionen skulle kunna ändras.

På grund av de stora kostnader en sådan förändring väntades medföra valde regeringen i stället en förändring som innebär att i de fall det saknas födelsenummer för en viss födelsetid får dagen i födelsetiden i stället anges med en födelsedagen närliggande dag i samma månad.[41] Den valda lösningen innebar i viss mån att skjuta problemen framåt eftersom nummerserierna tar slut även på närliggande datum.

Ett annat problem handlar om att person- och samordningsnumren är värdebärande. Numren innehåller information om individen i fråga. Ålder, födelsedatum, kön och i vissa fall var individen är född går att utläsa av person- och samordningsnummer. Det kan finnas integritetsskäl för att i stället använda ett nummersystem som är neutralt i dessa avseenden. En aspekt av detta har nyligen beskrivits av Utredningen om stärkt ställning och bättre levnadsvillkor för transpersoner. Utredaren föreslår bl.a. att regeringen ska tillsätta en ut-

[39] Regeringens och finansdepartementets uppdrag till Skatteverket för att tillgodose kraven på fri rörlighet för medborgare i Europeiska unionen och Europeiska ekonomiska samarbetsområdet från den 6 juli 2017, dnr. Fi2017/02960/S3.
[40] SOU 2008:60, Personnummer och samordningsnummer.
[41] Prop. 2008/09:111, s. 25.

redning i syfte att utreda möjligheten till ett tredje juridiskt kön i Sverige samt därmed ett införande av könsneutrala personnummer.[42]

Person- och samordningsnummersystemen är en grundbult i det svenska samhället och används av en mängd aktörer i olika syften och sammanhang. Kostnaderna för att ändra konstruktionen av numren eller införa nya system är svåröverskådliga och mycket stora. Bara Skatteverkets kostnader beräknades beroende på vilket alternativ som valdes uppgå till 450 miljoner kronor. Andra stora statliga myndigheter med liknande ärendehantering skulle ha lika stora kostnader.[43] Dessa kostnader beräknades då på ett förhållandevis snabbt genomförande. Det handlade om några års tid.

Utredningen konstaterar att frågan om brister i person- och samordningsnummersystemen inte ligger inom utredningens mandat. Det handlar samtidigt om problem som återkommande har visat sig under utredningstiden och som lyfts av flera inblandade statliga myndigheter. Utredningen vill därför i sammanhanget belysa frågan och peka på möjligheten att genomföra en systemförändring på annat sätt än den som tidigare utretts. I Norge arbetar man för närvarande med en liknande systemförändring där man använder en tidsperiod om 20–25 år för att successivt och stegvis kunna ställa om och dessutom få en spridning på kostnaderna så att de ska bli mer hanterliga.

17.6 Rättsliga konsekvenser och kompletterande författning om den svenska offentliga noden

Utredningen föreslår:
att det ska ingå i det offentliga åtagandet att Sverige tillhandahåller en offentlig nod för gränsöverskridande identifiering i enlighet med eIDAS-förordningens krav.
att kompletterande författning om den svenska noden ska införas i lagen (2016:561) och förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

[42] SOU 2017:92, Transpersoner i Sverige, Förslag för stärkt ställning och bättre levnadsvillkor, s. 488 ff.
[43] Prop. 2008/09:111, s. 20.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Av eIDAS-förordningen följer vissa givna utgångspunkter. Sverige måste se till att det finns minst en nod som kan ta emot och dirigera vidare begäran om bekräftelse av identitet när det gäller utländska användares elektroniska identitetshandlingar. Det finns inget i förordningstexten som hindrar förekomst av flera sådana noder i Sverige. Behovet av eventuella ytterligare noder kan diskuteras men först och främst behöver Sverige se till att det åtminstone finns en officiell nod för detta ändamål.

Behovet av en nod finns också när det gäller användning av svenska elektroniska identitetshandlingar i utländska e-tjänster. Det följer av förordningstexten att varje medlemsstat ska tillhandahålla endast en nod för detta ändamål.

E-legitimationsnämnden fick den 23 mars 2016 i uppdrag av regeringen att påbörja arbetet med att utveckla en nod för användning enligt eIDAS-förordningens bestämmelser.[44] Den nod som i skrivande stund är under uppbyggnad ska klara att sköta flöden av elektroniska identitetshandlingar både när det gäller de europeiska där användaren vill nyttja en svensk e-tjänst och de svenska där användaren vill nyttja en e-tjänst i ett annat medlemsland.

För att se till att Sverige uppfyller eIDAS-förordningens krav när det gäller att tillhandahålla en nod och samtidigt tydliggöra ansvarsfördelningen för noden föreslår utredningen kompletterande författning om den svenska noden. Det finns redan en lag[45] och en förordning[46] med kompletterande bestämmelser till eIDAS-förordningen som kan utökas med de ytterligare regler som behövs.

[44] Uppdrag att utveckla central teknisk arkitektur för hantering av europeiska e-legitimationer enligt eIDAS-förordningen, N2016/02305/EF.
[45] Lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.
[46] Förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

17.6.1 Digitaliseringsmyndigheten ansvarar för den svenska offentliga noden

Utredningen föreslår:
att digitaliseringsmyndigheten ska ansvara för den svenska offentliga noden.
att regeringen eller, efter regeringens bemyndigande, digitaliseringsmyndigheten får meddela föreskrifter om noden.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering samt förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Hittills har regeringen tilldelat ansvaret för uppbyggnaden av noden till E-legitimationsnämnden genom tidsbegränsade uppdrag. För att få kontinuitet i arbetet med noden och förutsebarhet i var ansvaret för noden ska ligga föreslår utredningen en regel om att regeringen ska utse en myndighet som ska ansvara för att tillhandahålla en nod för de ändamål som eIDAS-förordningen kräver. Utredningen föreslår att regeringen i förordningen med kompletterande bestämmelser till eIDAS-förordningen utser digitaliseringsmyndigheten till nodmyndighet.

E-legitimationsnämnden, vars verksamhet ska ingå i digitaliseringsmyndigheten, kommer att driva arbetet med noden fram till dess att digitaliseringsmyndigheten inleder sin verksamhet.

Utredningen föreslår även att regeringen eller, efter regeringens bemyndigande, nodmyndigheten, det vill säga digitaliseringsmyndigheten, får meddela föreskrifter om noden.

17.6.2 Digitaliseringsmyndigheten är personuppgiftsansvarig för behandlingar av personuppgifter i noden

Utredningen föreslår:
att digitaliseringsmyndigheten ska vara personuppgiftsansvarig för behandlingar av personuppgifter i noden.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Från och med den 25 maj 2018 kommer den nya dataskyddsförordningen[47] att gälla i EU:s medlemsstater vilket innebär att dataskyddsförordningens regler är grunden för all behandling av personuppgifter i Sverige. I förslag om personuppgiftshantering och personuppgiftsansvar måste därför alla bedömningar göras gentemot detta regelverk.

Dataskyddsförordningen förutsätter att varje behandling av personuppgifter ska utgå från en rättslig grund. Personuppgifter får därför bara behandlas under de omständigheter som särskilt anges i förordningen. I dataskyddsförordningen räknas dessa rättsliga grunder upp i artikel 6.1. Behandling är enligt denna bestämmelse endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

[47] Europaparlamentet och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

f) Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Uppräkningen i artikel 6.1 är uttömmande. Om inget av dessa villkor är uppfyllda är behandlingen inte laglig och får därmed inte utföras. De olika villkoren är i viss mån överlappande. Flera rättsliga grunder kan därför vara tillämpliga avseende en och samma behandling.

Den personuppgiftsansvarige måste också uppfylla kraven i övriga bestämmelser i förordningen, t.ex. de allmänna principerna i artikel 5. Principerna lyder:

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet).

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).

c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).

d) De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (korrekthet).

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskap-

liga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (lagringsminimering).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

Den personuppgiftsansvarige ska enligt artikel 5.2 även ansvara för och kunna visa att principerna efterlevs (ansvarsskyldighet).

Artiklarna 5 och 6 i dataskyddsförordningen är grundläggande och kumulativa. Dels måste någon av de rättsliga grunder som anges i artikel 6.1 vara tillämplig, dels måste samtliga principer i artikel 5.1 följas. Det är endast om någon av de rättsliga grunder som anges i artikel 6.1 är tillämplig som behandling av personuppgifter över huvud taget får utföras. Om behandlingen är laglig enligt artikel 6 ska kraven i artikel 5 uppfyllas.[48]

I dataskyddsförordningens artikel 4.7 definieras personuppgiftsansvarig: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

[48] SOU 2017:39, Ny dataskyddslag Kompletterande bestämmelser till EU:s dataskyddsförordning, s. 108.

Rättslig grund

Regler om noder finns i kommissionens genomförandeförordning om interoperabilitetsramverket enligt eIDAS-förordningen.[49] Interoperabilitet mellan medlemsstaterna är en förutsättning för att gränsöverskridande elektronisk identifiering ska kunna genomföras. I genomförandeförordningen sägs bland annat i artikel 6.2 att noderna inte får lagra några personuppgifter, utom för det ändamål som anges i artikel 9.3. Ändamålet i artikel 9.3 gäller att uppgifter ska lagras för att kunna rekonstruera ordningsföljden av händelser vid incidenter.

Sverige har skyldighet enligt artikel 6 i eIDAS-förordningen att under vissa förhållanden erkänna utländska elektroniska identitetshandlingar. För att kunna göra det krävs att det finns minst en nod som förmedlar uppgifter enligt vad som tidigare har beskrivits i avsnitt 17.1. Utredningen bedömer därför att personuppgiftsbehandlingen i noden är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Därmed uppfylls villkoret i artikel 6.1 c i dataskyddsförordningen.

Det kan också hävdas att villkoret i artikel 6.1 e är uppfyllt eftersom behandlingen kan ses som nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Enligt Dataskyddsutredningen är statliga och kommunala myndigheters verksamhet i allt väsentligt av allmänt intresse. Det är därmed den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som vanligen bör tillämpas av myndigheter, även utanför området för myndighetsutövning. De offentliga myndigheternas uppdrag och skyldigheter framgår av författningar, regeringsbeslut och kommunala reglementen, antagna i enlighet med grundlagens bestämmelser om normgivningskompetens och kommunalt självstyre. De åtgärder som de offentliga myndigheterna vidtar i syfte att utföra dessa uppdrag eller uppfylla dessa skyldigheter har därmed i sig en legal grund, som har offentliggjorts genom tydliga, precisa och förutsebara regler. Nödvän-

[49] Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

dig behandling av personuppgifter kan därmed göras med stöd av artikel 6.1 e i dataskyddsförordningen.[50]

Proportionalitet

Enligt dataskyddsförordningens artikel 6.3 ska den grund för behandlingen som avses i punkt 1 c och e fastställas i enlighet med unionsrätten, eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Enligt andra stycket sista meningen ska unionsrätten eller medlemsstaternas nationella rätt uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas.

Det innebär att en proportionalitetsbedömning måste göras av den kompletterande lagstiftning som föreslås för att se till att de legitima mål som eftersträvas genom aktuella behandlingar av personuppgifter står i proportion till det intrång i integriteten som behandlingen innebär. Endast då kan behandlingen tillåtas.

Enligt eIDAS-förordningens krav har Sverige skyldighet att under vissa i förordningen beskrivna förhållanden erkänna utländska elektroniska identitetshandlingar i svenska e-tjänster. För att kunna göra det krävs att det i Sverige finns en nod som klarar av att dirigera trafiken av inkommande elektroniska identitetshandlingar för att kunna bekräfta identiteten på de användare som vill ha tillträde till svenska e-tjänster. Det kräver i sin tur den föreslagna behandlingen av de personuppgifter som anges i kommissionens genomförandeförordning (EU) 2015/1501.

Det är användaren själv som initierar identifieringsprocessen. Även om inte alla användare känner till exakt vad som händer när de använder elektroniska identitetshandlingar får det förutsättas att användaren förstår att någon form av behandling av personuppgifter kommer att behövas. Avsikten är att den föreslagna lagstiftningen ska tillåta minsta möjliga personuppgiftsbehandling för att ändå lösa uppgiften att dirigera den information som behövs för att kunna identifiera användaren. Utredningen bedömer att detta måste anses stå i proportion till det eventuella intrång i integriteten som användaren kan uppleva.

[50] SOU 2017:39, Ny dataskyddslag Kompletterande bestämmelser till EU:s dataskyddsförordning, s. 128 f.

Ändamål och allmänna principer

Den personuppgiftsansvariga offentliga myndigheten ska även kunna visa att principerna i artikel 5 efterlevs.

Ändamålet med nodens personuppgiftsbehandling är att användare som vill ha tillträde till svenska e-tjänster ska kunna identifieras. Identitetskontrollen utförs av den offentliga myndighet som tillhandahåller e-tjänsten men noden behöver behandla uppgifter genom att dirigera dem till rätt aktör innan identitetskontrollen kan genomföras.

Uppgifterna måste vidare behandlas på ett lagligt och korrekt sätt genom att nodmyndigheten följer bestämmelserna i eIDAS-förordningen och dess genomförandeakter om hur noden ska byggas upp och fungera.

När det gäller öppenhet kan det diskuteras om förfarandet för inloggning med elektroniska identitetshandlingar är tillräckligt öppet i förhållande till användaren. Det är viktigt att användaren informeras om vad som händer och vilken aktör som är ansvarig i olika skeden av inloggningsförfarandet.

Personuppgifterna är minimerade enligt kommissionens genomförandeförordning (EU) 2015/1501. Inga personuppgifter utöver de som anges där får behandlas av noden. I bilagan till genomförandeförordningen anges att en minimiuppsättning av uppgifter för en fysisk person ska innehålla följande obligatoriska attribut: nuvarande efternamn, nuvarande förnamn, födelsedatum samt en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständig i tid. En minimiuppsättning för en fysisk person kan dessutom innehålla ett eller flera av följande ytterligare attribut: förnamn och efternamn vid födseln, födelseort, nuvarande adress och kön.

Nodmyndigheten måste se till att personuppgifterna som behandlas hålls korrekta och att säkerheten upprätthålls för att skydda integritet och konfidentialitet.

Enligt artikel 6.2 i kommissionens genomförandeförordning (EU) 2015/1501 får noderna inte lagra några personuppgifter utom för att det vid en incident ska gå att rekonstruera ordningsföljden i det som har hänt för att fastställa platsen för incidenten och dess art.

Regeringen eller, efter regeringens bemyndigande, nodmyndigheten får enligt utredningens förslag meddela föreskrifter om noden.

Det kan komma att visa sig att ytterligare föreskrifter krävs för att nodmyndigheten ska kunna visa att de ovanstående principerna uppfylls.

Vad säger de andra medlemsstaterna?

De medlemsstater som besvarade utredningens enkät som beskrivits i avsnitt 17.3.4 svarade också på frågan om de upptäckt några tänkbara konflikter mellan dataskyddsförordningen och eIDAS-förordningen.

Ingen av de svarande hade identifierat någon sådan konflikt men uttryckte tydligt intresse av att få veta om Sverige gjort det.

De förutsätter att medlemsstaterna ska leva upp till sina skyldigheter enligt dataskyddsförordningen när det gäller behandlingen av personuppgifter för att möta eIDAS-förordningens krav.

Finland bedömer att dataskyddsförordningens krav kan komma att begränsa deras lösningar medan Österrike anser att eIDAS-förordningen i sig ger laglig rätt att behandla åtminstone minimiuppsättningen av uppgifter och valfria tilläggsdata från varje medlemsstat.

17.6.3 Alla offentliga myndigheter som omfattas av eIDAS-förordningens krav ska ansluta till noden

Utredningen föreslår:
att alla statliga myndigheter, kommuner och landsting som har e-tjänster där det krävs elektronisk identifiering på tillitsnivå väsentlig eller hög för att få tillträde ska ansluta till den svenska offentliga noden.
att övriga statliga myndigheter, kommuner och landsting får ansluta till den svenska offentliga noden.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

De offentliga myndigheter som omfattas av eIDAS-förordningens krav när det gäller erkännande av utländska elektroniska identitetshandlingar kommer att behöva ansluta sig till noden. Därför föreslår

utredningen att alla offentliga myndigheter som, för att ge åtkomst till sina e-tjänster, omfattas av kraven på elektronisk identifiering enligt eIDAS-förordningen, ska ansluta till den svenska offentliga noden. Kravet att ansluta till noden gäller alltså de offentliga myndigheter som i dag kräver elektronisk identifiering på tillitsnivå väsentlig eller hög för att ge användare tillträde till någon av sina e-tjänster.

Offentliga myndigheter som inte omfattas av förordningens krav får enligt förslaget också ansluta till den svenska offentliga noden men det är på frivillig basis. Detta gäller alltså offentliga myndigheter som inte kräver elektronisk identifiering på tillitsnivå väsentlig eller hög för att logga in användare i någon e-tjänst utan där det räcker med en lägre tillitsnivå. Även dessa offentliga myndigheter kan ha intresse av att identifiera utländska användare elektroniskt för att ge tillträde och ges på detta sättet möjlighet att använda noden.

17.6.4 Övriga aktörer får ansluta till noden

Utredningen föreslår:
att privata aktörer får ansluta till den svenska offentliga noden.
att regeringen eller, efter regeringens bemyndigande, digitaliseringsmyndigheten får meddela föreskrifter om skyldighet för privata aktörer att betala avgift för att ansluta till noden.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Under utredningstiden har det framkommit att aktörer i privat sektor också har intresse av att kunna ansluta till noden och på så sätt hantera utländska användare i sina e-tjänster. Därför föreslår utredningen att även privata aktörer får ansluta till den svenska offentliga noden.

Noden kommer att finansieras med offentliga medel. Den byggs upp för att i första hand tillgodose ett behov inom offentlig sektor. Inledningsvis förväntas trafiken genom noden inte bli särskilt omfattande, varken av offentliga eller privata aktörer. Utvecklingen kan dock gå snabbt, särskilt inom den privata sektorn. Det kan därför på sikt komma att bli aktuellt att ta ut avgifter från privata aktörer för att de ska kunna utnyttja noden. Utredningen föreslår därför att

regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om skyldighet för privata aktörer att betala avgift för att ansluta till noden.

17.6.5 Incidentrapportering

Utredningen föreslår:
att alla aktörer som är anslutna till noden utan otillbörligt dröjsmål ska underrätta digitaliseringsmyndigheten om alla händelser som påverkat funktionalitet och säkerhet i noden.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

För att noden ska fungera på bästa möjliga sätt krävs det enligt utredningens mening att de inblandade aktörerna bidrar och tar ansvar för det de kan i förhållande till sina respektive roller. Ett sätt att praktiskt upprätthålla säkerhetsnivån är att informera nodmyndigheten om alla incidenter som på något sätt påverkar säkerhet eller funktionalitet av noden. Utredningen föreslår därför att alla som är anslutna till noden utan otillbörligt dröjsmål ska underrätta nodmyndigheten om alla händelser som påverkat funktionalitet eller säkerhet i noden.

17.6.6 Försvarets radioanstalt ska utföra tekniska säkerhetsgranskningar

Utredningen föreslår:
att regeringen ger Försvarets radioanstalt i uppdrag att utföra en teknisk säkerhetsgranskning av det system som den svenska noden omfattar innan det sätts i drift.
att digitaliseringsmyndigheten vid större förändringar av det system som den svenska noden omfattar, ska begära en teknisk säkerhetsgranskning av Försvarets radioanstalt. Granskningsförfarandet får ta max tre månader från det att digitaliseringsmyndigheten ansökt om granskning.

Förslaget genomförs genom förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Noden är en viktig del i infrastrukturen för elektronisk identifiering och det är därför viktigt att den skyddas mot användning på ett bedrägligt sätt. Noden ses inte som samhällsviktig enligt det s.k. NIS-direktivet[51] bilaga II, men konsekvenserna av eventuella angrepp kan bli allvarliga.

För att skydda noden mot angrepp föreslår utredningen ett granskningsförfarande av en it-säkerhetsexpertmyndighet, Försvarets radioanstalt, FRA. Den första granskningen ska genomföras innan systemet sätts i drift och kan initieras direkt av regeringen eftersom digitaliseringsmyndigheten inte kommer att ha tagit över uppgifterna från E-legitimationsnämnden innan en sådan granskning behöver begäras. E-legitimationsnämnden bör även under processen med att ta fram noden under våren 2018 involvera FRA för att processen ska bli så smidig som möjligt. Vid större förändringar av det system som den svenska noden omfattar ska digitaliseringsmyndigheten därefter begära att FRA utför en sådan teknisk säkerhetsgranskning.

Utredningen föreslår även att FRA ska ha tre månader på sig att utföra sin granskning efter digitaliseringsmyndighetens begäran.

17.6.7 Noden utöver eIDAS-förordningen

Utredningen föreslår:
att digitaliseringsmyndigheten ska ha rätt att behandla tekniska uppgifter för de aktörer vars uppgifter ska behandlas av noden.
att digitaliseringsmyndigheten ska få behandla de personuppgifter som är nödvändiga för att säkerställa behörigheter för aktörernas ombud.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

[51] Europaparlamentet och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

När det gäller den svenska noden har utredningen utgått från den definition som ges i eIDAS-förordningen. I eIDAS-förordningen regleras det som händer mellan den svenska noden och de utländska noderna. Den nationella delen av noden är vidare än denna definition. Det medför att inte allt som det är tänkt att nodmyndigheten ska utföra täcks av den reglering som utredningen föreslår.

E-legitimationsnämnden arbetar parallellt med utredningen med att ta fram specifikationer för och bygga upp ett s.k. metadataregister. I metadataregistret kommer att lagras t.ex. tekniska uppgifter för de aktörer vars uppgifter ska behandlas av noden och även personuppgifter som är nödvändiga för att säkerställa behörighet för aktörernas ombud. Metadataregistret kommer att behöva finnas på plats när noden ska tas i bruk. I skrivande stund är det dock inte helt klart hur det kommer att fungera, vad som kommer att omfattas av det och hur det behöver regleras. Utredningen föreslår dock redan nu en regel som ger nodmyndigheten rätt att behandla tekniska uppgifter för de aktörer vars uppgifter ska behandlas av noden. Nodmyndigheten ska även få behandla de personuppgifter som är nödvändiga för att säkerställa behörigheter för aktörernas ombud.

17.6.8 Ikraftträdande

Utredningen föreslår:
att de föreslagna kompletterande reglerna till EU:s förordning om elektronisk identifiering (eIDAS-förordningen) träder i kraft den 29 september 2018.

Från och med den 29 september 2018 kommer svenska offentliga myndigheter som har e-tjänster som kräver identifiering med elektroniska identitetshandlingar att ha skyldighet att erkänna europeiska elektroniska identitetshandlingar i sina e-tjänster. Därför behöver den föreslagna kompletterande regleringen till eIDAS-förordningen också gälla från samma tidpunkt.

18 Anmälan av svenska elektroniska identitetshandlingar

18.1 Beskrivning av processen

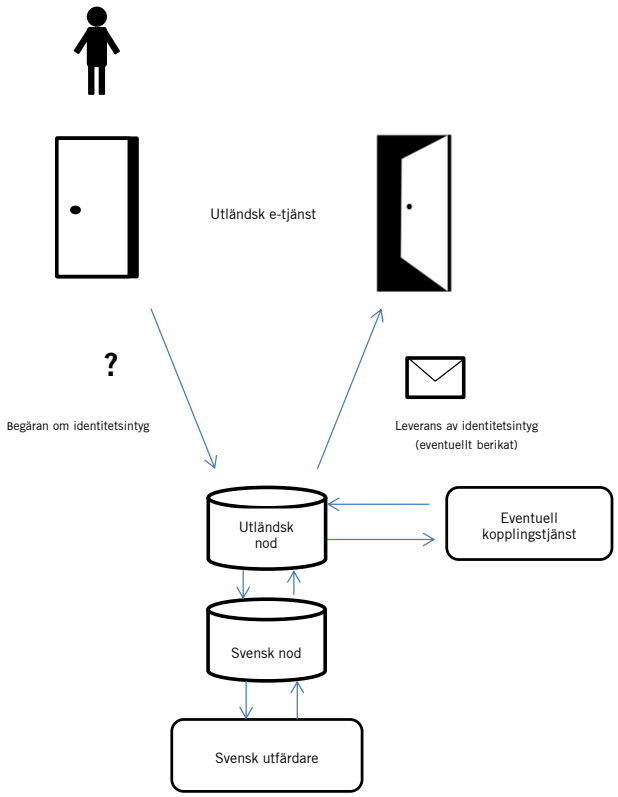
På samma sätt som beskrivits ovan när det gäller utländska användare som ska identifiera sig i svenska e-tjänster kommer det också att fungera för svenska användare som ska identifiera sig i utländska e-tjänster. Nedan följer en förenklad beskrivning av vad som händer när en användare med svensk elektronisk identitetshandling identifierar sig i en utländsk e-tjänst.

Användaren med svensk elektronisk identitetshandling får ange att hon eller han vill identifiera sig med en svensk elektronisk identitetshandling. Begäran om identitetsintyg skickas via den utländska noden som dirigerar begäran vidare till den svenska noden. Den svenska noden skickar begäran om identitetsintyg till den utfärdare som har utfärdat den elektroniska identitetshandlingen i Sverige. Identitetsintyget ska innehålla användarens nuvarande förnamn, nuvarande efternamn, födelsedatum och landets unika identitetsbeteckning. Det kan också innehålla några ytterligare attribut som Sverige behöver ta ställning till om de ska skickas med eller inte. Identitetsintyget levereras tillbaka från utfärdaren via den svenska noden till den utländska noden.

I vissa medlemsstater kommer det att finnas en motsvarighet till förslaget om det svenska kopplingsregistret. Identitetsintyget kan komma att berikas med användarens eventuella utländska identitetsbeteckning innan det levereras till e-tjänsten. Detta kan utformas på olika sätt i olika medlemsstater. Liksom i Sverige kan det även i andra medlemsstater vara avgörande att användaren har en nationell identitetsbeteckning för att få tillgång till offentliga myndigheters e-tjänster. I figuren nedan är det den utländska noden som gör en slagning mot ett eventuellt kopplingsregister men denna funktion kan

vara utformad på flera andra sätt. Uppgifterna om koppling kan vara integrerade med folkbokföringen och det kan vara e-tjänstmyndigheten som gör slagningen.

Figur 18.1 Individ identifierar sig i utländsk e-tjänst med svensk elektronisk identitetshandling



18.1.1 Processuella frågor

Anmälan

För att en elektronisk identitetshandling ska kunna anmälas för gränsöverskridande identifiering enligt eIDAS-förordningen måste samtliga villkor i artikel 7 vara uppfyllda. Det innebär följande:

a) Medlet för elektronisk identifiering inom ramen för systemet för elektronisk identifiering ska vara utfärdat

i) av den anmälande medlemsstaten,

ii) på uppdrag av den anmälande medlemsstaten, eller

iii) oberoende av den anmälande medlemsstaten och erkännas av den medlemsstaten.

b) Medlet för elektronisk identifiering inom systemet för elektronisk identifiering ska kunna användas för att få åtkomst till åtminstone en tjänst som tillhandahålls av ett offentligt organ och som kräver elektronisk identifiering i den anmälande medlemsstaten.

c) Systemet för elektronisk identifiering och det medel för elektronisk identifiering som utfärdats inom ramen för det ska uppfylla kraven för åtminstone en av de tillitsnivåer som anges i den genomförandeakt som avses i artikel 8.3.

d) Den anmälande medlemsstaten ska se till att de personidentifieringsuppgifter som unikt representerar personen i fråga, i enlighet med de tekniska specifikationer, standarder och förfaranden för den relevanta tillitsnivå som anges i den genomförandeakt som avses i artikel 8.3, tillskrivs den fysiska eller juridiska person som avses i artikel 3.1 vid tidpunkten för utfärdandet av medlet för elektronisk identifiering inom detta system.

e) Den part som utfärdar medlet för elektronisk identifiering inom detta system ska se till att medlet för elektronisk identifiering tilldelas den person som avses i led d i denna artikel i enlighet med de tekniska specifikationer, standarder och förfaranden för den relevanta tillitsnivå som anges i den genomförandeakt som avses i artikel 8.3.

f) Den anmälande medlemsstaten ska se till att autentisering är tillgänglig via internet så att alla förlitande parter som är etablerade på någon annan medlemsstats territorium kan bekräfta de personidentifieringsuppgifter som tas emot i elektronisk form.

För andra förlitande parter än offentliga organ får den anmälande medlemsstaten fastställa tillträdesvillkoren för autentiseringen. Så-

dan gränsöverskridande autentisering ska tillhandahållas kostnadsfritt när den utförs i samband med en nättjänst som tillhandahålls av ett offentligt organ.

Medlemsstaterna får inte ålägga förlitande parter som har för avsikt att utföra en sådan autentisering oproportionella tekniska krav om sådana krav skulle hindra eller avsevärt försvåra kompatibiliteten mellan anmälda system för elektronisk identifiering.

g) Minst sex månader före anmälan enligt artikel 9.1 ska den anmälande medlemsstaten när det gäller den skyldighet som anges i artikel 12.5 förse andra medlemsstater med en beskrivning av detta system i enlighet med de förfaranden som fastställts genom de genomförandeakter som avses i artikel 12.7.

h) System för elektronisk identifiering ska uppfylla kraven i den genomförandeakt som avses i artikel 12.8.1

Anmälan av privata utfärdare av elektroniska identitetshandlingar är alltså tillåtet om den elektroniska identitetshandlingen är godkänd i den anmälande medlemsstaten. Den elektroniska identitetshandlingen ska kunna användas för att få åtkomst till åtminstone en e-tjänst som tillhandahålls av en myndighet och som kräver elektronisk identifiering i den anmälande medlemsstaten.

Av artikel 9 i eIDAS-förordningen framgår hur anmälan av elektroniska identitetshandlingar ska gå till. Det är medlemsstaten som anmäler elektroniska identitetshandlingar för gränsöverskridande identifiering enligt eIDAS-förordningens sytem. I artikel 9.1 finns en lista av vad anmälan ska innehålla. Det framgår också att den anmälande medlemsstaten utan onödigt dröjsmål ska anmäla eventuella ändringar av uppgifterna.

Anmälan ska innehålla:

a) En beskrivning av systemet för elektronisk identifiering, inbegripet dess tillitsnivåer och av utfärdaren eller utfärdarna av medel för elektronisk identifiering inom systemet.

[1] Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentet och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

b) Det tillämpliga systemet för tillsyn och information om systemet för skadeståndsansvar med avseende på följande:

   i) Den part som utfärdar medlet för elektronisk identifiering.

   ii) Den part som handhar autentiseringsförfarandet.

c) Den myndighet eller de myndigheter som ansvarar för systemet för elektronisk identifiering.

d) Information om den enhet eller de enheter som hanterar registreringen av de unika personidentifieringsuppgifterna.

e) En beskrivning av hur kraven i den genomförandeakt som avses i artikel 12.82 har uppfyllts. Dessa krav innefattar i synnerhet tekniska minimikrav om tillitsnivåer och kartläggning av nationella tillitsnivåer för anmälda elektroniska identitetshandlingar, tekniska minimikrav på interoperabilitet, minimiuppsättningen av personidentifieringsuppgifter, gemensamma standarder för operativ säkerhet och bestämmelser för tvistlösning.

f) En beskrivning av den autentisering som avses i artikel 7 f (se beskrivning ovan).

g) System för tillfälligt upphävande eller återkallelse av det anmälda systemet för elektronisk identifiering eller autentisering eller av de berörda utsatta delarna.

Kommissionen ska enligt artikel 9.2 offentliggöra en förteckning över de elektroniska identitetshandlingar som har anmälts i Europeiska unionens officiella tidning.

Processen för anmälan ses inte som särskilt svår eller komplicerad. Det är väl beskrivet i förordningstext och genomförandeakter vad som behövs för att göra en anmälan. Dessutom har Tyskland anmält två elektroniska identitetshandlingar så det finns redan erfarenhet av hur det går till. Svenska representanter från E-legitimationsnämndens kansli har deltagit i arbetet med att granska Tysklands anmälda elektroniska identitetshandlingar och kunnat följa processen på nära håll.

[2] Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentet och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

Avanmälan

Processen för avanmälan finns också beskriven i förordningstext och genomförandeakter men den har ännu inte prövats av någon medlemsstat. Enligt artikel 9.4 i eIDAS-förordningen får en medlemsstat lämna in en begäran till kommissionen om att ta bort ett system för elektronisk identifiering som anmälts av medlemsstaten från förteckningen i Europeiska unionens officiella tidning. Kommissionen ska offentliggöra motsvarande ändringar i förteckningen i Europeiska unionens officiella tidning inom en månad från den dag då medlemsstatens begäran mottogs.

I artikel 2.2.3 i bilagan till genomförandeförordning 2015/1502[3] finns ytterligare bestämmelser om avanmälan av elektroniska identitetshandlingar. Där står att det är möjligt att avbryta och/eller återkalla ett medel för elektronisk identifiering i god tid och på ett verksamt sätt. Det ska finnas åtgärder för att förhindra att upphävande, återkallelse och/eller reaktivering utförs på otillåtet sätt. Återaktivering ska utföras endast om samma krav angående tilliten som fastställts före upphävandet eller återkallelsen fortsätter att uppfyllas.

18.2 Sverige ska anmäla elektroniska identitetshandlingar

Utredningen föreslår:
att Sverige som en del av det offentliga åtagandet ska anmäla elektroniska identitetshandlingar för gränsöverskridande identifiering enligt eIDAS-förordningen.

I skäl (2) till eIDAS-förordningen anges att syftet med förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndig-

[3] Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

heter, och därigenom öka effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen.

För att svenska användare ska kunna ta del av detta syfte och ta tillvara eIDAS-förordningens nytta och potential behöver Sverige se till att medborgare och folkbokförda har möjlighet att använda e-tjänster i andra medlemsstater genom gränsöverskridande identifiering. Därför behöver det ingå i det offentliga åtagandet att det i Sverige finns minst en elektronisk identitetshandling som kan användas för detta ändamål.

Det finns privata aktörer på den svenska marknaden som har uttryckt intresse för att utveckla elektroniska identitetshandlingar för gränsöverskridande identifiering enligt eIDAS-förordningen. Utredningen anser dessutom att det finns goda skäl för staten att låta det ingå i det offentliga åtagandet tillsammans med åtagandet att tillhandahålla statliga elektroniska identitetshandlingar för användning inom landet[4] att samtidigt erbjuda dessa även för gränsöverskridande identifiering. Jämförelse kan här göras med det offentliga åtagandet att utfärda pass för utrikes resor. Behovet av att kunna kommunicera med utländska myndigheter kan likställas med detta.

18.2.1 Behov av elektronisk identitetshandling i utländska e-tjänster

Utredningen bedömer:
att det finns behov av minst en svensk elektronisk identitetshandling för gränsöverskridande identifiering enligt eIDAS-förordningen.

Under utredningens arbete har det i flera sammanhang lyfts att användare av svenska elektroniska identitetshandlingar behöver använda dessa även i e-tjänster i Europa. Det följande är ingen uttömmande lista över de behov som finns men det visar att behovsbilden är stor och diversifierad.

[4] Se avsnitt 12.7.5.

- Studenter som studerar eller avser studera utomlands kan komma att behöva tillträde till e-tjänster i studielandet.
- Patienter som behöver vård utomlands.
- Företagare som vill etablera sig i en annan medlemsstat.
- Pensionärer som bor utomlands.
- Arbetssökande i andra medlemsstater.
- Boende i gränstrakter till andra länder och vill kunna nyttja e-tjänster på båda sidorna gränsen.
- Resenärer som tillfälligt befinner sig i andra medlemsstater och upptäcker att de behöver använda e-tjänster där.
- Individer som står inför att flytta utomlands.
- Skattskyldiga i andra medlemsstater.

Utredningens uppfattning är att det finns behov av en svensk elektronisk identitetshandling för gränsöverskridande identifiering enligt eIDAS-förordningen.

18.2.2 Risker med anmälan

Utredningen bedömer:
att det finns både rättsliga och ekonomiska risker med att anmäla elektroniska identitetshandlingar, framför allt om de är utfärdade av en privat aktör.
att staten behöver ha största möjliga kontroll över de elektroniska identitetshandlingar som anmäls för gränsöverskridande identifiering enligt eIDAS-förordningen.
att skadeståndsansvarets fördelning måste regleras tydligt i avtal mellan staten och privata utfärdare. Avtalet bör också innehålla uppgift om regress av skadeståndsanspråk för de fall skador uppkommer senare i processen.
att ansvaret vid säkerhetsincidenter måste regleras tydligt mellan staten och privata utfärdare i avtal så att staten kan ges förutsättningar att ta det ansvar som eIDAS-förordningen kräver.

Det är den anmälande medlemsstaten som går i god för de anmälda elektroniska identitetshandlingarna. Det innebär att staten får svara för eventuella säkerhetsincidenter och skador även när det är en privat utfärdare som står för den elektroniska identitetshandlingen. Det är staten som är part i medlemsstaternas granskningsförfarande av anmälda elektroniska identitetshandlingar och det är staten som måste upphäva eller återkalla en elektronisk identitetshandling som har utsatts för intrång eller äventyras på ett sätt som påverkar tillförlitligheten enligt artikel 10.1. Detta talar för att staten behöver ha största möjliga kontroll över de elektroniska identitetshandlingar som anmäls enligt eIDAS-förordningen.

Rättsliga risker

Skadeståndsansvaret behandlas i artikel 11 i eIDAS-förordningen. Enligt artikel 11.1 ska den anmälande medlemsstaten ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom dess underlåtenhet att uppfylla sina skyldigheter enligt artikel 7 d och f vid en gränsöverskridande transaktion.[5]

Utfärdaren har enligt artikel 11.2 skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla den skyldighet som avses i artikel 7 e vid en gränsöverskridande transaktion.[6]

Den part som handhar autentiseringsförfarandet (här avses både nodmyndigheten och utfärdaren av den elektroniska identitetshandlingen i sina respektive delar av autentiseringen) har enligt artikel 11.3 skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att säkerställa korrekt handhavande av den autentisering som avses i artikel 7 f vid en gränsöverskridande transaktion.

Därefter hänvisar eIDAS-förordningen till nationella regler om skadeståndsansvar.

[5] Artikel 7 d gäller den anmälande medlemsstatens skyldighet att se till att unika personidentifieringsuppgifter tillskrivs rätt person vid tidpunkten för utfärdandet av den elektroniska identitetshandlingen. Artikel 7 f gäller den anmälande medlemsstatens skyldighet att se till att autentisering är tillgänglig via internet.

[6] Artikel 7 e gäller att utfärdaren ska se till att den elektroniska identitetshandlingen tilldelas den person som avses i led d.

Av skadeståndsansvaret som är beskrivet ovan följer vissa konsekvenser. Om staten har anlitat en privat aktör för att utföra något led i den gränsöverskridande identifieringen (t.ex. identitetskontrollen) är det viktigt att avtalet mellan staten och den privata aktören reglerar en eventuell ansvarskedja som uppstår om en skada inträffar.

Det är framför allt anmälan av elektroniska identitetshandlingar utfärdade av privata aktörer som aktualiseras här men det finns även andra situationer där staten kan anlita privata underleverantörer för att uppfylla sina åtaganden, t.ex. när det gäller uppbyggnad av noden.

När det blir aktuellt att anmäla privat utfärdade elektroniska identitetshandlingar behöver tydliga avtal som reglerar skadeståndsansvar utformas mellan staten och de privata utfärdarna. Annars finns det risk för att staten tvingas ta ett skadeståndsansvar som man inte har tänkt sig eller att tvist uppstår mellan staten och de privata aktörerna.

Avtalen behöver också behandla ansvaret vid eventuella säkerhetsincidenter. Det är medlemsstaten som ansvarar enligt artikel 10.1, eIDAS-förordningen för att upphäva eller återkalla den elektroniska identitetshandlingen som är utsatt för intrång eller äventyras. Sverige måste därför ges förutsättningar att ta sådant ansvar när avtal sluts med privata utfärdare.

Ekonomiska risker

En ekonomisk risk utgörs av skadeståndsansvaret som är beskrivet ovan.

Att staten har skadeståndsansvar för dessa situationer är i sig inget anmärkningsvärt. Det faller sig naturligt att staten får ta ansvar för skada som orsakats på grund av statens agerande eller brist på agerande. Däremot är det naturligtvis ändå en ekonomisk risk som följer av att Sverige anmäler elektroniska identitetshandlingar för gränsöverskridande identifiering enligt eIDAS-förordningen. Risken måste vägas in i bedömningen när det ska avgöras vilka elektroniska identitetshandlingar som Sverige ska anmäla för gränsöverskridande identifiering.

En annan ekonomisk risk med anmälan är att Sverige tar fram en statlig elektronisk identitetshandling för gränsöverskridande identifiering utan att den blir använd i någon större utsträckning. Det kan visa sig att behovet av gränsöverskridande elektronisk identifiering är

överskattat eller att användarna av någon anledning väljer att inte nyttja systemet. De förslag som utredningen lämnar i kapitel 12 handlar dock om att ta fram statliga elektroniska identitetshandlingar som kan fylla flera syften. Även om den gränsöverskridande verksamheten inte skulle utvecklas i takt med förhoppningarna finns ändå stora värden, beskrivna i kapitel 12, i att staten tillhandahåller elektroniska identitetshandlingar på den högsta tillitsnivån.

18.3 Digitaliseringsmyndigheten ansvarar för anmälan av elektroniska identitetshandlingar

Utredningen föreslår:
att digitaliseringsmyndigheten ska ansvara för att anmäla svenska elektroniska identitetshandlingar till kommissionen för gränsöverskridande identifiering enligt eIDAS-förordningen.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering samt förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Enligt eIDAS-förordningens lydelse[7] är det medlemsstaterna som anmäler elektroniska identitetshandlingar för gränsöverskridande identifiering till EU-kommissionen. I Sverige bör denna uppgift delegeras till en lämplig statlig myndighet. En anmälningsprocess av elektroniska identitetshandlingar för granskning inom Sverige är lång och kostnadskrävande. Enligt uppgift från E-legitimationsnämndens kansli kan en sådan process ta ett år på grund av de anpassningar utfärdarna kan behöva genomföra för att nå upp till de krav som gäller för att få bli kvalitetsmärkta.

Utredningen anser att regeringen bör utse den nya digitaliseringsmyndigheten att ha denna uppgift tillsammans med övriga administrativa och granskande uppgifter som rör gränsöverskridande identifiering enligt eIDAS-förordningen.

[7] Artikel 9.1, eIDAS-förordningen.

18.3.1 Vilka elektroniska identitetshandlingar får anmälas?

Utredningen föreslår:
att Sverige tillämpar ett öppet system för anmälan. Utfärdare som ansöker om att bli anmälda ska bli det om de uppfyller uppställda krav. När det finns en statlig svensk elektronisk identitetshandling ska den anmälas.
att digitaliseringsmyndigheten ska tillhandahålla ett parallellt valfrihetssystem för elektroniska identitetshandlingar för gränsöverskridande identifiering.

Nästa fråga att ta ställning till är hur lämpliga elektroniska identitetshandlingar ska utses för anmälan. Utredningen konstaterar att Tyskland, som redan har anmält elektroniska identitetshandlingar, och merparten av de länder som står i begrepp att anmäla någon elektronisk identitetshandling väljer att anmäla statligt utfärdade elektroniska identitetshandlingar.[8] Det kan bero på att de inte har inhemska privata alternativ men också på de skäl som anges ovan om att det ändå i flera avseenden är den anmälande medlemsstaten som ansvarar för den elektroniska identitetshandlingen.

I Sverige saknas en statligt utfärdad elektronisk identitetshandling. Utredningen föreslår i kapitel 12 att det ska ingå i det offentliga åtagandet att tillhandahålla en statlig elektronisk identitetshandling som ska fästas på en fysisk bärare i form av en befintlig identitetshandling. Eftersom 2017 års ID-kortsutredning[9] har i uppdrag att se över vilka identitetshandlingar som ska betraktas som sådana behöver processen för statliga elektroniska identitetshandlingar invänta denna utrednings förslag om vilka fysiska identitetshandlingar som ska finnas kvar. 2017 års ID-kortsutredning ska lämna sina förslag senast den 29 mars 2019. Det innebär att det dröjer flera år innan det i Sverige finns någon *statligt* utfärdad elektronisk identitetshandling att anmäla.

En konsekvens av att använda ett öppet system för anmälan kan bli att Sverige kan komma att anmäla många elektroniska identitetshandlingar för gränsöverskridande identifiering, till skillnad från

[8] Den 8 december 2017 anmälde Italien som andra land i EU ett system för elektroniska identitetshandlingar för gränsöverskridande identifiering. Det anmälda systemet innehåller åtta elektroniska identitetshandlingar. Utfärdaren, SPID, är en privat aktör.
[9] Dir. 2017:90, Åtgärder för att minska bedrägeribrottsligheten – skärpta krav och rutiner för svenska identitetshandlingar.

andra medlemsstater som kanske nöjer sig med varsin statligt utfärdad. Det kan leda till att det gemensamma systemet för granskning av anmälda elektroniska identitetshandlingar belastas oproportionerligt mycket av svenska anmälningar vilket i sin tur kan leda till missnöje bland de andra medlemsstaterna. Granskningen kan vara omfattande och resurskrävande.

Utredningen bedömer att Sverige behöver anmäla åtminstone en svensk elektronisk identitetshandling för gränsöverskridande identifiering innan det finns en statligt utfärdad elektronisk identitetshandling tillgänglig. Därför behövs ett förfarande för hur det ska gå till.

Upphandlingsförfarande är inte lämpligt

När en offentlig aktör behöver anlita en privat tjänst eller vara är huvudregeln att detta ska upphandlas enligt LOU.[10] Det finns dock möjligheter till undantag och det finns skäl för att undvika ett vanligt upphandlingsförfarande.

Ett skäl är att upphandling innebär att endast en leverantör kan vinna upphandlingen och det utesluter därmed att andra leverantörer kan ta del av marknaden. Det gör att marknadsutvecklingen riskerar att hämmas eftersom det i praktiken endast blir en aktör som kan agera per tidsperiod som upphandlingen avser.

Dessutom bör förfarandet med elektroniska identitetshandlingar för gränsöverskridande identifiering i möjligaste mån korrelera med elektroniska identitetshandlingar för användning inom Sverige. Inom Sveriges gränser föreslår utredningen fortsatt tillämpning av valfrihetssystem (se avsnitt 13.5.4) och det är därför lämpligt att göra det även när det gäller gränsöverskridande identifiering.

Valfrihetssystem

Marknaden för elektroniska identitetshandlingar i Sverige beskrivs i flera kapitel ovan. Den domineras av en stark och inom landet väl utbredd aktör, BankID, men det finns även andra aktörer som är intresserade av tillgång till den inre marknaden inom EU. För att kunna ge de aktörer som är intresserade chansen att medverka bedömer utredningen att ett valfrihetssystem med tydliga villkor är ett

[10] Lagen (2016:1145) om offentlig upphandling.

lämpligt sätt att gå tillväga för att Sverige ska kunna anmäla elektroniska identitetshandlingar för gränsöverskridande identifiering.

Lagen om valfrihet i fråga om tjänster för elektronisk identifiering[11] utesluter inte att det kan finnas flera parallella valfrihetssystem. Det valfrihetssystem som används i dag för elektronisk identifiering inom Sverige kan därför kompletteras med ytterligare ett valfrihetssystem där utfärdare av elektroniska identitetshandlingar får ansluta sig om de vill att deras elektroniska identitetshandling ska kunna användas för gränsöverskridande identifiering.

Utfärdare av privata elektroniska identitetshandlingar kan ha olika syften med sina produkter. Vissa kan vilja tillhandahålla sina elektroniska identitetshandlingar enbart på den svenska marknaden. För dem behöver det finnas ett valfrihetssystem som är utformat som det som finns i dag. Andra utfärdare kan vilja erbjuda elektroniska identitetshandlingar för gränsöverskridande identifiering. För dem behövs då ett separat valfrihetssystem med fler krav än vad som ställs i valfrihetssystemet för den svenska marknaden.

Enligt artikel 7 b) eIDAS-förordningen krävs dock att elektroniska identitetshandlingar ska kunna användas för att få åtkomst till åtminstone en offentlig e-tjänst som kräver elektronisk identifiering i den anmälande medlemsstaten.

18.3.2 Förutsättningar för anmälan

Utredningen föreslår:
att för att kunna anmälas av Sverige för gränsöverskridande identifiering måste en elektronisk identitetshandling:

1. vara kvalitetsgranskad och godkänd av digitaliseringsmyndigheten,
2. endast utfärdas till medborgare eller folkbokförda i Sverige,
3. ingå i valfrihetssystem enligt lagen om valfrihetssystem i fråga om tjänster för elektronisk identifiering,[12]

[11] SFS 2013:311.
[12] Denna lag föreslås i ett annat kapitel byta namn till lag om valfrihetssystem i fråga om funktioner för elektronisk identitetskontroll. Det förslaget kan dock inte väntas träda i kraft så snart som de ändringar som föreslås i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Utredningen benämner därför lagen med sitt nuvarande namn i detta kapitel.

4. vara utfärdad av en aktör som har tecknat försäkring som täcker ersättning för skada som åsamkats fysiska eller juridiska personer avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla de skyldigheter som avses i artikel 7 i eIDAS-förordningen.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Utredningen föreslår ett antal kriterier som måste uppfyllas för att en elektronisk identitetshandling ska få anmälas för gränsöverskridande identifiering.

Såsom utredningen tidigare har beskrivit kvalitetsgranskar E-legitimationsnämnden elektroniska identitetshandlingar mot ett nationellt tillitsramverk som bygger på internationell standard.

En elektronisk identitetshandling som anmäls måste vara kvalitetsgranskad och godkänd av digitaliseringsmyndigheten. En kvalitetsmärkt elektronisk identitetshandling går att lita på för offentliga och privata aktörer med e-tjänster som kräver elektroniska identitetshandlingar. Även användare kan känna sig trygga med att en kvalitetsmärkt elektronisk identitetshandling är en säker identitetshandling.[13] Vidare får den elektroniska identitetshandlingen endast utfärdas till medborgare eller folkbokförda i Sverige. Det innebär att innehavarna av identitetshandlingen har ett svenskt personnummer. I den svenska folkbokföringen är personnummer en bas för vidare identifiering. Utredningen bedömer att svenska samordningsnummer inte uppnår den nivå av säkerhet som krävs för att Sverige ska kunna uppfylla kraven i artikel 7 d) och e) om att de personidentifieringsuppgifter som unikt representerar personen i fråga tillskrivs den fysiska person som avses vid tidpunkten för utfärdandet samt att den elektroniska identitetshandlingen faktiskt tilldelas den person som avses. Mer information om samordningsnummer och dess säkerhetsbrister finns i avsnitt 17.5.

Den elektroniska identitetshandlingen måste även ingå i valfrihetssystem enligt lagen om valfrihetssystem i fråga om tjänster för elektronisk identifiering. Det är ett sätt att låta användaren välja vilken

[13] www.elegnamnden.se/leverantor/bligodkandeidutfardareenligtsvenskelegitimation.4.5a85666214dbad743ffe6e6.html, 2017-11-23.

elektronisk identitetshandling hon eller han föredrar att använda och det är samtidigt en garant för att alla utfärdare av elektroniska identitetshandlingar för gränsöverskridande identifiering ska erhålla samma ersättning av staten.

Slutligen ska utfärdaren av den elektroniska identitetshandlingen även teckna en försäkring som täcker ersättning för skada som åsamkats fysiska eller juridiska personer avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla de skyldigheter som avses i artikel 7 i eIDAS-förordningen. Om något inträffar som innebär sådan skada kommer den anmälande medlemsstaten i många fall att hållas ansvarig enligt eIDAS-förordningen. För att Sverige ska kunna anmäla privat utfärdade elektroniska identitetshandlingar behövs därför en försäkring som täcker eventuella skador så att staten inte behöver betala för en skada som är orsakad av en privat utfärdare.

18.3.3 Ansvarsfördelning vid anmälan av elektroniska identitetshandlingar

Utredningen föreslår:
att den myndighet som anmäler de elektroniska identitetshandlingarna för gränsöverskridande identifiering också ska ansvara för att tillfälligt upphäva, återkalla, återinföra och dra tillbaka elektroniska identitetshandlingar vid säkerhetsincidenter enligt artikel 10 i eIDAS-förordningen.

Förslaget genomförs genom lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Utöver de frågor som redan har behandlats ovan när det gäller ansvarsfrågor tillkommer några ytterligare situationer där det krävs att ansvaret från början är fördelat mellan aktörerna på ett godtagbart och förutsebart sätt.

Artikel 10 behandlar säkerhetsincidenter och i 10.1 anges att den anmälande medlemsstaten utan dröjsmål tillfälligt ska upphäva eller återkalla den elektroniska identitetshandling eller gränsöverskridande autentisering som utsätts för intrång eller delvis äventyras på ett sätt som påverkar tillförlitligheten. Vidare beskrivs i artikel 10.2

och 10.3 förutsättningar för att återinföra eller dra tillbaka den elektroniska identitetshandlingen.

Utredningen anser att det bör ankomma på digitaliseringsmyndigheten att vara behörig myndighet för att utföra sådana uppgifter. Det är digitaliseringsmyndigheten som har varit involverad i anmälan av den elektroniska identitetshandlingen och har insyn i detaljerna om hur den fungerar. Det är även digitaliseringsmyndigheten som ingår avtal med utfärdare av elektroniska identitetshandlingar där incidentsituationer bör regleras och ge digitaliseringsmyndigheten tekniska möjligheter att utföra uppgifterna.

Mer om skadestånd

När det gäller skadeståndsfrågor har utredningen i avsnitt 18.2.2 behandlat skadeståndsansvar enligt artikel 11.1 och 11.2. Det återstår frågor om ansvarsfördelning i situationer enligt artikel 11.3, 11.4 och 11.5.

Enligt artikel 11.3 ska den part som handhar autentiseringsförfarandet ha skadeståndsansvar för skada som åsamkats en fysisk och juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att säkerställa korrekt handhavande av den autentisering som avses i artikel 7 f vid en gränsöverskridande transaktion.

Enligt artikel 7 f ska den anmälande medlemsstaten se till att autentisering är tillgänglig via internet så att alla förlitande parter som är etablerade på någon annan medlemsstats territorium kan bekräfta de personidentifieringsuppgifter som tas emot i elektronisk form.

Svårigheten här är att det kan vara flera aktörer som handhar olika delar av autentiseringsförfarandet. Så länge det är fråga om en statlig aktör får staten (genom digitaliseringsmyndigheten) ta skadeståndsansvaret. Det gäller med andra ord alla uppgifter som utförs av noden. Om noden ligger nere, skickar fel uppgifter eller på något annat sätt orsakar skada enligt 11.3 är staten ansvarig enligt eIDAS-förordningens lydelse.

Om skadan handlar om kontroll av äkthet och eventuell spärr av den elektroniska identitetshandlingen eller något annat som utfärdaren står för är det utfärdaren som har skadeståndsansvar enligt samma bestämmelse.

I artikel 11.4 och 11.5 hänvisas till att de tidigare reglerna om skadestånd (artikel 11.1, 11.2 och 11.3) ska tillämpas i enlighet med nationella bestämmelser samt att nationell rätt dessutom har företräde framför förordningstexten. Här är svårigheten att det inte anges vilken nationell rätt som avses. I frågor om gränsöverskridande identifiering ligger det i sakens natur att den skadelidande kan befinna sig i en medlemsstat och den skadeståndsansvarige i en annan. Dessa respektive medlemsstater kan ha nationell rätt som ger motstående lösningar på problemen.

Enligt huvudregeln i artikel 4.1 i den s.k. Rom II-förordningen[14] ska i fråga om en utomobligatorisk[15] förpliktelse som har sin grund i en skadeståndsgrundande händelse, lagen i det land där skadan uppkommer tillämpas oavsett i vilket land den skadevållande händelsen inträffade och oavsett i vilket eller vilka länder indirekta följder av händelsen uppkommer.

Det finns dock undantagsbestämmelser i artikel 4.2 och 4.3. Av artikel 4.2 följer att om både den person vars ansvar görs gällande och den skadelidande har sin vanliga vistelseort i samma land vid den tidpunkt då skadan uppkommer ska lagen i det landet tillämpas.

I artikel 4.3 beskrivs ytterligare en situation som kan avgöra vilket lands lagstiftning som ska tillämpas. Om det framgår av alla omständigheter i fallet att den skadeståndsgrundande händelsen har en uppenbart närmare anknytning till ett annat land än det som anges i punkt 1 eller 2, ska lagen i det landet tillämpas. En uppenbart närmare anknytning till ett annat land kan särskilt grundas på att det redan finns ett rättsförhållande mellan parterna, såsom ett avtal som har nära anknytning till den skadeståndsgrundande händelsen i fråga.

De beskrivna undantagssituationerna är inte något som privata leverantörer kan räkna med. Den återgivna regleringen måste därmed innebära att en svensk privat utfärdare eller leverantör som är ansvarig i något led av autentiseringsförfarandet kan behöva förhålla sig till skadeståndsbestämmelser i alla de länder som omfattas av eIDAS-förordningen (28 medlemsstater och ytterligare fyra som skrivit avtal

[14] Europaparlamentet och Rådets förordning (EG) nr 864/2007 av den 11 juli 2007 om tillämplig lag för utomobligatoriska förpliktelser (Rom II).

[15] När två parter står i kontraktsförhållande till varandra bestäms skadeståndsskyldigheten dem emellan av avtalet eller åtminstone av regler som anknyter till kontraktsförhållandet. När ett kontraktsförhållande inte finns eller inte inverkar – en ofta viktig modifikation – befinner man sig på området för den utomobligatoriska skadeståndsrätten. Skadeståndsrätt, Jan Hellner och Marcus Radetzki, upplaga 9, publicerad i Zeteo, 2014-08-11, s. 23.

om att få ingå i regelverket) beroende på var den elektroniska identitetshandlingen används och var skadan således kan sägas uppstå.

Skadeståndsansvaret regleras alltså när det gäller elektronisk identifiering i stora drag på samma sätt som när det gäller andra varor och tjänster. Det behöver inte vara ett problem men utredningen vill ändå belysa frågan i detta sammanhang för att inblandade aktörer ska känna till den.

18.4 Vilka svenska uppgifter ska överföras?

Sverige måste ta ställning till vilka personuppgifter om svenska användare som ska överföras till utländska noder och e-tjänster vid gränsöverskridande identifiering.

I artikel 11.1 i genomförandeförordningen 2015/1501[16] anges att en minimiuppsättning av personidentifieringsuppgifter som är unika för en fysisk eller juridisk person ska uppfylla kraven i bilagan vid användning i ett gränsöverskridande sammanhang. I dagsläget finns inga elektroniska identitetshandlingar för juridiska personer i Sverige. I eIDAS-förordningen behandlas inte heller frågor om behörighet för att företräda juridiska personer. Därför kommer i det följande enbart uppgifter för fysiska personer att behandlas.

Enligt första punkten i bilagan är kraven följande:

Minimiuppsättning av uppgifter för fysisk person

En minimiuppsättning av uppgifter för en fysisk person ska innehålla följande obligatoriska attribut:

h) nuvarande efternamn,

i) nuvarande förnamn,

j) födelsedatum,

k) en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikatio-

[16] Kommissionens genomförandeförordning (EU) 2015/1501 av den 8 september 2015 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

nerna för gränsöverskridande identifiering och som är mest beständig i tid.

En minimiuppsättning för en fysisk person kan innehålla ett eller flera av följande ytterligare attribut:

a) förnamn och efternamn vid födseln,

b) födelseort,

c) nuvarande adress,

d) kön.

De första fyra attributen måste ingå och de senare fyra attributen är valfria. Sverige behöver ta ställning till dels hur den unika identitetsbeteckningen ska utformas, dels om några valfria attribut ska översändas.

18.4.1 Minimering av behandling av personuppgifter

Utredningen bedömer:
att en princip om minimering av personuppgifter bör råda så att inga valfria attribut sänds över så länge inga särskilda avtal träffas med vissa länder om detta.

En lämplig informationssäkerhetsåtgärd är att alltid se till att minimera behandlingen av personuppgifter. Det följer även av dataskyddsförordningen. Utgångspunkten bör därför enligt utredningens mening vara att inga valfria attribut sänds över så länge inga särskilda överenskommelser görs med vissa länder i detta avseende.

18.4.2 Pseudonym i stället för överföring av svenska personnummer

Utredningen bedömer:
att Sverige bör använda pseudonymer vid gränsöverskridande identifiering.

Utredningen föreslår:
att regeringen ger Skatteverket i uppdrag att i samråd med digitaliseringsmyndigheten ta fram ett system för pseudonymer för gränsöverskridande identifiering.

Artikel 5 eIDAS-förordningen gäller behandling och skydd av uppgifter. I första punkten anges att personuppgifter ska behandlas i enlighet med direktiv 95/46/EG.[17] Dataskyddsreformen som i skrivande stund är under genomförande innebär att personuppgifter från och med den 25 maj 2018 ska behandlas i enlighet med dataskyddsförordningen.[18]

I artikel 5.2 i eIDAS-förordningen anges att utan att det påverkar rättsverkan av pseudonymer enligt nationell rätt ska användningen av pseudonymer vid elektroniska transaktioner inte förbjudas. Det innebär att Sverige behöver ta ställning till om ett nytt system för pseudonymer behöver tas fram för ändamålet elektronisk identifiering.

Offentlighetsprincipen har en stark ställning i Sverige. Den innebär enligt 2 kap. 1 § tryckfrihetsförordningen[19] att varje svensk medborgare ska ha rätt att ta del av allmänna handlingar till främjande av ett fritt meningsutbyte och en allsidig upplysning. Offentlighetsprincipen kan inskränkas genom sekretessregler men folkbokföringsuppgifter är normalt offentliga. Dessa uppgifter kan i särskilda fall beläggas med sekretess, exempelvis när det rör sig om känsliga uppgifter. Som känsliga uppgifter räknas bl.a. adoption och könsbyte. Personnummer räknas inte som känsliga uppgifter.

[17] Dataskyddsdirektivet.
[18] Europaparlamentet och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[19] SFS 1949:105.

I många andra länder inom EU behandlas motsvarigheten till personnummer med sekretess. I bl.a. Tyskland och Österrike används pseudonymer inom respektive land.

Det finns integritetsskäl för att inte föra ut personnummer utanför Sveriges gränser och man kan argumentera för att dessa integritetsskäl egentligen också gäller inom landets gränser. Offentlighetsprincipen har lett till att det är enkelt att få tag i personnummer och därefter kan man begära ut väldigt mycket information om en individ, t.ex. inkomstuppgifter, ägande av fastigheter, familjeförhållanden och brottshistorik. Det gör det också möjligt för bedragare att kapa identiteter.

Utredningen anser att Sverige bör använda möjligheten i eIDAS-förordningen att använda pseudonymer vid gränsöverskridande identifiering. Ett uppdrag att ta fram systemet för pseudonymer bör ges till Skatteverket i samråd med digitaliseringsmyndigheten.

Riktlinjer för pseudonymen

Det är viktigt att den persistenta[20] effekten av personnummer kvarstår. Det behövs därför ett samlat system av pseudonymer i stället för att varje utfärdare av elektroniska identitetshandlingar ska ta fram sitt eget.

Om ett nytt begrepp skulle bli aktuellt att införa som pseudonym, finns det vissa önskvärda egenskaper att tänka på. Detta har bland annat beskrivits av E-legitimationsnämnden.[21] Pseudonymbegreppet bör utformas så att det

- inte är värdebärande, t.ex. inte beskriva födelsedag,
- är unikt,
- är kort och enkelt att förstå,
- är stabilt över tid,

[20] Med persistens avses i detta sammanhang att numret ska vara detsamma så att man kan lita på att individen är densamma, helst under hela sin livstid.
[21] E-legitimationsnämndens rapport E-legitimationer enligt eIDAS, E-legitimationsnämndens analys av EU-förordningen om elektronisk identifiering och betrodda tjänster (EU nr 910/2014), regeringsuppdrag (N2015/2620/EF), dnr: 131 182017-15/9513 | 2015-12-16, s. 19 f.

- är möjligt att verifiera med kontrollsiffra,
- inte krockar med annan nummerserie av betydelse,
- är uppbyggt så att det innehåller både bokstäver och siffror,
- skapas enligt en slumpmässig metod och inte till exempel är ett serienummer.

Dessutom menar E-legitimationsnämnden att det är viktigt för individen att känna till sin eventuella pseudonym och att spårbarheten behöver säkras.

Nästa fråga är vem som ska ha ansvar för att omvandla personnummer till pseudonym. Det kan vara Skatteverket, som ansvarar för folkbokföringen. Det kan också vara utfärdarna av elektroniska identitetshandlingar. Det skulle även kunna vara digitaliseringsmyndigheten som via noden omvandlar personnummer till pseudonym.

18.5 Ersättningsmodell till privata utfärdare av anmälda elektroniska identitetshandlingar som används i utländska e-tjänster

Utredningen föreslår:
att privata utfärdare av anmälda elektroniska identitetshandlingar som används i utländska e-tjänster i offentlig sektor ska ersättas av statliga medel och fakturera Kammarkollegiet för det antal identitetsintyg som utländska offentliga myndigheter har begärt.
att privata utfärdare av anmälda elektroniska identitetshandlingar som används i utländska e-tjänster i privat sektor inte ska ersättas av statliga medel.

När det gäller ersättningsmodell är det önskvärt att systemen inom Sverige och i Europa korrelerar med varandra. Enligt vad som tidigare har beskrivits i avsnitt 13.7 ska privata utfärdare av elektroniska identitetshandlingar som används i Sverige fakturera Kammarkollegiet för det antal identitetsintyg som utländska offentliga myndigheter har begärt. Staten ska stå för kostnaden när det gäller användning av privat utfärdade elektroniska identitetshandlingar i alla offentliga e-tjänster.

I linje med det förslag som gäller användandet av privat utfärdade elektroniska identitetshandlingar i svenska offentliga e-tjänster föreslår utredningen att staten ska stå för kostnaden även när det gäller användningen av privat utfärdade elektroniska identitetshandlingar i utländska e-tjänster inom offentlig sektor. Den privata utfärdaren kan fakturera Kammarkollegiet för den användning som förekommit i utländska offentliga e-tjänster. Den svenska noden kan avgöra om e-tjänsten är offentlig eller privat och meddela aktörerna (utfärdaren och Kammarkollegiet) när det är fråga om offentliga e-tjänster.

När det gäller privata e-tjänster bör dock inte det offentliga åtagandet sträcka sig längre än vad det ska göra inom Sverige. Det får till följd att privata utfärdare av elektroniska identitetshandlingar inte får ersättning av staten när de elektroniska identitetshandlingarna används i e-tjänster i privat sektor utomlands. Kostnaden för sådan användning av elektroniska identitetshandlingar får privata utfärdare i stället täcka på annat sätt, genom att ta betalt av användarna eller inkludera kostnaden i andra tjänster till användarna, precis som det fungerar i Sverige för närvarande.

19 Betrodda tjänster enligt eIDAS-förordningen

19.1 Svenska offentliga myndigheters användning av betrodda tjänster

19.1.1 Betrodda tjänster enligt eIDAS-förordningen

Syftet med eIDAS-förordningen är enligt artikel 1 att säkerställa en väl fungerande marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster.

I artikel 4 i förordningen slås principen om en inre marknad fast. Den som tillhandahåller betrodda tjänster i en medlemsstat får inte hindras att tillhandahålla sådana tjänster i en annan medlemsstat av skäl som anges i förordningen. Anordningar för underskrifter och stämplar, och betrodda tjänster som överensstämmer med förordningen ska omfattas av fri rörlighet på den inre marknaden.

I förordningen finns allmänna bestämmelser om betrodda tjänster och kvalificerade betrodda tjänster samt särskilda bestämmelser om elektroniska underskrifter, elektroniska stämplar, elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och autentisering av webbplatser. Dessutom finns det bestämmelser om elektroniska dokument som är innehåll lagrat i elektronisk form som även omfattar ljud- och bildinspelningar och audiovisuella inspelningar.

19.1.2 Tillämpningsområde

Förordningen gäller enligt artikel 2.1 system för elektronisk identifiering som en medlemsstat har anmält och tillhandahållare av betrodda tjänster som är etablerade inom unionen. Förordningen gäller

däremot inte tillhandahållande av betrodda tjänster som till följd av nationell lagstiftning eller avtal mellan en avgränsad krets deltagare endast används inom slutna system. Detta framgår av artikel 2.2. I skäl (21) utvecklas vad som menas med slutna system. Där anges att förordningen inte gäller tillhandahållare av tjänster som endast används inom slutna system mellan en avgränsad uppsättning deltagare och som inte påverkar tredje man. Som exempel nämns system som inrättats i företag eller offentlig förvaltning för hantering av interna förfaranden. I skälet anges vidare att endast betrodda tjänster som tillhandahålls för allmänheten och som påverkar tredje man bör uppfylla de krav som ställs i förordningen.

Enligt artikel 2.3 påverkar förordningen inte heller bestämmelser i nationell lagstiftning eller unionslagstiftningen som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav. Förordningen bör enligt skäl (21) inte heller inverka på nationella formkrav avseende offentliga register, i synnerhet inte kommersiella register eller fastighetsregister. I svensk lagstiftning ställs för närvarande inte några krav på att använda kvalificerade betrodda tjänster vare sig mellan enskilda eller gentemot offentliga organ.

19.1.3 Definitioner

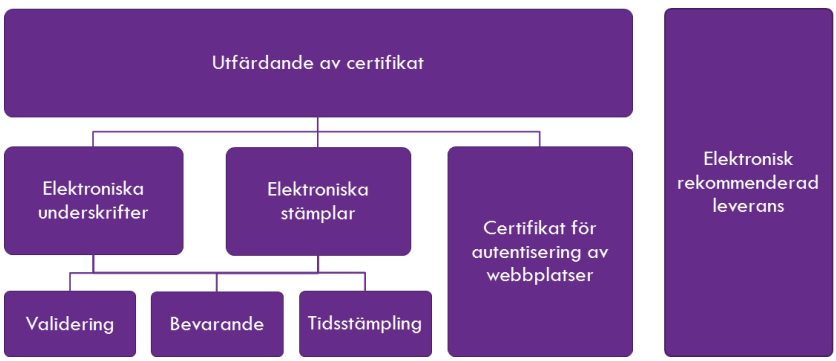
I artikel 3 återfinns vissa definitioner. Där anges bl.a. att med en *betrodd tjänst* avses en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar samt elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster. Med betrodda tjänster avses också skapande, kontroll och validering av certifikat för autentisering av webbplatser samt bevarande av elektroniska underskrifter, stämplar och certifikat med anknytning till dessa tjänster.

19.1.4 Vilka betrodda tjänster regleras i eIDAS-förordningen?

I förordningen finns ett antal betrodda tjänster reglerade genom fullständig harmonisering. Flera av dessa betrodda tjänster är beroende av certifikat och certifikatutfärdare. En förutsättning för att kunna skapa en avancerad eller kvalificerad elektronisk underskrift är att ett certifikat med tillhörande privat nyckel har utfärdats av en certifikatutfärdare. Med hjälp av nycklarna och certifikaten kan certifikatinnehavaren med sin privata nyckel skapa en avancerad eller elektronisk underskrift som sedan kan kontrolleras med den publika nyckeln och personen kan identifieras genom uppgifterna i certifikatet. Flera av kraven i förordningen i artikel 24 är riktade till kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat.

Följande bild har tagits fram av Post- och telestyrelsen (PTS) och kan förenkla förståelsen av vilka de fullständigt harmoniserade betrodda tjänsterna är.

Figur 19.1 Betrodda tjänster i relation till varandra



En *elektronisk stämpel* är för en juridisk person motsvarigheten till en elektronisk underskrift av en fysisk person.

Med *elektronisk tidsstämpling* avses uppgifter i elektronisk form som binder andra uppgifter i elektronisk form till en viss tidpunkt och därmed utgör bevis för att de senare uppgifterna existerade vid den angivna tidpunkten.

Elektroniska tjänster för rekommenderade leveranser gör det möjligt att överföra uppgifter mellan tredje män på elektronisk väg på ett sätt som tillhandahåller bevis om uppgifternas hantering, inklusive

sändande och mottagande, och som skyddar uppgifterna mot risken för förlust, stöld, skada eller otillåtna ändringar.

Genom *autentisering av webbplatser* är det möjligt att bekräfta att en fysisk eller juridisk person är kopplad till en viss webbplats och att uppgifterna på webbplatsen är korrekta.

Även skäl (21)–(25) är av intresse för bedömningen av vad som ska betraktas som en betrodd tjänst.

19.1.5 Kvalificerade betrodda tjänster

I artiklarna 20–24 finns särskilda bestämmelser om kvalificerade betrodda tjänster. Den som vill tillhandahålla sådana tjänster ska anmäla detta till tillsynsmyndigheten[1] och samtidigt lämna in en rapport med en överensstämmelsebedömning som är utfärdad av ett ackrediterat organ för bedömning av överensstämmelse.[2] Om tillhandahållaren och dennes betrodda tjänster uppfyller förordningens krav beviljas dessa status som kvalificerade och förs upp på en nationell förteckning (eng. *trusted list*) över kvalificerade tillhandahållare av betrodda tjänster inom EU och de tjänster som dessa tillhandahåller. Det finns även ett förfarande för återkallande av en tillhandahållares eller en tjänsts status som kvalificerad om kraven inte längre uppfylls.

För kvalificerade tillhandahållare av betrodda tjänster gäller särskilda krav på, t.ex.

- Kontroll av identiteten hos den till vilken ett kvalificerat certifikat utfärdas,
- Personalens utbildning och kunskaper,
- Ekonomisk förmåga att bära risken för verksamheten,
- Teknisk säkerhet och tillförlitlighet hos system,
- Löpande planering för att kunna garantera tjänstens kontinuitet i fall av verksamhetens upphörande.

Förordningen innehåller också krav på att kvalificerade tillhandahållare av betrodda tjänster återkommande ska granskas av ackredite-

[1] I Sverige är det PTS.
[2] Organen brukar benämnas som certifieringsorgan eller Conformity Assessment Body (CAB).

rade organ i syfte att kontrollera att tillhandahållarna uppfyller förordningens krav.

19.2 Krav som omfattar såväl kvalificerade som icke kvalificerade tillhandahållare

Vissa bestämmelser i förordningen berör alla tillhandahållare, dvs. även tillhandahållare som inte är kvalificerade i förordningens mening. Såväl kvalificerade som icke kvalificerade tillhandahållare omfattas bl.a. av kraven som gäller skadeståndsansvar i artikel 13 och säkerhet i artikel 19.

Av skäl (35) följer att syftet med regleringen är att säkerställa att även de icke kvalificerade tillhandahållarna har vederbörlig noggrannhet, insyn och ansvarighet i sina verksamheter och tjänster. Det anges dock att med tanke på den typ av tjänster som tillhandahålls bör det göras åtskillnad mellan kraven på kvalificerade och på icke kvalificerade tillhandahållare.

19.3 Vilka betrodda tjänster används av den offentliga förvaltningen i Sverige?

Den svenska offentliga förvaltningen använder betrodda tjänster, både internt och externt i samband med tillhandahållande av e-tjänster. De flesta aktörer i den offentliga förvaltningen som har e-tjänster använder elektroniska identitetshandlingar för elektronisk identitetskontroll och underskrift. För att nå e-tjänsten används även certifikat för autentisering av webbplatser. Det innebär att en individ identifierar sig med en elektronisk identitetshandling, t.ex. mobilt BankID. Den offentliga myndigheten använder ett certifikat för autentisering av webbplatser för att identifiera sig till individen och skydda informationen som överförs genom att kryptera förbindelsen. Efter identitetskontrollen får individen i e-tjänsten se uppgifter om sig själv. Individen kan sedan förändra informationen i en deklaration eller ansöka om studiemedel och skriva under elektroniskt innan informationen skickas vidare in i den offentliga myndighetens verksamhetssystem.

När den offentliga myndigheten tar emot den underskrivna handlingen tidsstämplas den för att i efterhand kunna visa när den kom in.

Därefter görs en validering, dvs. en kontroll av att certifikatet som användes för att skapa underskriften var giltigt vid tidpunkten för underskrift och tidpunkten för mottagande. Valideringen innefattar även en kontroll av den kryptografiska kopplingen mellan de underskrivna uppgifterna och underskriften. Om detta steg inte validerar så har den underskrivna informationen förändrats sedan tidpunkten för underskrift. Den offentliga myndigheten bevarar informationen och underskrifterna för vidarebearbetning och arkivändamål. Hur länge detta behöver bevaras kan variera.

I flera fall tas ovanstående steg hos den statliga myndighet, kommun eller det landsting som tillhandahåller e-tjänsten. Eftersom ingen av dessa delar kommuniceras med, eller på annat sätt berör, tredje man kan ett sådant användande anses vara inom en sluten grupp. Till följd av detta är dessa interna tjänster undantagna från de skyldigheter för en betrodd tjänst som annars följer av förordningen. Det finns även företag som tillhandahåller dessa tjänster, t.ex. validering av elektroniska identitetshandlingar, som en tjänst. Om en leverantör gör detta åt den offentliga myndigheten uppstår ett tredjemansförhållande mellan användaren och den offentliga myndigheten och då kan leverantören ses som en tillhandahållare av betrodda tjänster.

Offentlig förvaltning tillhandahåller även i vissa fall blanketter eller dokument som skickas in i ett asynkront flöde, dvs. den som använder blanketten laddar ner, fyller i och skriver under blanketten för att sedan skicka den vidare till en statlig myndighet, kommun eller landsting. Även i dessa fall används tjänster för underskrift, tidsstämpling, validering och bevarande på samma sätt som beskrivits ovan. Avgörande för om de betrodda tjänsterna omfattas av förordningens regler är om det är en del i ett slutet system, dvs. om de påverkar tredje man eller inte.

Flera offentliga myndigheter använder *Mina meddelanden.* Det är en funktion som har två huvudsakliga användningsområden; dels att specificera ramverket för hur meddelanden kan förmedlas mellan en *avsändande myndighet* och en *mottagare*, dels att vara den uppslagsfunktion som kopplar en registrerad mottagare till en specifik elektronisk brevlådeoperatör. Dessa brevlådeoperatörer kan troligen ses som tillhandahållare av den betrodda tjänsten elektronisk rekommenderad leverans eftersom Mina meddelanden möjliggör för att individer ska kunna ta emot, läsa och bevara elektronisk myndighetspost. För

att en användare ska kunna ta del av meddelanden som skickats genom Mina meddelanden krävs att hon eller han har en elektronisk identitetshandling och är ansluten till en digital brevlåda godkänd för att användas i Mina meddelanden.

19.3.1 Tillhandahållare av betrodda tjänster på den svenska marknaden

Det är svårt att av göra hur många tillhandahållare av betrodda tjänster som finns på den svenska marknaden. Det beror på att det inte finns någon anmälningsplikt för de som tillhandahåller betrodda tjänster om dessa inte har valt att bli kvalificerade tillhandahållare och tillhandahålla kvalificerade betrodda tjänster. En annan svårighet är att regelverket är nytt och det finns en otydlighet och gränsdragningsproblematik om en tillhandahållare tillhandahåller betrodda tjänster eller ej. Det finns ännu inte någon rättslig prövning som kan klargöra vad som är att ses som en betrodd tjänst eller ej.

Den svenska marknaden präglas av de formkrav som ställs i svensk lagstiftning på användning av betrodda tjänster och de behov som tillhandahållare av e-tjänster har. Formkraven ska uppfyllas för att möjliggöra elektroniska förfaranden. De tillhandahållare av betrodda tjänster som är etablerade i Sverige är främst sådana som utfärdar elektroniska identitetshandlingar vilket inkluderar certifikat för elektroniska underskrifter och tillhandahållare av underskriftstjänster baserade på identitetsintyg.

En annan kategori möjliga tillhandahållare är leverantörerna av digitala brevlådetjänster i Mina meddelanden. Mina meddelanden gör det möjligt för individer att ta emot, läsa och bevara digital myndighetspost. För att en användare ska kunna ta del av meddelanden som skickats genom Mina meddelanden krävs att hon eller han har en elektronisk identitetshandling och är ansluten till en digital brevlåda godkänd för att användas i Mina meddelanden. Leverantörer som tillhandahåller digitala brevlådetjänster kan ses som att de tillhandahåller den betrodda tjänsten elektronisk rekommenderad leverans.

En tredje kategori är tillhandahållare av tjänsten validering av elektroniska underskrifter.

19.4 Vad kräver eIDAS-förordningen när det gäller erkännande av elektroniska underskrifter från andra medlemsstater?

Av artikel 27 i eIDAS-förordningen följer en skyldighet att erkänna elektroniska underskrifter i offentliga e-tjänster från andra medlemsstater i EU och EES-området. Skyldigheten omfattar att godta *samma* eller *högre* (dvs. kvalificerade) nivå av elektroniska underskrifter och stämplar som används i den egna e-tjänsten.

Kommissionen har fattat beslut om en genomförandeakt[3] med referensformat för avancerade elektroniska underskrifter och stämplar i enlighet med artiklarna 27.5 och 37.5. Det innebär, enligt artikel 1 i genomförandeakten, en skyldighet för medlemsstaterna att i offentliga e-tjänster erkänna avancerade elektroniska underskrifter i vissa format.[4] Skyldigheten gäller även, enligt artikel 2, andra underskriftsformat under förutsättning att den medlemsstat där tillhandahållaren av betrodda tjänster som används av undertecknaren är etablerad, erbjuder andra medlemsstater möjligheter till validering av underskrift som är lämpad, när så är möjligt, för automatiserad behandling.

Samma krav som genomförandeakten anger för underskrifter gäller för stämplar i enlighet med artikel 3 och 4 i genomförandeakten.

19.4.1 Möjliga undantag till kravet om erkännande av elektroniska underskrifter och stämplar från andra medlemsstater

Av skäl (21) och artikel 2 framgår att förordningen inte påverkar nationell rätt eller unionsrätt som avser ingående av avtal eller andra rättsliga och förfarandemässiga skyldigheter avseende formkrav. Vidare framgår av skäl (21) att det inte finns någon allmän skyldighet att

[3] Kommissionens genomförandebeslut (EU) 2015/1506 av den 8 september 2015 om fastställande av specifikationer rörande format för avancerade elektroniska underskrifter och avancerade elektroniska stämplar i enlighet med artiklarna 27.5 och 37.5 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

[4] Formaten XML, CMS eller PDF på överensstämmelsenivå Basic, Timestamping eller Long Term eller använda en tillhörande underskriftsbehållare, ASIC.

använda eller installera en accesspunkt för alla befintliga betrodda tjänster.

19.5 Hur används elektroniska underskrifter i svenska offentliga e-tjänster?

Flera svenska offentliga myndigheter använder i dag e-tjänster som bygger på synkrona onlineförfaranden, dvs. där en användare av e-tjänsten identifierar sig i e-tjänsten som i sin tur hämtar information om användaren utifrån dennes behörighet. Som exempel kan nämnas att om man vill söka föräldrapenning för ett barn via Försäkringskassans e-tjänst kommer en kontroll göras att användaren är vårdnadshavare till ett barn (och i övrigt är behörig) innan ansökan kan hanteras. I sådana fall med synkrona flöden där allt är online styr e-tjänsten över den elektroniska underskriften som tecknas efter att användaren har identifierats och vidtagit någon åtgärd. I ett sådant flöde är det praktiskt svårt att ta emot och utveckla e-tjänsten på ett sådant sätt att den godtar andra elektroniska underskrifter än de som tjänsten förväntar sig kopplat till identitetskontrollen med hjälp av en elektronisk identitetshandling. Ett sätt att lösa elektroniska underskrifter i en sådan tjänst är att använda en underskriftstjänst som avropas från Kammarkollegiets ramavtal. En sådan underskriftstjänst utfärdar ett engångscertifikat utifrån den använda elektroniska identitetshandlingen för en underskrift. Samma förfaranden kan då användas för en utländsk elektronisk identitetshandling.

Andra offentliga myndigheter använder sig av asynkrona flöden, dvs. att en blankett laddas ner av undertecknaren som fyller i och skapar en elektronisk underskrift i sin miljö och skickar in till mottagande offentlig myndighet. Det kan också vara för de fall att undertecknarens verksamhetssystem undertecknar informationen och skickar in till mottagande myndighet. I dessa fall styr inte den offentliga myndigheten över de mottagna underskrifterna och de kan vara från olika länder och i olika format.

19.5.1 Svårigheter med att ta emot elektroniska underskrifter från andra länder

I svenska e-tjänster används främst underskrifter från elektroniska identitetshandlingar som BankID och underskriftstjänster från leverantörer på Kammarkollegiets ramavtal. Dessa underskrifter brukar anses vara på nivån avancerade elektroniska underskrifter och baserar sig på certifikat utfärdade av tillhandahållare av betrodda tjänster, dvs. det är inte kvalificerade certifikat. Avancerade elektroniska underskrifter ska enligt förordningens artikel 26 uppfylla följande krav:

a) Den ska vara unikt knuten till undertecknaren.

b) Undertecknaren ska kunna identifieras genom den.

c) Den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll.

d) Den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

En avancerad elektronisk underskrift kan sedan skapas utifrån certifikat som utfärdats av en betrodd tjänst eller en kvalificerad betrodd tjänst. Ett certifikat som utfärdats av en kvalificerad betrodd tjänst brukar benämnas ett kvalificerat certifikat. Som tidigare beskrivits innebär förordningen enligt artikel 27 att en medlemsstat som kräver en avancerad elektronisk underskrift för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska erkänna avancerade elektroniska underskrifter, avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat för elektroniska underskrifter och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i genomförandeakten på området.

Det finns svårigheter med att godta olika sorters format och underskrifter i onlinetjänster. Det är enklare när det gäller e-tjänster med asynkrona flöden där underskriften är helt separat från en offentlig myndighets e-tjänst, i undertecknarens miljö, och sedan skickas in med en underskrift. I dessa fall styr undertecknaren över underskriften och underskriftens format. Skyldigheten när det gäller nivåer av underskrifter och format följer av kraven enligt artikel 27 och den

tillhörande genomförandeakten. En e-tjänst kan känna igen de underskrifter som baserar sig på kvalificerade certifikat oavsett om de är avancerade eller kvalificerade elektroniska underskrifter genom att dessa kvalificerade tillhandahållare och deras kvalificerade betrodda tjänster finns förtecknade i ”trusted list”. Det finns dock en svårighet att känna igen avancerade elektroniska underskrifter från tillhandahållare av betrodda tjänster och betrodda tjänster som inte är kvalificerade eftersom dessa inte omfattas av någon anmälningsplikt och därmed inte finns i någon nationell eller internationell förteckning.

Betrodda tjänster som inte är kvalificerade omfattas inte av samma detaljreglering som kvalificerade betrodda tjänster vilket medför att det är svårt att jämföra en betrodd tjänst som en avancerad elektronisk underskrift från en tillhandahållare av betrodd tjänst jämfört med en annan tillhandahållare av avancerade elektroniska underskrifter. Det gör det svårt för en mottagande offentlig myndighet att avgöra om och hur en avancerad underskrift från en okänd tillhandahållare lever upp till kraven på en avancerad elektronisk underskrift.[5]

19.5.2 Behov av gemensamma insatser för att underlätta gränsöverskridande användning av elektroniska underskrifter och stämplar

Utredningen föreslår:
att regeringen ger digitaliseringsmyndigheten i uppdrag att specificera, tillhandahålla eller upphandla en gemensam valideringstjänst för att statliga myndigheter, kommuner och landsting ska kunna validera elektroniska underskrifter från andra länder.
att regeringen tillsätter en utredning som ser över behovet av svensk reglering av betrodda tjänster som inte är kvalificerade.

Skyldigheten att erkänna elektroniska underskrifter och stämplar från andra medlemsstater innebär ett behov för svenska tillhanda-

[5] Jfr Högsta domstolens dom den 22 december 2017 i mål T435-17, som rörde bevisbördan i tvistemål för invändning om att en elektronisk underskrift använts obehörigen av annan än innehavaren. Tvisten gällde en elektronisk låneförbindelse. Högsta domstolen bedömde att det var långivaren som måste visa att det är den påstådda elektroniska underskriften som har använts och att, om så sker innehavaren måste göra antagligt att användningen av underskriften skett obehörigen.

hållare av e-tjänster att kunna validera elektroniska underskrifter från andra medlemsländer. Det är svårt och betungande för varje statlig myndighet, kommun och landsting att själv upphandla den nödvändiga funktionaliteten som krävs för att ta emot elektroniska underskrifter och stämplar från andra länder.

Detta innebär att en samlad valideringstjänst bör införas enligt utredningens mening eller åtminstone upphandlas centralt för nyttjande av den offentliga förvaltningen. En sådan tjänst kan validera elektroniska underskrifter från de andra medlemsländerna.

I den enkät som utredningen skickade till andra medlemsstater (se avsnitt 17.3.4) ingick frågan om de har en valideringstjänst för elektroniska underskrifter. Det finns åtskilliga exempel på sådana valideringstjänster.

Danmark har en central tjänst som kan erkänna utländska elektroniska underskrifter (Kvikskranken).

Finland har ingen gemensam valideringstjänst men kommer att behöva överväga det om offentliga myndigheter börjar använda elektroniska underskriftstjänster. Väldigt få offentliga tjänster i Finland kräver elektroniska underskrifter enligt lag.

Nederländerna har implementerat en valideringstjänst för elektroniska underskrifter. Nederländerna accepterar alla utländska avancerade e-underskrifter baserade på vissa specificerade format.

Österrike har en valideringstjänst på följande webbplats: www.signature-verification.gv.at

Digitaliseringsmyndigheten bör få i uppdrag att specificera och tillhandahålla eller upphandla en sådan valideringstjänst. En sådan valideringstjänst kan komma att utvecklas till ytterligare en förvaltningsgemensam digital funktion enligt vad som tidigare har beskrivits.

En annan insats som identifierats under arbetets gång är att tydliggöra vilka krav på avancerade elektroniska underskrifter som behövs för att de kunna användas i svenska e-tjänster. I dag fastställs säkerhetsnivån i avtal mellan en tillhandahållare av en betrodd tjänst och den som tillhandahåller en e-tjänst eller tar emot elektroniska underskrifter.

Det smidigaste sättet att ta emot underskriven handling är i ett synkront flöde där man som mottagare själv kan sätta kraven och parametrarna på den ingående underskriften. När en organisation eller offentlig myndighet önskar att själva översända underskrivna handlingar till en annan offentlig myndighet så uppstår ett problem i

att båda inte kan styra över underskriftens format. Det kan endast antingen avsändare eller mottagare göra. Om det finns en gemensam nationell överenskommen standard för hur sådana underskrifter skapas och valideras så förenklas flödet betydligt. Det kommer dock alltid att finnas fall där en offentlig myndighet behöver ta emot en underskriven handling från utfärdare som inte följer en sådan standard eller kan valideras genom ”trusted list”. Samma problem uppstår när en individ i ett annat land skriver under en handling med ett avancerat certifikat utfärdat av en betrodd tjänst med säte i ett annat land och översänder den till en offentlig myndighet nationellt. Den offentliga myndigheten är enligt förordningen skyldig att ta emot handlingen och validera den om det finns en kostnadsfri tjänst eller mjukvara för validering.

Förordningens krav på kvalificerade certifikat är omfattande och tydliga. Kraven på certifikat som inte är kvalificerade är otydliga vilket innebär en svårighet för en mottagare av en avancerad elektronisk underskrift att avgöra vilken kvalitet och säkerhet som en sådan underskrift har, t.ex. hur väl identifierad undertecknaren är.

Om en nationell säkerhetsnivå fastställs i regelverk så underlättar det såväl möjligheten att avgöra vilka underskrifter som godtas i offentliga e-tjänster nationellt som vilka tjänster som kan godtas internationellt. Kraven på elektroniska underskrifter bör samordnas med kraven på elektronisk identifiering och på ett motsvarande sätt med tillitsramverk genom lagstiftning med övergripande krav, samt förordning med mandat att utfärda föreskrifter. Sådana krav skulle kunna innefatta:

– Kontroll av identiteten hos den till vilken ett certifikat utfärdas,
– Personalens utbildning och kunskaper, och
– Teknisk säkerhet och tillförlitlighet hos system.

Behovet och innehållet av en sådan reglering behöver utredas vidare.

20 Framtida användning av elektroniska identitetshandlingar inom Europa

Utredningen bedömer:
att Sverige bör ha en hög ambitionsnivå för användningen av elektroniska identitetshandlingar och betrodda tjänster.
att digitaliseringsmyndigheten bör prioritera deltagande i samarbetsnätverket för elektroniska identitetshandlingar och sakkunnigbedömningar.

Utredningen föreslår:
att regeringen ger uppdrag till offentliga myndigheter som har särskilt frekventa ärenden rörande nordiska medborgare att delta i och stödja samarbetsprojekt med motsvarande offentliga myndigheter i de nordiska och baltiska länderna.
att Skatteverket får i uppdrag att inrätta ett svenskt register över säkerställda kopplingar mellan europeiska elektroniska identitetshandlingar och svenska personnummer enligt det av Skatteverket tidigare lämnade förslaget.

20.1 Hög ambitionsnivå för användningen av europeiska elektroniska identitetshandlingar och betrodda tjänster

Under det estniska ordförandeskapet i ministerrådet hösten 2017 genomfördes två ministerkonferenser i Tallinn med inriktning på digital utveckling. Detta resulterade i två ministerdeklarationer.

Den 5 oktober 2017 skrev ansvariga ministrar i Armenien, Azerbadjan, Vitryssland, Georgien, Moldavien, Ukraina och EU under en gemensam deklaration. Den innehåller bl.a. mål för regler för elektronisk kommunikation och infrastruktur, tillit och säkerhet i den digitala ekonomin, eHandel inklusive tull- och transportfrågor, digital kompetens, ICT innovation och startups ekosystem, eHälsa samt EU-stöd för harmonisering av digitala marknader. Flera av de angivna målsättningarna ska uppnås till år 2020.[1]

Den 6 oktober 2017 skrev ansvariga ministrar i alla medlemsstater i EU och EFTA under en ministerdeklaration för att nå visionen och levandegöra principerna i EU:s eGovernment handlingsplan 2016–2020. Inom de närmsta fem åren ska länderna arbeta för ett antal mål inom den offentliga verksamheten. Ett av dessa innebär att öka användningen av elektroniska identitetshandlingar. Medlemsländerna förklarar sig villiga att vidta åtgärder så att eIDAS -förordningen kan genomföras vid utsatt tidpunkt och får spridd tillämpning, bland annat genom att anmäla elektroniska identitetshandlingar till kommissionen. Vidare vill medlemsstaterna verka för bred användning av betrodda tjänster hos dess myndigheter och att möjliggöra privatsektors användning av elektroniska identitetshandlingar och betrodda tjänster. Kommissionen uppmanas att verka för att europeiska elektroniska identitetshandlingar ska erkännas även utanför Europa samt att fortsätta stödja utvecklingen och användningen av standards inom ramen för eIDAS-förordningen.[2]

Även om ministerdeklarationer inte har en bindande verkan så finns det starka skäl för Sverige att ta fasta på de möjligheter som ges av ett förverkligande av syftena bakom eIDAS-förordningen. Det ger möjlighet till bättre service medlemsstaternas offentliga myndigheter och det medför att svenska offentliga myndigheter kan ge en bättre och mer kostnadseffektiv service till såväl utländska medborgare som till svenskar bosatta utomlands. Vidare kan ökat erkännande av elektroniska identitetshandlingar och betrodda tjänster skapa möjligheter för svenska företag att utveckla tjänster och produkter.

[1] https://ec.europa.eu/digital-single-market/en/news/second-eastern-partnership-ministerial-meeting-digital-economy, 2017-10-09.
[2] https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration, 2017-11-27.

20.2 Sverige bör prioritera deltagandet i nätverk och sakkunnigbedömningar

Kommissionen har i ett särskilt genomförandebeslut[3] etablerat ett nätverk för samarbete med syfte att vara ett forum för informationsutbyte, med kapacitet att yttra sig över anmälningar och utarbeta riktlinjer för sakkunnighetsbedömningar. Deltagande i nätverket är obligatoriskt för medlemsstaterna.

Samma beslut reglerar närmare hur sakkunnighetsbedömningarna ska gå till. Sakkunnighetsbedömningarna ska inte bara vara en grund för ömsesidigt erkännande. De ska också enligt beslutet ses som en möjlighet till gemensamt lärande. Deltagandet i bedömningarna är dock frivilligt.

Utredningen bedömer det som angeläget att Sverige prioriterar deltagande i sakkunnighetsbedömningarna. Det ger en möjlighet till insyn i andra länders system för elektroniska identitetshandlingar, vilket ger en grund för tillit eller för att framföra befogade invändningar. Sveriges ambitionsnivå bör, enligt utredningen, vara att utnyttja fördelarna med den inre digitala marknaden fullt ut. Då är det viktigt att svenska offentliga myndigheter befinner sig i fronten på utvecklingen. Det bidrar till att höja kompetensnivån hos de offentliga myndigheterna. Vidare ger det bättre förutsättningar för att via nätverket påverka hur bedömningarna görs. Utredningen föreslår i kapitel 18 att Sverige ska ha ett öppet system för anmälan. Det innebär att det i ett lite längre perspektiv kan finnas mer än en svensk elektronisk identitetshandling anmäld. Andra länder kan i så fall uppleva detta som att Sverige ianspråktar en oproportionellt stor del av deras resurser för bedömningar. Eftersom Sverige även har ett öppet system för kvalitetsgranskning av elektroniska identitetshandlingar kommer Sveriges process för anmälan att skilja sig från många övriga länders. Ett aktivt deltagande i samarbetsnätverk torde bidra till att höja acceptansen för den svenska modellen.

[3] Kommissionens genomförandebeslut (EU) 2015/296 av den 24 februari 2015 om inrättande av förfaranden för samarbete mellan medlemsstaterna om elektronisk identifiering i enlighet med artikel 12.7 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden.

20.3 Norden och Baltikum först

Att öppna offentliga myndigheters e-tjänster för andra länders medborgare är ett på många sätt komplicerat åtagande. Det handlar inte bara om att tekniskt bekräfta ett annat lands elektroniska identitetshandling. Det måste också kunna fastställas, som tidigare anförts, om den som vill identifiera sig för inloggning får använda e-tjänsten. Vidare måste det finnas sådana uppgifter som gör att identiteten kan matchas mot de uppgifter som redan finns i systemet.

För att kunna dra nytta av de möjligheter eIDAS-förordningen erbjuder måste etableras ett djupare samarbete mellan olika länder. Eftersom förändringar av de aktuella systemen kan vara både tids- och kostnadskrävande finns det skäl att låta några principer vägleda arbetet. Det är därför rimligt att sträva efter gemensam nytta. Samarbete med andra länder bör i första hand gälla:

- Länder som har identitetsbeteckningar som liknar det svenska personnumret i utformning och persistens.
- Länder som har anmält eller avser att anmäla ett system för elektronisk identifiering.
- Svenska e-tjänster som har använts i relativt hög omfattning av andra länders medborgare respektive andra länders e-tjänster som svenskar i stor omfattning använder.
- Vidare bör tillgängliggörandet av e-tjänster vara ömsesidigt. Sverige bör prioritera samarbete med länder som också öppnar sina e-tjänster för svenskar.

Den 25 april 2017 i Oslo skrev Nordiska Rådets ministrar med ansvar för olika delar av digitaliseringen i Norge, Sverige, Danmark, Finland, Island, Färöarna, Estland, Lettland och Litauen under en deklaration för att göra den nordisk-baltiska regionen till en digital föregångare. Deklarationen har tre mål:

1. Att stärka möjligheterna till digitalisering av offentlig verksamhet och samhället i övrigt, särskilt genom att skapa gemenskap genom offentliga gränsöverskridande digitala tjänster.

2. Att stärka konkurrenskraften hos företagen genom digitalisering.
3. Uppmuntra den gemensamma digitala marknaden i den nordisk-baltiska regionen.

Under varje mål finns närmare specifikationer om vad målen innebär. Det första delmålet innebär att det ska etableras ett närmare samarbete mellan de berörda ländernas myndigheter med syfte att möjliggöra gränsöverskridande e-tjänster. Som en del av detta ska landsöverskridande användning av identitetsbeteckningar möjliggöras. Samverkan mellan ländernas system och säker identifiering inom ramen för eIDAS-förordningen ska också stödjas. Ministrarna uttalar sig även för ökad nordisk-baltisk samverkan i frågor om lagstiftning och nationell implementering som gäller Europas digitala inre marknad.

Ministrarna uppmanar Nordiska ministerrådets sekretariat att upprätta en plan för att ta fram relevanta initiativ och projekt för att uppnå målen. För att uppnå effektivitet i arbetet förordar man att arbetet drivs decentraliserat genom att ansvaret för olika frågor delas upp mellan länderna.[4]

De nordiska samarbetsministrarna beslutade den 22 juni 2017 att upprätta ett tillfälligt ministerråd för digitalisering (MR-DIGITAL) för perioden 2017–2020. Detta ministerråd består av en minister från varje nordiskt land samt en från Grönland, Färöarna respektive Åland. Ministerrådet kommer att sammanträda 1–2 gånger per år. De baltiska länderna kommer så långt som möjligt att bjudas in till samarbetet som deltagare i sammanträdena och som partner i gemensamma projekt. Varje medlemsland har utsett en hög representant som ska representera landet på tjänstemannanivå. En handlingsplan har tagits fram för att förverkliga målen i ministerdeklarationen. Planen sträcker sig från januari 2018 till juli 2020. Ansvaret för planen har fördelats på olika länder och aktörer. Norska DIFI har i uppdrag att samordna arbetet med elektroniska identitetshandlingar och eIDAS-förordningen med stöd av referensgrupp. I ett första steg ska e-tjänster som är lämpade för samarbete identifieras. Avsikten är att

[4] www.norden.org/en/nordic-council-of-ministers/council-of-ministers/nordic-council-of-ministers-for-digitalisation-mr-digital/declarations/the-nordic-baltic-region-a-digital-frontrunner, 2017-11-27.

göra en gemensam nordisk ansökan om EU-stöd för utvecklingsinsatserna.

Sverige kommer 2018 att ha ordförandeskapet i Nordiska ministerrådet och har ställt samman ett program som innehåller beskrivningar av de ämnen och punkter som ska behandlas under ordförandeskapet.[5]

Utredningen bedömer att det finns goda förutsättningar för samarbete mellan de nordiska och baltiska myndigheterna. Även om myndighetsstrukturen och styrningsmodellerna skiljer sig åt länderna emellan så finns det stora likheter i synen på vad som ska vara ett offentligt åtagande och kunskap om hur de andra länderna arbetar.

Det är viktigt att de goda intentionerna omsätts i konkreta resultat och att respektive lands regering ger särskilda uppdrag till berörda myndigheter att delta i samarbetet.

20.4 Kopplingsregister en viktig förutsättning

Utredningen har i avsnitt 17.1.3 beskrivit Skatteverkets förslag om ett centralt kopplingsregister. De svenska offentliga myndigheterna måste kunna lita på att det är samma individ bakom en utländsk elektronisk identitetshandling som bakom ett svenskt personnummer. Annars bör utländska användare inte ges tillträde till e-tjänster som kräver viss säkerhetsnivå.

Enligt Skatteverkets förslag ska den svenska noden kunna förmedla till den offentliga myndigheten om koppling finns eller inte. För att få en koppling registrerad ska det krävas samma grad av säkerhet som vid utfärdandet av en fysisk identitetshandling. Det innebär enligt Skatteverket att koppling kan registreras först efter noggrann kontroll som kan genomföras på tre sätt.

För att få till stånd en elektronisk lösning kan Sverige i bilaterala avtal komma överens med främst de andra nordiska länderna om att den elektroniska identitetshandlingen ska innehålla personnummer eller motsvarande som kan jämföras med redan registrerade uppgifter i folkbokföringsdatabasen. Ett alternativt sätt som också ger en elektronisk lösning är att användaren först loggar in med en redan

[5] Nordiska ministerrådets skrift, Ett inkluderande, innovativt och tryggt Norden, Sveriges ordförandeskap 2018.

registrerad elektronisk identitetshandling och därefter kopplar ytterligare en elektronisk identitetshandling till sitt personnummer eller styrkta samordningsnummer. För de användare som inte kan få en koppling registrerad elektroniskt finns slutligen alternativet att användaren inställer sig fysiskt för identitetskontroll hos en registrerande myndighet.

Den första varianten med bilaterala avtal är det som samarbetet inom Nordiska ministerrådet kan förväntas leda till.

För att arbetet med kopplingsregister ska ta fart föreslår utredningen att Skatteverket får i uppdrag att inrätta ett kopplingsregister med utgångspunkt i det förslag som lämnades i rapporten 2016.[6]

Med anledning av de brister i samordningsnummersystemet som redogjorts för i avsnitt 17.5 anser utredningen att kopplingsregistret till att börja med endast ska omfatta kopplingar mellan utländska elektroniska identitetshandlingar och svenska personnummer.

[6] Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer, Skatteverkets promemoria från den 24 oktober 2016, dnr. 131 184020-16/113.

21 En lag om infrastruktur för digital post

Utredningen föreslår:
en lag om infrastruktur för digital post som ska reglera de nuvarande informationsflödena i infrastrukturen samt det som kan väntas uppstå av att infrastrukturen öppnas upp för fler användare.

Förslaget genomförs genom lagen om infrastruktur för digital post.

I stället för den förordning som utredningen föreslog i delbetänkandet föreslår utredningen nu en lag om infrastruktur för digital post (Mina meddelanden). Skälen för detta behandlas nedan. Sammanfattningsvis handlar det om att utredningen nu föreslår att öppna upp infrastrukturen för privata aktörer som avsändare samt att personuppgiftsansvaret i Mina meddelanden bör regleras i en lag.

21.1 Utredningens tidigare överväganden och förslag

I delbetänkandet föreslog utredningen att en ny förordning skulle införas för att i den samla det regelverk som behövs för infrastrukturen Mina meddelanden.

I delbetänkandet bedömde utredningen att den nuvarande regleringen av Mina meddelanden är otillfredsställande på flera plan.[1] Det författningsstöd som finns för Mina meddelanden i dag utgörs av 5 § förordningen om statliga myndigheters elektroniska informationsutbyte.[2] Där sägs egentligen bara att Skatteverket ska tillhandahålla

[1] SOU 2017:23, digitalforvaltning.nu, s. 190 f.
[2] Förordningen (2003:770) om statliga myndigheters informationsutbyte.

en infrastruktur för säker elektronisk post från myndigheter till enskilda, vilka som får ansluta sig som avsändare och mottagare samt att Skatteverket får föra register över de anslutna och i vilket ändamål personuppgifter i registret får behandlas. Skatteverket får även föreskriftsrätt för inrättande och drift av strukturen. Enligt utredningens mening är denna reglering otillräcklig.

Erfarenheter under uppbyggnaden av funktionen Mina meddelanden pekar på ett behov av förtydliganden på flera punkter. Vissa delar i infrastrukturen behöver, enligt utredningen, ett tydligare författningsstöd. Det faktum att övriga bestämmelser i den nuvarande förordningen avser elektroniskt informationsutbyte mellan statliga myndigheter talade också för det.[3]

Den tillkommande regleringen, enligt utredningens förslag i delbetänkandet, var så pass omfattande att det var lämpligt att reglera detta i en egen författning. Utredningen föreslog därför en ny förordning om en infrastruktur för säkra elektroniska försändelser. I förslaget förtydligades bl.a. hur långt personuppgiftsansvaret sträcker sig för avsändaren och vilka befogenheter brevlådeoperatörerna[4] har i Mina meddelanden. Förslagen var inte menade att ändra på några av de förutsättningar som ges inom ramen för den befintliga regleringen i, eller i de nu gällande allmänna villkoren för Mina meddelanden. Avsikten var i stället att tydliggöra det som inte regleras i paragrafen i dag, genom att utöka den till en egen förordning och lägga till de regler som behövs.

När det gäller personuppgiftsbehandlingen resonerade utredningen enligt följande.[5] Dataskyddsförordningen medger enligt artikel 4.8 att den personuppgiftsansvarige, eller de särskilda kriterierna för hur denne ska utses, kan föreskrivas i svensk nationell rätt.

Enligt regeringsformen[6] är var och en gentemot det allmänna – utan samtycke – skyddad mot betydande intrång i den personliga integriteten som innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet, enligt denna bestämmelse, kan begränsas endast enligt den särskilda ordning som föreskrivs i regeringsformen.[7]

[3] Förordningen (2003:770) om statliga myndigheters informationsutbyte.
[4] Numera benämnda leverantörer av brevlådetjänster för digital post.
[5] SOU 2017:23, digitalforvaltning.nu, s. 213 ff.
[6] 2 kap. 6 § andra stycket regeringsformen (1974:152).
[7] 2 kap. 20–22 §§ regeringsformen (1974:152).

Bestämmelsen i regeringsformen[8] innebär att sådana åtgärder som föreslås ska prövas mot grundlagen och regleras i lag. Det är endast tillåtet med lagar som inskränker integritetsskyddet om det intresse som ska tillgodoses är så starkt och integritetsskyddsintresset så förhållandevis svagt att inskränkningen framstår som proportionerlig. Bestämmelsen innebär också att lagstiftaren tydligt måste redovisa vilka avvägningar som gjorts vid proportionalitetsbedömningen.[9]

Utredningen anförde att en anslutning som mottagare till Mina meddelanden inte innebär ett betydande intrång i den personliga integriteten, eftersom en sådan anslutning enligt förslaget även fortsättningsvis ska vara frivillig. Ingen kommer att anslutas som mottagare utan samtycke. Det innebär inte heller övervakning eller kartläggning av individens förhållanden utan att någon först har brutit mot gällande regler.

Av ovanstående drog utredningen slutsatsen att det skulle räcka att reglera Mina meddelanden i en egen förordning. Efter att delbetänkandet lämnades har en rad utredningar[10] behandlat följder av och anpassningar till dataskyddsförordningen. Kunskapen om det nya regelverket har ökat och det har påpekats i remissvar[11] över delbetänkandet att en förordning inte är tillräcklig för den reglering som behövs av Mina meddelanden.

Utredningen har tagit fasta på de synpunkter om lagreglering framför förordningsreglering som framförts i remissvaren. Dessa ligger väl i linje med de behov som utredningen under hela utredningstiden har ansett finnas för en ny, fristående författning. Därför föreslår utredningen nu en lag om infrastruktur för digital post.

Enligt direktiven[12] skulle utredningen i delbetänkandet lämna förslag om hur privata utförare av offentligfinansierad verksamhet skulle kunna ansluta som avsändare inom Mina meddelanden. Utredningen fann det i delbetänkandet komplicerat att formulera ett förslag bland annat mot bakgrund av svårigheter att definiera vilka företag som

[8] 2 kap. 6 § andra stycket regeringsformen (1974:152).
[9] Datainspektionens Vägledning för integritetsanalys, september 2016, s. 32.
[10] Se t.ex. SOU 2017:39, Ny dataskyddslag Kompletterande bestämmelser till EU:s dataskyddsförordning, SOU 2017 :49, EU:s dataskyddsförordning och utbildningsväsendet, SOU 2017:50, Personuppgiftsbehandling för forskningsändamål, SOU 2017:66, Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning, Ds 2017:19, Ds 2017:33, Ds 2017:41.
[11] Datainspektionens yttrande den 5 juli 2017, dnr. 702-2017.
[12] Dir. 2016:39, s. 13.

skulle anses vara privata utförare samt hur rätten att ansluta skulle avgränsas.

Utredningen gör nu en förnyad bedömning och finner att privata utförare kan ansluta genom anmälan av berörda kommuner och landsting. Eftersom detta medför vissa skyldigheter för kommunen och landstinget måste bestämmelserna även av detta skäl regleras i lag.

21.2 Definitioner och bestämmelser

Utredningen föreslår:
att lagen ska innehålla bestämmelser om informationsflödet i infrastrukturen samt definitioner.

Den myndighet som regeringen utser ska tillhandahålla en infrastruktur för digital post. I enlighet med vad utredningen föreslog i delbetänkandet föreslår utredningen nu att Skatteverket under ytterligare en period ska ansvara för Mina meddelanden. Därefter ska ansvaret tas över av digitaliseringsmyndigheten.[13]

Lagen ska innehålla en paragraf om definitioner av en rad centrala begrepp i infrastrukturen. De begrepp som definieras är:

1. *ankomstkontroll:* att leverantören av brevlådetjänster för digital post utför kontroll mot förmedlingsadressregistret att avsändaren är ansluten.
2. *avsändare:* offentlig myndighet eller en juridisk person som genom avsändningskontroll skickar digital post till en mottagare inom infrastrukturen.
3. *avsändningskontroll:* att avsändaren utför kontroll mot förmedlingsadressregistret att mottagaren är ansluten till infrastrukturen, i så fall hos vilken leverantör mottagarens brevlådetjänst för digital post finns samt att avsändaren får sända digital post till mottagaren.

[13] Kommittédirektiv för inrättande av en myndighet för digitalisering av den offentliga sektorn, Dir. 2017:117, s. 7.

4. *brevlådetjänster för digital post:* den del inom infrastrukturen som lagrar digital post efter att den har gjorts tillgänglig för mottagaren.
5. *digital post:* meddelanden genom digitala kanaler mellan olika aktörer i infrastrukturen.
6. *förmedlare:* en fysisk eller juridisk person som utför uppdrag åt en avsändare genom att vidarebefordra digital post.
7. *förmedlingsadressregister:* det register som innehåller uppgifter, däribland personuppgifter, om de anslutna i infrastrukturen.
8. *leverantör av brevlådetjänster för digital post:* en juridisk person eller en individ som tillhandahåller brevlådetjänster för digital post.
9. *mottagare:* individer och företag som anslutit sig till förmedlingsadressregistret som mottagare och i sin brevlådetjänst för digital post tar emot digital post inom infrastrukturen.
10. *privat utförare:* en juridisk person eller en individ som har hand om en kommunal angelägenhet.

Utredningen föreslår även att lagen ska innehålla en bestämmelse om vad som ingår i infrastrukturen: förmedlingsadressregister, brevlådetjänster för digital post samt föreskrifter.

21.3 Min myndighetspost

Utredningen föreslår:
att den myndighet som regeringen bestämmer ska tillhandahålla brevlådetjänster för digital post till mottagare som enbart tar emot digital post från avsändare som är anslutna till Mina meddelanden.

Uppdraget att tillhandahålla brevlådetjänsten Min myndighetspost är i dag inte reglerat i författning, något som utredningen i delbetänkandet föreslog skulle åtgärdas genom reglering i förslaget till förordning om infrastruktur för säkra elektroniska försändelser. Utredningen föreslår nu att denna statliga brevlådetjänst i stället ska regleras i lagen om infrastruktur för digital post.

21.4 Att underlåta att skicka försändelsen digitalt via Mina meddelanden ska kräva särskilda skäl

Utredningen föreslår:
att mottagare, om de begärt det, har rätt att få digital post från statliga myndigheter om det inte finns särskilda skäl för undantag.

Regeln innebär att individer och företag, om de begärt det, har rätt att som mottagare få digital post från statliga myndigheter om det inte finns särskilda skäl för undantag. Sådana särskilda skäl kan t.ex. vara att den statliga myndigheten bedömer att man inte kan ta sitt personuppgiftsansvar eller att den statliga myndighetens verksamhetskaraktär är olämplig för att använda digital post i det enskilda fallet. Förslaget innebär att det skulle vara en rättighet för alla mottagare att få sin post från statliga myndigheter digitalt genom Mina meddelanden. Förslaget lämnades även i delbetänkandet men utredningen föreslår nu att regeln ska ingå i lagen om infrastruktur för digital post.

21.5 Förhållandet till dataskyddsreglering

Utredningen föreslår:
att en upplysningsbestämmelse om dataskyddsförordningen och den föreslagna dataskyddslagen ska finnas i den föreslagna lagen om infrastruktur för digital post. Dataskyddslagen föreslås vara subsidiär till lagen om infrastruktur för digital post.

När dataskyddsförordningen börjar tillämpas kommer den att vara direkt tillämplig på all personuppgiftsbehandling inom dess materiella och territoriella tillämpningsområde i medlemsstaterna. Dataskyddsförordningens bestämmelser kommer därmed att gälla för Mina meddelanden oberoende av om förhållandet till förordningen regleras i lagen om infrastruktur för digital post. För att underlätta för de som ska tillämpa lagen anser utredningen att det bör införas en upplysningsbestämmelse i lagen om infrastruktur för digital post som klargör att lagen innehåller kompletterande bestämmelser till dataskyddsförordningen.

Till skillnad från dataskyddsförordningen kommer dataskyddslagen att vara subsidiär till lagen, vilket också framgår av 1 kap. 3 § i Dataskyddsutredningens författningsförslag.[14]

Det kan noteras att några av leverantörerna av brevlådetjänster för digital post redan i dag tillåter företag som avsändare, dvs. sådana företag som inte omfattas av kretsen i den föreslagna 11 § lagen om infrastruktur för digital post. Dessa företag är inte anslutna till infrastrukturen Mina meddelanden, utan skickar digital post ”vid sidan” med stöd av ett civilrättsligt avtal. Denna digitala post träffas inte av den föreslagna lagen om infrastruktur för digital post. I stället tillämpas dataskyddsförordningen och dataskyddslagen i sådana situationer fullt ut. Dessa leverantörer av brevlådetjänster för digital post behöver därmed ha allmänna villkor för de anslutna som tar utgångspunkt i detta.

21.6 Rättslig grund för personuppgiftsbehandlingar

Infrastrukturen Mina meddelanden bygger på att en rad aktörer i en viss ordning behandlar individers personuppgifter i en förhållandevis stor omfattning. Det är viktigt att klargöra den rättsliga grunden för dessa behandlingar.

Innan avsändaren skickar post kontrollerar avsändaren i förmedlingsadressregistret om mottagaren är ansluten till infrastrukturen. Om mottagaren är ansluten sänds en bekräftelse om detta tillbaka till avsändaren. En sådan bekräftelse är en allmän handling om den skickas från en statlig eller kommunal myndighet. Om mottagaren inte är ansluten kommer det inget svar alls och avsändaren får då skicka fysisk post i stället.

Detta betyder att slagningar görs av avsändare på i stort sett hela Sveriges befolkning fastän de inte har anmält sig till infrastrukturen Mina meddelanden eller vill registreras i förmedlingsadressregistret.

Frågan är vilken rättslig grund som gäller för dessa slagningar och för övrig personuppgiftsbehandling i infrastrukturen.

[14] SOU 2017:39 s. 83 ff.

21.6.1 Rekvisitet nödvändig

Enligt artikel 6.1 i dataskyddsförordningen får personuppgifter endast behandlas om någon av de rättsliga grunder som räknas upp i artikeln gäller. Enligt denna bestämmelse är personuppgiftsbehandling tillåten om den är *nödvändig* för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Personuppgiftsbehandling är även tillåten om den är *nödvändig* för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige är skyldig att göra. Detta framgår av artikel 6.1 c i förordningen.

Dataskyddsutredningen konstaterar i sitt betänkande att det unionsrättsliga begreppet *nödvändig* inte har samma strikta innebörd som i svenska språket.[15] Även om exempelvis en uppgift av allmänt intresse hade kunnat utföras utan behandling av personuppgifter, kan behandlingen ur ett unionsrättsligt perspektiv anses vara nödvändig och därmed tillåten enligt artikel 6 i dataskyddsförordningen om den leder till effektivitetsvinster.[16]

Det står enligt utredningen klart att personuppgiftsbehandlingen i infrastrukturen Mina meddelanden kan bedömas som nödvändig eftersom den bidrar till en stor effektivitetsvinst för offentliga myndigheter och individer.

För de som själva har anmält sig som mottagare till Mina meddelanden bedömer utredningen att personuppgiftsbehandlingarna är laglig enligt flera av leden som anges i artikel 6.1 i dataskyddsförordningen.

21.6.2 Samtycke som rättslig grund

Enligt artikel 6.1 a) i dataskyddsförordningen ska den registrerade ha lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål. Genom att frivilligt ansluta sig som mottagare till Mina meddelanden anser utredningen att mottagaren får anses ha lämnat sitt samtycke till den behandling som behöver ut-

[15] SOU 2017:39 s. 105 f.
[16] Datalagskommitténs betänkande SOU 1997:39 s. 359, EU-domstolens dom den 16 december 2008 i mål nr C-524/06, och den 19 juni 2014 i mål nr C-683/13.

föras med mottagarens personuppgifter för att hon eller han ska kunna få sin post på elektronisk väg.

21.6.3 Rättslig förpliktelse som rättslig grund

Enligt artikel 6.1 c) i dataskyddsförordningen ska behandlingen vara nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige är skyldig att utföra.

I Sverige följer det av regeringsformen att den offentliga makten utövas under lagarna.[17] Offentligrättsliga förelägganden och beslut som medför förpliktelser för mottagaren ska därför ha sin grund i en författning. Förpliktelser som har en generell räckvidd, och alltså inte riktas mot en specifik mottagare, ska också regleras i författning. Detta gäller både offentligrättsliga och civilrättsligaskyldigheter.[18]

Dataskyddsutredningen gör dock bedömningen att det faktum att den rättsliga förpliktelsen måste ha en legal grund inte innebär att förpliktelsen nödvändigtvis måste framgå av en författning eller liknande. Rättsliga förpliktelser kan också framgå av exempelvis förelägganden, myndighetsbeslut och domar som har meddelats med stöd av gällande rätt. Avtalsrättsliga förpliktelser som rättslig grund för personuppgiftsbehandling regleras dock i artikel 6.1 b i dataskyddsförordningen och ligger således utanför begreppet rättslig förpliktelse.[19]

Genom utredningens förslag om en lag om infrastruktur för digital post införs tydligare rättsliga förpliktelser för den personuppgiftsansvarige (avsändaren i det här fallet) att fullgöra sina rättsliga förpliktelser. Avsändaren ska enligt 16 § i lagen kontrollera i förmedlingsadressregistret om mottagaren är ansluten till infrastrukturen. Utredningen föreslår också i 7 § en rättighet att få sin post digitalt om man begär det.

[17] 1 kap. 1 § tredje stycket regeringsformen (1974:152).
[18] SOU 2017:39 s. 115.
[19] Dataskyddsutredningens betänkande SOU 2017:39 s. 113 f.

21.6.4 Uppgift av allmänt intresse eller myndighetsutövning som rättslig grund

Enligt artikel 6.1 e) i dataskyddsförordningen ska behandlingen vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Uppgift av allmänt intresse

Dataskyddsutredningen anser att mycket talar för att begreppet uppgift av allmänt intresse har fått en vidare unionsrättslig betydelse genom dataskyddsförordningen än det hittills har haft i svensk rätt.[20] Dataskyddsutredningen gör även bedömningen att begreppet uppgift av allmänt intresse rent språkligt kan antas avse något som är av intresse för eller berör många människor på ett bredare plan. Av skäl 45 till dataskyddsförordningen följer att allmänintresset inbegriper hälso- och sjukvårdsändamål, folkhälsa, socialt skydd och förvaltning av hälso- och sjukvårdstjänster. Dataskyddsutredningen gör också bedömningen att alla uppgifter som utförs av statliga myndigheter i syfte att uppfylla ett uttryckligt uppdrag av riksdagen eller regeringen är av allmänt intresse.[21]

Myndighetsutövning

Myndighetsutövning är ytterst ett uttryck för samhällets maktbefogenheter i förhållande till individer. Befogenheten till myndighetsutövning måste vara grundad på lag eller annan författning eller på annat sätt kunna härledas ur bemyndiganden från de högsta statsorganen. Till myndighetsutövning hör först och främst sådan offentlig verksamhet, varigenom myndigheterna ensidigt bestämmer om enskildas skyldigheter eller om ingrepp i enskildas frihet eller egendom. Hit hör alltså beslut som innebär skyldigheter att göra eller avstå från något eller som avser ingrepp i personlig frihet eller egendom, men även rent faktiska åtgärder som innebär sådana ingrepp, vare sig de grundas på formella beslut eller inte. Så långt kan begrep-

[20] Dataskyddsutredningens betänkande SOU 2017:39 s. 122 f.
[21] A.a. s. 124.

pet myndighetsutövning sägas sammanfalla med begreppet offentlig maktutövning.

21.6.5 Bedömning av rättslig grund

Utredningen anser att det finns stöd för att bedöma uppgift av allmänt intresse som rättslig grund för personuppgiftsbehandlingarna i Mina meddelanden eftersom infrastrukturen Mina meddelanden har införts som en service som kan sägas vara av allmänt intresse. Viss post från myndigheter kan vara en del av myndighetsutövning gentemot individen. Att posten skickas digitalt medför enligt utredningen inte någon annan bedömning. Det finns därför stöd även för att bedöma myndighetsutövning som rättslig grund. Att mottagarna har samtyckt till att ansluta sig till Mina meddelanden är också rättslig grund för laglig personuppgiftsbehandling.

Det finns således enligt utredningens mening rättslig grund i dessa tre led för de behandlingarna av personuppgifter i Mina meddelanden när det gäller individer som själva har anslutit sig till infrastrukturen.

När det gäller slagning i förmedlingsadressregistret på individer som inte är anslutna till Mina meddelanden kan inte den rättsliga grunden i artikel 6.1 a) om samtycke användas. Däremot borde samma principer om rättslig grund enligt artiklarna 6.1 c) om rättslig förpliktelse och e) om allmänt intresse eller myndighetsutövning kunna gälla som rättslig grund för sådan behandling av personuppgifter.

21.7 Ändamål för personuppgiftsbehandling inom Mina meddelanden

Utredningen föreslår:
att de primära ändamålen för personuppgiftsbehandling inom infrastrukturen Mina meddelanden regleras. Personuppgifter i registret ska bara få behandlas om det behövs för att

1. förmedla digital post i syfte att kunna utföra en arbetsuppgift inom en författningsreglerad verksamhet hos någon av de som anslutit sig till infrastrukturen, eller

2. förvara och bearbeta digital post som avses i p. 1 i syfte att erbjuda tilläggstjänster för mottagarna.

att de sekundära ändamålen med personuppgiftsbehandling inom infrastrukturen Mina meddelanden regleras särskilt. Personuppgifter i registret som behandlas eller har behandlats enligt de primära ändamålen med registret ska även få behandlas om det behövs för att fullgöra uppgiftslämnande i överensstämmelse med lag eller förordning.

I ett enskilt fall ska personuppgifter som behandlas eller har behandlats enligt de primära ändamålen med registret även få behandlas för att tillhandahålla information för något annat ändamål än det som anges, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in.

Enligt artikel 5.1 b) i dataskyddsförordningen ska det vid behandling av personuppgifter gälla att de ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).

Utgångspunkten i lagen om infrastruktur för digital post är att personuppgifter bara ska få behandlas för vissa berättigade, särskilt angivna ändamål. Därmed kan användningen och spridningen av personuppgifterna begränsas.

Ändamålet ska vara specifikt och tydligt angivet. Den aktuella verksamheten för infrastrukturen är att förmedla digital post och ha möjlighet att lagra och bearbeta sådan post. Informationen som flödat in i infrastrukturen och behandlats där, kommer till stor del från annat håll. Informationen, ska kunna flöda igenom infrastrukturen för att den ska kunna genomföra sin verksamhet. Det finns även information om aktörerna i infrastrukturen i form av det förmedlingsadressregister som syftar till att matcha informationen som flödar genom infrastrukturen med rätt mottagare, dvs. en del i att förmedla den digitala posten.

De primära ändamålen som utredningen föreslår i 9 § i förslaget till lag om infrastruktur för digital post är utformade för att till-

godose den behandling som behövs i en sådan verksamhet. För att skilja ut och precisera vilken information som får flöda igenom infrastrukturen begränsas denna till att bara avse sådan information som från början kommer från en författningsreglerad verksamhet som ingår bland infrastrukturens aktörer. Det är bara den informationen som, tillsammans med förmedlingsadressregistret, ingår i infrastrukturens verksamhet. Utredningen bedömer t.ex. att personuppgiftsbehandlingen från handläggning av en avsändares ärende eller faktiska handläggning från början till slut kan flöda genom infrastrukturen och ingå i dess verksamhet om denna information ingår i en författningsreglerad verksamhet. Utredningen bedömer att även generella servicemeddelanden som ingår i en arbetsuppgift inom en författningsreglerad verksamhet hos en avsändare kan omfattas av infrastrukturens verksamhet. Utredningens bedömning är att detta innebär att statliga myndigheter, kommuner och landsting, i deras författningsreglerade uppdrag, träffas av ändamålens formulering utan att ramen blir alltför vid i förhållande till mängden information som kan kvalificera. Personuppgiftsbehandlingarna bedöms vara proportionerliga.

Vilken kategori av information som ska få finnas i registret är en bedömningsfråga, eftersom det bara är de personuppgiftsbehandlingar som behövs som är tillåtna. Det är därmed inte ändamålsenligt att specificera vilka kategorier av personuppgifter som kan ingå i registret. Det skulle hypotetiskt kunna variera från fall till fall.

Sekundära ändamål (10 §) reglerar i vilken utsträckning uppgifter som samlats in för något primärt ändamål får behandlas för att lämnas ut från den reglerade verksamheten till enskilda eller till andra myndigheter eller verksamheter. Uppgifterna lämnas således ut i syfte att tillgodose deras behov, dvs. trots att det inte behövs för något primärt ändamål.

Finalitetsprincipen innebär att insamlade personuppgifter inte får behandlas för något ändamål som är oförenligt med det ursprungliga ändamålet. Det finns flera möjligheter att utforma ändamålsregleringen i särskilda registerförfattningar i förhållande till finalitetsprincipen. Det går dock att urskilja två principiellt olika sätt. Det ena är att i en uttömmande uppräkning ange samtliga ändamål för vilka behandling får förekomma, både primära och sekundära. Det andra är att de i lagen angivna ändamålen kompletteras med en möjlighet att vidarebehandla personuppgifter även för ändamål som inte är oförenliga med insamlingsändamålet. Möjligheten till vidarebehand-

ling får då avgöras med tillämpning av finalitetsprincipen. I flera särskilda registerförfattningar, däribland polisdatalagen[22] och kustbevakningsdatalagen,[23] är ändamålsbestämmelserna utformade enligt det senare alternativet.[24]

Ambitionen med utredningens förslag om en lag om infrastruktur för digital post är att de tillåtna ändamålen för behandling av personuppgifter ska anges så tydligt och fullständigt som möjligt. De primära ändamålen, dvs. de ändamål för vilka den aktuella myndigheten får samla in personuppgifter för Mina meddelanden, anges därför uttömmande. En svårare fråga är om även de sekundära ändamålen – som anger när de personuppgifter som med stöd av de primära ändamålen har samlats in av myndigheten enligt ovan får lämnas ut trots att det inte behövs enligt de primära ändamålen – bör anges uttömmande.

I förarbetena till flera särskilda registerförfattningar har regeringen gjort bedömningen att det inte är möjligt att i en lag om behandling av personuppgifter på ett visst område på ett tillräckligt preciserat sätt ange alla de situationer där utlämnande av uppgifter kan komma att aktualiseras, se t.ex. propositionen Integritet och effektivitet i polisens brottsbekämpande verksamhet[25] och propositionen Kustbevakningsdatalag.[26]

Regeringen ansåg även i propositionen Nya möjligheter till operativt polissamarbete med andra stater[27] att de sekundära ändamålen inte skulle anges uttömmande i den nya tullbrottslagen. I ett enskilt fall bör personuppgifter som samlats in enligt de primära ändamålen även få behandlas för att tillhandahålla information för något annat ändamål än de som uttryckligen anges i lagen, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket personuppgifterna samlades in.

Det skulle kunna anföras att det i dagsläget inte finns en så varierande verksamhet för infrastrukturen Mina meddelanden att det i sig skulle utesluta möjligheten att på ett tillräckligt preciserat sätt ange

[22] SFS 2010:361. Jfr även nytt förslag om polisdatalag i SOU 2017:74 s. 418 ff. där de sekundära ändamålen fortsatt inte är uttömmande.
[23] SFS 2012:145. Se även nytt förslag om kustbevakningsdatalag i Ds 2017:58 s. 118 ff. där de primära- och sekundära ändamålsbestämmelserna behålls som de är i dag.
[24] Prop. 2011/12:45 s. 102.
[25] Prop. 2009/10:85 s. 98.
[26] Prop. 2011/12:45 s. 102.
[27] Prop. 2016/17:91 s. 88 f.

alla de situationer där utlämnande av uppgifter kan komma att aktualiseras. Å andra sidan är det, som utredningen redogjort för ovan, problematiskt att definiera infrastrukturens verksamhet. Det finns då en risk för att exkludera någon del av personuppgiftsbehandlingarna.

Utredningen föreslår därför, främst med hänsyn till hur lagstiftaren tidigare har resonerat avseende de sekundära ändamålen, att dessa inte anges uttömmande i 10 § andra stycket.

21.8 Fördelning av personuppgiftsansvar

För att underlätta för de inblandade aktörerna föreslår utredningen ett klargörande av det personuppgiftsansvar som den aktuella myndigheten har, avsändare av digital post och leverantörer av digitala brevlådetjänster. Även förmedlarens roll behöver förtydligas i detta sammanhang. Bland annat inför utredningen nya regler för att visa dels vilka slagningar som avsändare, förmedlare och leverantörer av digitala brevlådetjänster gör mot förmedlingsadressregistret, dels när en avsändares personuppgiftsansvar upphör och personuppgiftsansvaret tas över av leverantörer av digitala brevlådetjänster.

21.8.1 Avsändningskontroll

Utredningen föreslår:
att avsändare före sändning av digital post ska kontrollera i förmedlingsadressregistret om mottagaren är ansluten till infrastrukturen och i så fall hos vilken leverantör mottagarens brevlådetjänst för digital post finns samt att avsändaren får sända digital post till mottagaren. Om mottagaren inte är ansluten till infrastrukturen eller inte tar emot meddelanden från den aktuella avsändaren ska den digitala posten inte få sändas via infrastrukturen.

Avsändningskontroll innebär att avsändaren måste genomföra en kontroll i förmedlingsadressregistret för att ta reda på om mottagaren är ansluten till Mina meddelanden, hos vilken leverantör mottagaren har sin digitala brevlåda samt att avsändaren av den digitala posten får sända post till mottagaren (att mottagaren inte har spärrat post från avsändaren) för att få skicka post via infrastrukturen. Detta

är en procedur som är en teknisk förutsättning för att meddelande ska sändas och som beskrivs i Skatteverkets allmänna villkor för Mina meddelanden.[28] Det finns, enligt utredningen ett behov av att i lagen kortfattat upplysa om hur infrastrukturen fungerar.

21.8.2 Förmedlarens kontroll

Utredningen föreslår:
att förmedlare före sändning av digital post ska kontrollera i förmedlingsadressregistret om mottagaren fortfarande är ansluten till infrastrukturen och om avsändaren får sända digital post till mottagaren. Om mottagaren inte är ansluten till infrastrukturen eller inte tar emot meddelanden från den aktuella avsändaren ska den digitala posten inte få sändas via infrastrukturen.

Eftersom digital post kan sändas både av avsändaren direkt och via en förmedlare behövs det, för tydlighetens skull, särskilt regleras vad som gäller för förmedlare.

Även denna slagning utförs i de fall en förmedlare är anlitad av avsändaren för att förmedla den digitala posten. Förmedlare kontrollerar på uppdrag av avsändaren i förmedlingsadressregistret att mottagaren fortfarande är ansluten och att avsändaren får sända digital post till mottagaren.

21.8.3 Ankomstkontroll

Utredningen föreslår:
att leverantör av brevlådetjänster för digital post vid ankomst av digital post till brevlådan ska kontrollera i förmedlingsadressregistret att avsändaren fortfarande är ansluten till infrastrukturen. Om avsändaren inte är ansluten och heller inte har något civilrättsligt avtal med mottagaren om digital brevlådetjänst ska meddelandet inte tas emot.

[28] Allmänna villkor för Mina meddelanden, version 1.3, s. 9 p. 6.5.1.

Som sista steg i sändningskedjan ska leverantören av brevlådetjänster för digital post också kontrollera i förmedlingsadressregistret att avsändaren fortfarande är ansluten till infrastrukturen. Om avsändaren inte är ansluten och inte heller har något civilrättsligt avtal med mottagaren om digital brevlådetjänst, alltså har kvar samma val av brevlådetjänst, ska meddelandet inte tas emot.

Den post som kommer till mottagaren kan antingen gå via infrastrukturen Mina meddelanden eller så kan posten också gå med anledning av ett avtal som mottagaren har slutit med leverantören av digital brevlådetjänst om att mottagaren vill ha digital post från de avsändare som i sin tur har slutit avtal med leverantören. Det här gäller de individer som t.ex. anslutit sig till en privat leverantör av digital brevlådetjänst för att få post från vissa företag. Denna digitala post har inget med Mina meddelanden att göra. Detta gäller inte brevlådetjänsten Min myndighetspost som bara tar emot post via Mina meddelanden. Mottagare med digitala brevlådor från andra leverantörer än Min myndighetspost får därmed post genom två olika informationsflöden, flödet via Mina meddelanden och det avtalsrättsliga ”civila” flödet.

När det gäller det civila flödet återstår det att avgöra om det finns rättslig grund för de behandlingar av personuppgifter (slagningar i register) som behöver göras för att avgöra om post ska skickas digitalt. Om det görs slagningar på individer som inte anmält sig till en brevlådetjänst för post som kommer från t.ex. företagare är detta något som genomförs utanför infrastrukturen Mina meddelanden. Utredningen har därför inte undersökt denna fråga närmare men vill i sammanhanget belysa att det kan vara en fråga för leverantörer av digitala brevlådetjänster att se över innan dataskyddsförordningen träder i kraft i maj 2018.

21.8.4 Registermyndighetens personuppgiftsansvar

Utredningen föreslår:
att myndigheten ska vara personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför när den tillhandahåller förmedlingsadressregistret.

Med myndigheten avses för närvarande Skatteverket. Enligt utredningens förslag i delbetänkandet ska detta ansvar i framtiden flyttas till digitaliseringsmyndigheten.[29] Så länge Skatteverket ansvarar för registret ska dock Skatteverket ha personuppgiftsansvaret för all behandling av personuppgifter som utförs i registret. Detta gäller i dag redan i praktiken. Ett av syftena med EU:s dataskyddsreform är att göra det tydligare vilket ansvar och vilka skyldigheter de som behandlar personuppgifter har. Att reglera vem som har personuppgiftsansvaret bör för tydlighetens skull skrivas ut i en regel i lagtexten.

21.8.5 Avsändarens personuppgiftsansvar

Utredningen föreslår:
att avsändaren ska vara personuppgiftsansvarig för behandling av personuppgifter till dess att leverantör av brevlådetjänster för digital post genom ankomstkontroll godkänt mottagandet.
att avsändaren ska vara personuppgiftsansvarig för behandling av uppgifter som leverantören utför på avsändarens begäran efter att meddelandet gjorts tillgängligt för mottagaren.

Avsändaren av den digitala posten ska vara personuppgiftsansvarig för de personuppgifter som behandlas i meddelandet till dess att leverantören av brevlådetjänsten har godkänt mottagandet genom ankomstkontrollen beskriven ovan. När mottagandet är godkänt upphör avsändarens personuppgiftsansvar utom i de fall avsändaren har begärt någon ytterligare behandling av personuppgifter efter att meddelandet har gjorts tillgängligt för mottagaren. En sådan behandling finns inte tillgänglig i dag, men skulle i framtiden kunna avse t.ex. en fakturabetalning. Då upphör personuppgiftsansvaret för avsändaren först i ett senare skede som får avgöras i varje konkret exempel på en sådan lösning.

[29] SOU 2017:23, digitalforvaltning.nu.

21.8.6 Har förmedlaren ett personuppgiftsansvar?

Utredningen bedömer:
att förmedlaren ska vara personuppgiftsbiträde i förhållande till avsändaren. Detta förhållande bör inte regleras i den föreslagna lagen.

Förmedlaren utför också en behandling av personuppgifter genom en kontrollslagning mot förmedlingsadressregistret för att veta om mottagaren fortfarande är ansluten och att avsändaren får skicka digital post till mottagaren. Den aktuella behandlingen utförs dock på uppdrag av avsändaren. Förmedlaren kan inte heller påverka informationen eller ändra den. Förmedlaren är därmed inte självt personuppgiftsansvarig för personuppgiftsbehandlingen.

I stället är förmedlaren att anse som ett personuppgiftsbiträde som utför uppgifter på grundval av ett uppdragsavtal. Det ligger i själva definitionen av ett personuppgiftsbiträde att det är en funktion som skapas genom avtal mellan den personuppgiftsansvarige och den som ska behandla personuppgifter för den personuppgiftsansvariges räkning. Det finns även ett värde i att dokumentera instruktionerna och relationen i övrigt mellan den personuppgiftsansvarige och personuppgiftsbiträdet i det aktuella avtalet.[30]

Det har i tidigare registerförfattningar inte bedömts lämpligt att reglera rollen som personuppgiftsbiträde.[31]

21.8.7 Personuppgiftsansvaret för leverantörer av digitala brevlådetjänster

Utredningen föreslår:
att leverantör av brevlådetjänster för digital post ska vara personuppgiftsansvarig för behandling av uppgifter efter att ankomstkontroll genomförts med undantag för om avsändaren har begärt någon ytterligare behandling.

[30] Prop. 2014/15:148 s. 35 f.
[31] Prop. 2014/15:148 s. 36.

att leverantören ska vara personuppgiftsansvarig för behandling av uppgift som denne erbjuder mottagaren och som inte utförs på avsändarens begäran. Sådan behandling innefattar förvaring.

Enligt förslaget ska leverantören av brevlådetjänster vara personuppgiftsansvarig för behandling av personuppgifter efter att ankomstkontroll har genomförts. Om avsändaren har begärt någon ytterligare behandling ska avsändaren dock vara fortsatt personuppgiftsansvarig för den behandlingen (t.ex. betallösning eller liknande). Leverantören ska även vara personuppgiftsansvarig för behandling av personuppgifter som erbjuds mottagaren och som inte utförs på avsändarens begäran.

I delbetänkandet[32] föreslog utredningen att personuppgiftsansvaret i denna del skulle tas över av innehavaren av brevlådan om det var en juridisk person. Om en fysisk person är mottagare är detta dock omöjligt eftersom behandling av personuppgifter för privat bruk inte omfattas av dataskyddsförordningen.[33] Det är med dagens utformning av brevlådorna enkelt för mottagare att låta meddelandena ligga kvar i brevlådan och använda den som ett digitalt förvar eller arkiv. Detta var dock inte avsikten med brevlådetjänsterna inom ramen för Mina meddelanden som de är utformade i dag.

21.8.8 Leverantörerna av digitala brevlådetjänster behöver utveckla tjänster för förvaring och arkivering

Genom att föreslå att leverantörerna av brevlådetjänster blir personuppgiftsansvariga för behandling av personuppgifter i brevlådan hoppas utredningen att förslaget ska skynda på leverantörernas utveckling av tjänster för förvaring och arkivering av digital post. Den situation som nu råder är otillfredsställande eftersom den som juridiskt och praktiskt har möjlighet att bestämma över informationen som ligger i brevlådan inte kan ta personuppgiftsansvaret för detta. Brevlådorna innehåller mycket information om Sveriges befolkning och dess förhållande till offentliga myndigheter och andra aktörer. Det finns framför allt ingen som kan ta ett övergripande ansvar för det fall en

[32] SOU 2017:23, digitalforvaltning.nu, s. 218 ff.
[33] Art. 2.2 c) dataskyddsförordningen.

säkerhetsincident inträffar.[34] Detta är enligt utredningens bedömning inte heller något som anslutna mottagare verkar vara medvetna om.

Därför behöver, enligt utredningen, tjänster utformas, gärna direkt länkade till brevlådans inkorg, för att användaren ska kunna göra ett val att ladda ner sina meddelanden till en privat enhet eller lagra dem i en tilläggstjänst eller ett digitalt arkiv som är avsett för det med tydliga personuppgiftsbestämmelser kopplade därtill.

21.9 Mina meddelanden och privata utförare av offentligt finansierade tjänster som en del av kommunens och landstingets åtaganden

Utredningen föreslår:
att privata utförare av kommunala angelägenheter[35] ska få ansluta sig som avsändare i infrastrukturen Mina meddelanden efter anmälan av kommunen eller landstinget. En förutsättning för anmälan ska vara att kommunen eller landstinget är ansluten samt har kommit överens med utföraren att denne ska använda infrastrukturen. Kommunen eller landstinget ska kontrollera att utföraren använder infrastrukturen på avsett sätt. Om kommunen eller landstinget finner att utföraren brister härvidlag eller då uppdraget upphör ska anmälan återkallas.

Utredningen tar här upp frågan om anslutning av privata utförare av offentligt finansierade tjänster till förnyad behandling. Skälet till det är att även om den finansieringsmodell som föreslogs i delbetänkandet[36] ger likabehandling ekonomiskt så är det en viss skillnad mellan att köpa tjänster direkt av leverantörerna av digitala brevlådetjänster

[34] Jfr Datainspektionens tillsynsbeslut den 21 april 2017 mot E-Hälsomyndigheten, dnr 2276-2016. Detta beslut är i skrivandets stund överklagat till Förvaltningsrätten i Stockholm (mål 11458-17).
[35] I begreppet privata utförare av kommunala angelägenheter ingår även privata utförare av landstingens angelägenheter. Enligt 10 kap. 1 § kommunallagen (2017:725) om överlämnande av kommunala angelägenheter får fullmäktige i kommuner eller landsting, om det inte i lag eller annan författning anges att angelägenheten ska bedrivas av en kommunal nämnd, besluta att lämna över skötseln av en kommunal angelägenhet till en juridisk person eller en enskild individ. Eftersom även landsting får lämna över sådan skötsel torde det innebära att privata utförare av kommunala angelägenheter inbegriper även privata utförare av landstingens angelägenheter.
[36] SOU 2017:23, digitalforvaltning.nu, s. 229 ff.

och att utnyttja deras tjänster via infrastrukturen Mina meddelanden. Genom att använda Mina meddelanden kan en avsändare sända meddelanden till alla privatpersoner som har en digital brevlåda, även de som har brevlådan Min myndighetspost som bara tar emot post från myndigheter.

Att inte öppna infrastrukturen Mina meddelanden för privata utförare kan därför innebära att kommunernas eller landstingens medlemmar får olika service enbart beroende på att kommunerna eller landstingen, i enlighet med de möjligheter som lagstiftaren bestämt,[37] valt att organisera sin verksamhet på olika sätt. Till exempel anlitar kommuner privata utförare i olika omfattning. Den digitala infrastrukturen bör, enligt utredningens mening, vara neutral i förhållande till hur kommunerna och landstingen organiserar sin verksamhet.

En utgångspunkt för utredningens analys i delbetänkandet var också att privata utförare tänktes att på egen hand, utan att gå via kommunen eller landstinget, ta ställning till om de ville ansluta till Mina meddelanden. Därmed uppstod frågan om hur utförarens användning av infrastrukturen som avsändare skulle regleras. Skulle t.ex. även verksamheter inom företaget som inte utför uppgifter för kommunen eller landstinget få använda infrastrukturen? Det var också rimligt att anslutningen till Mina meddelanden upphörde när uppdraget upphörde, men frågan om hur det skulle hanteras i praktiken kvarstod.

Det förslag som presenteras här besvarar dessa frågor, men innebär samtidigt en viss begränsning när det gäller vilka som får ansluta sig som avsändare i infrastrukturen Mina meddelanden.

21.9.1 Förslagets innebörd

Förslaget innebär att privata utförare ska få ansluta sig som avsändare genom anmälan av den kommun eller landsting som de utför uppdrag åt. Det är således kommunen eller landstinget som ska bedöma om utföraren har behov av anslutning. Sett på några års sikt är det inte omöjligt att utförarens förmåga att skicka säker digital post till brukare skulle kunna vara ett krav i kommunernas eller lands-

[37] Se kommunallagen (2017:725).

tingens upphandling. En utgångspunkt för anmälan bör därför vara att kommunen eller landstinget kommit överens med utföraren om att denne ska vara ansluten.

Vidare är det rimligt att den anmälande kommunen eller landstinget själv är ansluten som avsändare. Som ansluten har kommunen eller landstinget en viss kompetens i hur infrastrukturen fungerar. Det är också troligt att en ansluten kommun eller landsting har en intern policy för hur infrastrukturen ska användas som även utföraren kan tillämpa.

Kommunen eller landstinget bör även ha viss tillsyn över användandet. Om kommunen eller landstinget finner att infrastrukturen inte används på avsett sätt får man återkalla anmälan. När utförarens uppdrag upphör ska kommunen eller landstinget vara skyldig att återkalla anmälan.

21.9.2 Privata utförare – utredningens tidigare överväganden

Enligt direktiven[38] skulle utredningen i delbetänkande redovisa hur privata utförare[39] av offentligfinansierad verksamhet ska kunna ansluta som avsändare inom Mina meddelanden. I delbetänkandet fann utredningen det svårt att lägga ett förslag med den innebörden. Ett tungt skäl för detta var svårigheten att på ett uttömmande sätt definiera vilka aktörer som skulle omfattas. Utredningen hade fram till dess inte heller kunnat notera ett tydligt behov. Inte minst mot bakgrund av att kommunernas anslutning till Mina meddelanden var låg.[40] Dessutom var inget landsting anslutet som avsändare. Slutligen bedömdes förslaget att myndigheter ska ersätta brevlådeoperatörerna ekonomiskt innebära en likabehandling av myndigheter och privata utförare. Privata utförare skulle liksom andra företag kunna träffa avtal med brevlådeföretagen direkt.[41]

Utredningen föreslår nu – till skillnad från vad som framgår av delbetänkandet – att öppna upp infrastrukturen för fler aktörer mot

[38] Tilläggsdirektiv till Utredningen om effektiv styrning av nationella digitala tjänster i en samverkande förvaltning, Dir. 2016:97 s. 3.
[39] För en analys av begreppet privata utförare se utredningens delbetänkande SOU 2017:23, digitalforvaltning.nu, s. 237. En legaldefinition av begreppet finns i 10 kap. 7 § kommunallagen (2017:725).
[40] I februari 2017 var endast sex kommuner anslutna och sände försändelser i Mina meddelande. I december 2017 hade antalet anslutna kommuner ökat till 17.
[41] SOU 2017:23, digitalforvaltning.nu, s. 229 ff.

bakgrund av de skäl som anges ovan. Det förslag som nu lämnas anser utredningen vara en möjlig lösning för att kunna ansluta privata utförare av offentligfinansierad verksamhet som avsändare i Mina meddelanden.

21.10 Företag och organisationer som utför uppgifter av allmänt intresse

Utredningen föreslår:
att regeringen får besluta att som avsändare får företag och organisationer som utför en uppgift av allmänt intresse ansluta sig. Regeringen får besluta om anslutningen bör villkoras med att företaget eller organisationen ska ha avtal med leverantör av brevlådetjänster för digital post.

Som anfördes i delbetänkandet tog Skatteverket redan år 2012 upp frågan om en breddad användning av Mina meddelanden. I anslutning till att Skatteverket föreslog att även kommuner skulle få ansluta sig till infrastrukturen anfördes följande:

> Vid kontakter med aktörer som överväger att bli brevlådeoperatörer och med myndigheter och företag som vill ha en infrastruktur av planerat slag för att sända och motta meddelanden har en återkommande fråga varit varför förmedlingsadressregistret inte ska få användas på ett öppnare och mer behovsanpassat sätt.[42]

Antalet anmälda datorbedrägerier har åttafaldigats sedan år 2007. Ökningen är mer än dubbelt så stor som den totala ökningen av antalet bedrägeribrott och medför att datorbedrägerier nu utgör 46 procent av alla anmälda bedrägeribrott. Brottskategorin avser brott där någon berett sig tillgång till annans utrustning för att för att skaffa sig vinning.[43]

Ett vanligt sätt att göra det är att via e-post förmå någon att klicka på en länk som laddar ned skadligt innehåll till datorn. Detta genom att avsändaren utger sig för att vara någon som mottagaren

[42] Hemställan om ändring i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte, Skatteverket, dnr 131-830189-12/111.
[43] https://www.bra.se/brott-och-statistik/kriminalstatistik/anmalda-brott.html

litar på, t.ex. en bank eller ett postföretag. Under år 2015 och 2016 uppmärksammades flera attacker med s.k. phishing av Postnord.[44] Det finns därför starka skäl att möjliggöra för företag och organisationer som har behov av att säkert kommunicera med kunder och medlemmar.

Som tidigare nämnts utgör privata utförare av offentligfinansierad verksamhet inom kommunerna och landstingen enbart en del av de ytterligare aktörer som kan behöva beredas möjlighet att ansluta som avsändare till infrastrukturen Mina meddelanden. Utredningen föreslår nu en väg som lämnar möjligheter för regeringen att öppna upp Mina meddelanden för fler aktörer. Regeringen får besluta att som avsändare får företag och organisationer som utför en uppgift av allmänt intresse ansluta sig.

En uppgift av allmänt intresse kan utföras exempelvis av friskolor, banker, försäkringsföretag, pensionsförvaltare, kreditupplysningsföretag, apotek, bilbesiktningsföretag och bostadsföretag. Utredningen föreslår att en lista över de verksamheter som regeringen vill öppna upp infrastrukturen för ska föras in i förordningen om infrastruktur för digital post.

En aktör måste dock ha ett organisationsnummer för att kunna vara avsändare i Mina meddelanden.

Utredningen föreslår även att regeringen får besluta om att anslutningen ska villkoras med att företaget eller organisationen har avtal med leverantörerna av brevlådetjänster för digital post.

21.11 Känsliga personuppgifter

21.11.1 Dataskyddsförordningen och 1995 års dataskyddsdirektiv

Behandling av känsliga personuppgifter regleras i artikel 9 i dataskyddsförordningen. Med känsliga personuppgifter menas enligt dataskyddsförordningen personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter om hälsa och en persons sexualliv eller sexuella läggning. Även behandling av biometriska uppgifter

[44] Massutskick av nytt bluffmejl som ser ut att komma från Postnord, pressmeddelande Postnord 2016-02-03.

för att entydigt identifiera en fysisk person och genetiska uppgifter utgör känsliga personuppgifter. Begreppet känsliga personuppgifter används inte uttryckligen i artikel 9, men förekommer i skäl 10 till dataskyddsförordningen.

Enligt dataskyddsförordningens huvudregel, som framgår av artikel 9.1, är behandling av känsliga personuppgifter förbjuden. Det finns dock en rad undantag från detta förbud. Exempel på när undantag från förbudet kan vara aktuellt är om en registrerad uttryckligen har lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål (9.2 a), om behandlingen är nödvändig på grund av hänsyn till ett viktigt allmänt intresse (9.2 g) eller om behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål (9.2 j).

Vissa av undantagen, t.ex. artikel 9.2 g och j, förutsätter att behandlingen är nödvändig på grundval av unionsrätten eller medlemsstaternas nationella rätt. Vissa särskilda krav ställs på denna rätt. I artikel 9.2 g krävs t.ex. att unionsrätten eller den nationella rätten står i proportion till det eftersträvade syftet, är förenligt med det väsentliga innehållet i rätten till dataskydd och innehåller bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Enligt artikel 9.4 i dataskyddsförordningen får medlemsstaterna behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriska uppgifter eller uppgifter om hälsa. Bestämmelserna innehåller krav på någon form av skyddsåtgärder. Vad som avses med skyddsåtgärder framgår inte av förordningen.

I skäl (10) i dataskyddsförordningen anges att förordningen ger medlemsstaterna handlingsutrymme att specificera sina bestämmelser, även för behandlingen av särskilda kategorier av personuppgifter, och att förordningen inte utesluter att det i medlemsstaternas nationella rätt fastställs närmare omständigheter för specifika situationer där uppgifter behandlas, inbegripet mer exakta villkor för laglig behandling av personuppgifter.

Av skäl (8) framgår vidare att om förordningen föreskriver förtydliganden eller begränsningar av dess bestämmelser genom medlemsstaternas nationella rätt, kan medlemsstaterna i den utsträckning det är nödvändigt för samstämmigheten och för att göra de nationella bestämmelserna begripliga för de personer som de tillämpas på, införliva delar av denna förordning i nationell rätt.

Även enligt 1995 års dataskyddsdirektiv är huvudregeln att behandling av känsliga personuppgifter är förbjuden. Något direkt undantag med hänsyn till viktiga allmänna intressen finns inte i direktivet. Enligt artikel 8.4 har medlemsstaterna dock möjlighet att med hänsyn till ett viktigt allmänt intresse besluta om ytterligare undantag från förbudet att behandla känsliga personuppgifter.

Något generellt undantag som skulle kunna träffa den personuppgiftsbehandling som utförs inom infrastrukturen för digital posts tillämpningsområde har dock inte införts i personuppgiftslagen, PuL.[45] Ett undantag för myndigheters behandling i löpande text av känsliga personuppgifter som lämnats i ett ärende eller är nödvändiga för handläggning av ett ärende har dock, med stöd av 20 § PuL, införts i 8 § personuppgiftsförordningen[46] med stöd av artikel 8.4 i 1995 års dataskyddsdirektiv.

21.11.2 Dataskyddslagen

Dataskyddsutredningen har i sitt betänkande förslagit att dataskyddslagen ska innehålla bestämmelser om rätten att behandla känsliga personuppgifter. Dataskyddsutredningen har gjort bedömningen att kravet på stöd i nationell rätt innebär att vissa av undantagen från förbudet att behandla känsliga personuppgifter bör föreskrivas i nationell rätt.[47]

Dataskyddsutredningen föreslår i 3 kap. förslaget till dataskyddslag ett antal bestämmelser om känsliga personuppgifter. I 3 kap. 1 § anges att utöver vad som framgår av artikel 9.2 a, c, d, e eller f i dataskyddsförordningen får sådana särskilda kategorier av personuppgifter som anges i artikel 9.1 i förordningen (känsliga personuppgifter) behandlas om förutsättningarna i någon av 2–8 §§ är uppfyllda. 3 kap. 3 och 4 §§ behandlar myndigheters behandling i vissa fall. Enligt förslaget ska myndigheter få behandla känsliga personuppgifter i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det (3 kap. 3 § 1). Dataskyddsutredningen föreslår också att myndigheter ska få behandla känsliga personuppgifter om de lämnats till myndigheten och behandlingen krävs en-

[45] SFS 1998:204.
[46] SFS 1998:1191.
[47] Se SOU 2017:39 s. 162.

ligt annan lag (3 kap. 3 § 2). Anledningen till detta anges vara att det utgör ett viktigt allmänintresse att myndigheterna ska kunna sköta sitt uppdrag på ett korrekt, rättssäkert och effektivt sätt. Detta förutsätter att den grundlagsstadgade handlingsoffentligheten och andra lagstadgade skyldigheter upprätthålls. Det anges också att viss behandling av känsliga personuppgifter är oundvikligt i myndigheternas verksamhet som en direkt följd av exempelvis tryckfrihetsförordningens, offentlighets- och sekretesslagens och förvaltningslagens bestämmelser. Sådan behandling bör uttryckligen tillåtas i dataskyddslagen så att det inte råder någon tveksamhet kring lagligheten av behandlingen.[48]

Utöver detta föreslår Dataskyddsutredningen att myndigheter i enstaka fall ska få behandla känsliga personuppgifter om det är absolut nödvändigt för ändamålet med behandlingen och inte innebär ett otillbörligt intrång i den registrerades personliga integritet (3 kap. 3 § 3). En myndighet som behandlar känsliga personuppgifter enbart med stöd av 3 kap. 3 § dataskyddslagen ska enligt Dataskyddsutredningens förslag inte få använda dessa personuppgifter som sökbegrepp (3 kap. 4 §). Därutöver föreslås att regeringen ska få meddela föreskrifter om ytterligare undantag från förbudet, om det behövs med hänsyn till ett viktigt allmänt intresse (3 kap. 8 §).

21.11.3 Behandling av känsliga personuppgifter i infrastrukturen för digital post behöver inget kompletterande författningsstöd

Utredningen bedömer:
att det inte behövs någon nationell bestämmelse som ger rätt att behandla känsliga personuppgifter inom lagens tillämpningsområde.

Utredningen bedömer att undantaget i artikel 9.2 g dataskyddsförordningen, som ger rätt att behandla känsliga personuppgifter om det är nödvändigt med hänsyn till ett viktigt allmänt intresse, omfattar den del av verksamheten som genomförs av registerförande myndighet respektive avsändare inom infrastrukturen Mina meddelanden. Denna verksamhet utgör en uppgift av allmänt intresse i dataskyddsförordningens mening. Infrastrukturen Mina meddelandens verksam-

[48] Se Dataskyddsutredningens betänkande, SOU 2017:39 s. 176 f.

het är viktig både för effektiviteten i den offentliga sektorn och för möjligheten för medborgarna att ta del av handlingar på ett smidigt och lättillgängligt sätt.

Artikel 9.2 g i dataskyddsförordningen innehåller vissa krav som måste vara uppfyllda för att undantaget ska bli tillämpligt. För det första ska det viktiga allmänna intresset framgå av unionsrätten eller medlemsstaternas nationella rätt. För det andra ska denna lagstiftning stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Verksamheten för infrastrukturen kommer enligt förslaget att bli fastställd genom den föreslagna författningen, men är redan i dag reglerad genom förordningen om statliga myndigheters elektroniska informationsutbyte.[49] När det gäller de grundläggande principerna för personuppgiftsbehandling motsvarar dataskyddsförordningen till allra största delen 1995 års dataskyddsdirektiv.[50] Mot den bakgrunden anser utredningen att det får förutsättas att riksdagen och regeringen bedömt att den behandling av personuppgifter som försiggår inom infrastrukturens och förordningen om statliga myndigheters elektroniska informationsutbytes tillämpningsområde är proporionerlig mot syftet med behandlingen och inte oförenlig med det grundläggande skyddet för personuppgifter. Genom utredningens förslag till lag om infrastruktur för digital post finns också bestämmelser som säkerställer skyddet för de registrerades integritet, t.ex. i form av behörighets- och sökbegränsningar.

Avseende leverantörens behandling av känsliga personuppgifter bedömer utredningen att det är undantaget i artikel 9.2 a dataskyddsförordningen, som ger rätt att behandla känsliga personuppgifter. Alla mottagare som genom leverantörer får sin digitala post i sina brevlådor, har samtyckt till detta.

Enligt den nya lagens sekundära ändamålsbestämmelse kommer personuppgifter att få behandlas om det behövs för att fullgöra uppgiftslämnande i överensstämmelse med lag eller förordning. Även känsliga personuppgifter kan naturligtvis ingå bland de personuppgifter som ska lämnas ut på denna grund.

[49] Förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.
[50] Se kap 5, jfr t.ex. artikel 5.1 i dataskyddsförordningen med artikel 6 i 1995 års dataskyddsdirektiv.

Utredningen bedömer också att ett utlämnande av personuppgifter i enlighet med lag eller förordning måste anses vara nödvändigt med hänsyn till ett allmänt intresse. Undantaget i artikel 9.2 g i dataskyddsförordningen – viktigt allmänt intresse – är därmed tillämpligt även på sådan behandling av känsliga personuppgifter med stöd av den föreslagna sekundära ändamålsbestämmelsen. Det får vidare förutsättas att ett utlämnande av personuppgifter som föreskrivs i författning är proportionerligt mot syftet med utlämnandet och inte oförenligt med det grundläggande skyddet för personuppgifter. För det fall känsliga uppgifter lämna ut till annan myndighet finns också ett skydd för uppgifterna, eftersom myndigheter enligt Dataskyddsutredningens förslag till dataskyddslag inte får använda sökbegrepp som avslöjar känsliga personuppgifter. Detta gäller dock bara när de specifika registerförfattningarna inte reglerar frågan med egna bestämmelser alternativt inte alls hänvisar till dataskyddslagen. Myndigheternas registerförfattningar kan innehålla skyddsåtgärder i form av bl.a. sökbegränsningar eller behörighetsbegränsningar.

Sammanfattningsvis anser utredningen att samtliga krav som ställs upp i artikel 9.2 g i dataskyddsförordningen för att känsliga personuppgifter ska få behandlas med hänsyn till ett viktigt allmänt intresse, tillsammans med det samtycke som avses i artikel 9.2 a, är uppfyllda för den personuppgiftsbehandling som utförs inom ramen för lagen om infrastruktur för digital posts primära och sekundära ändamålsbestämmelser. Dataskyddsförordningen tillåter enligt utredningens mening därmed att känsliga personuppgifter behandlas på hela lagens tillämpningsområde om det är nödvändigt för att verksamheten ska kunna bedrivas. Någon bestämmelse som ger rätt att behandla känsliga personuppgifter inom lagens tillämpningsområde behövs därmed inte.

Det finns inte något hinder mot att medlemsstaterna inför mer restriktiva bestämmelser för sina myndigheters personuppgiftsbehandling än vad som följer av dataskyddsförordningen. Utredningen bedömer dock inte att sådana bestämmelser är nödvändiga här och ser därmed inte något behov av att särskilt reglera om känsliga personuppgifter i lagen om infrastruktur för digital post. I stället kommer bestämmelser i den föreslagna dataskyddslagen att tillämpas.

21.12 Föreskriftsrätt, ersättningsrätt och den tillkommande förordningen

21.12.1 Föreskriftsrätt

Utredningen föreslår:
att lagen om infrastruktur för digital post ska innehålla ett bemyndigande om att regeringen, eller den myndighet som regeringen bestämmer, ska få meddela föreskrifter om inrättande och drift av infrastrukturen, den längsta tid under vilken personuppgifter får behandlas, säkerhetsåtgärder till skydd för personuppgifter, behörighets- och sökbegränsningar och vilka verksamheter som regeringen vill ge möjlighet att ansluta som avsändare i infrastrukturen.
att lagen ska innehålla ett bemyndigande om att när myndigheten tillämpar lagen om valfrihet om digitala brevlådor ska regeringen, eller den myndighet som regeringen bestämmer, fastställa ersättning till leverantör av brevlådetjänster för digital post anslutna enligt 14 §.

Medlemsstaterna har, enligt artikel 6.2 och 6.3 i dataskyddsförordningen, rätt att i nationell lagstiftning behålla eller införa mer specifika bestämmelser för personuppgiftsbehandling. Detta kan genomföras exempelvis genom nationella registerförfattningar. Varken artikel 6.2 eller 6.3 innehåller något krav på att de bestämmelser som avses måste regleras i lag. Det är därmed utredningens uppfattning att det bör vara upp till den enskilda medlemsstaten på vilken nivå i normhierarkin sådana bestämmelser införs. I enlighet med detta ställningstagande hindrar dataskyddsförordningen inte att bestämmelser om personuppgiftsbehandling införs i en förordning eller i en myndighetsföreskrift. Detta förutsätter naturligtvis att föreskrifterna tillkommit i laga ordning. Mot den bakgrunden anser utredningen att det inte finns hinder i dataskyddsförordningen mot att föreslå föreskriftsrätt av olika slag i den nya lagen om infrastruktur för digital post.

Utredningen föreslår att lagen om infrastruktur för digital post ska innehålla ett bemyndigande om att regeringen, eller den myndighet som regeringen bestämmer, ska få meddela föreskrifter om inrättande och drift av infrastrukturen, den längsta tid under vilken personuppgifter får behandlas, säkerhetsåtgärder till skydd för personuppgifter, behörighets- och sökbegränsningar och vilka verksam-

heter som regeringen vill ge möjlighet att ansluta som avsändare i infrastrukturen. När myndigheten tillämpar lagen om valfrihet om digitala brevlådor ska regeringen eller den myndighet regeringen bestämmer också fastställa ersättning till leverantör av brevlådetjänster för digital post anslutna enligt 14 §.

21.12.2 Ersättning till leverantör av brevlådetjänster för digital post

Utredningen föreslår:
att den ersättning som erbjuds leverantörerna av digitala brevlådetjänster ska bestämmas av regeringen, uppgå till samma belopp för alla berörda leverantörer, vara rörlig och utgå från volymen digital myndighetspost. Leverantörerna fakturerar respektive avsändare.

Förslaget genomförs genom lagen om infrastruktur för digital post.

I delbetänkandet föreslog utredningen att ersättning till leverantörer av digitala brevlådetjänster skulle regleras i ett valfrihetssystem.[51] Skälen för förslaget var sammanfattningsvis att mottagarna av digital post skulle ha möjlighet att välja bland flera olika leverantörer av brevlådetjänster för digital post samtidigt som dessa leverantörer behövde få betalt för sina tjänster.

Förutsättningarna för förslaget om valfrihetssystem kvarstår och det är utredningens uppfattning att det mottogs väl av berörda aktörer. Med några språkliga justeringar låter utredningen därför samma förslag ingå i det förslag som utredningen lämnar nu.

Ersättningsmodellen ska kompensera för leverantörernas verksamhet att göra myndighetspost tillgänglig för mottagaren. Modellen ska samtidigt bidra till att förenkla för mottagarna av myndighetsposten samt sänka utgifterna för det offentligas myndighetspost. En övergång till elektronisk myndighetspost medför att myndigheterna får lägre utgifter för porto och det måste vara utgångspunkten när ersättningen till leverantörerna bestäms.

[51] SOU 2017:23, digitalforvaltning.nu, s. 229 ff.

Ett pris för en tjänst eller vara kan många gånger bestämmas enhetligt till ett fast pris. Denna prissättning lämpar sig för enhetligt bestämda prestationer. Leverantörernas tjänster är i grunden enhetliga men kan variera i volym. Det finns dock kostnader i delar i av leverantörernas verksamhet som är fasta, åtminstone språngvis.

Leverantörernas tjänster varierar i omfattning. En rörlig ersättning är därför ett huvudalternativ och ersättningen bör så långt möjligt variera med de kostnader som följer med tjänsterna.

Ett antagande är att kostnaderna för de enskilda tjänsterna minskar efter hand som volymen ökar och att de tjänster som leverantörerna själva använder sig av blir mindre kostsamma i takt med ökade volymer.

Ersättningen kan bestå av en ersättning grundad på antalet förmedlade försändelser och lämnas med nedsättningar grundade på större försändelsevolymer. Det vill säga att om man väljer denna form bör ersättningen kunna minska per försändelse i takt med ökad volym förmedlade försändelser.

En leverantör av digitala brevlådetjänster har dock inte enbart rörliga kostnader. Även i fortsatt löpande drift finns kostnader som inte beror av antalet försändelser utan av att avsändarna anpassar och uppdaterar sina rutiner, system och program. Därtill kommer support till avsändare och mottagare. Mot denna bakgrund skulle man kunna överväga att använda grundersättningar. Det kan röra sig om engångsersättningar för nyanslutningar och om årliga grundersättningar för driften.

Ytterligare ett alternativ är att lämna en årlig ersättning för varje individ och företag som anslutit sig som mottagare till en leverantör av digital myndighetspost. En sådan ersättning skulle kunna lämnas månadsvis och flyttas mellan leverantörerna om mottagarna byter leverantörer.

Ett alternativ eller komplement till *ekonomisk* ersättning är att staten ger leverantörerna gratis eller subventionerad tillgång till tjänster i anslutning till brevlådetjänsten. En sådan ersättning kan vara att ge en allmän tillgång till infrastrukturen i Mina meddelanden.

Enligt utredningens bedömning ska ersättningen till leverantörerna vara rörlig och utgå från volymen försändelser från avsändare till mottagare. Ersättningen ska kunna variera över tid, efterhand som volymerna ökar. Ersättningen, som ska vara samma för alla berörda leverantörer, ska beslutas av regeringen eller den myndighet som

regeringen bestämmer. Så länge Skatteverket har uppgiften att godkänna och sluta avtal med leverantörer av digitala brevlådetjänster, inklusive Min myndighetspost, bör dock inte Skatteverket få detta uppdrag.

Förslaget innebär vidare att respektive leverantör, ska fakturera respektive avsändare (som skickat försändelser till mottagare i brevlådan). Skälet till att leverantörerna av digitala brevlådetjänster ska fakturera avsändarna, dvs. statliga och kommunala myndigheter, direkt är att de olika avsändarna ska behandlas lika.

De företag och organisationer som utför uppgifter av allmänt intresse och är anslutna som avsändare ska inte omfattas av förslaget ovan. De sluter själva avtal med en leverantör av digital brevlådetjänst och kommer där överens om ersättningen. Denna grupp avsändare ska inte vara anslutna till valfrihetssystemet.

21.12.3 En tillkommande förordning

Utredningen föreslår:
att det införs en förordning om infrastruktur för digital post med regler om vilken myndighet som ska tillhandahålla infrastrukturen, vilka verksamheter som utför uppgifter av allmänt intresse som ska få ansluta som avsändare samt att de ska ha avtalat om att skicka digital post med leverantörerna av brevlådetjänster för digital post som är anslutna till infrastrukturen.

Förslaget genomförs genom förordningen om infrastruktur för digital post.

Utredningen har föreslagit att lagen om infrastruktur för digital post ska innehålla en föreskriftsrätt om inrättande och drift av infrastrukturen, den längsta tid under vilken personuppgifter får behandlas, säkerhetsåtgärder till skydd för personuppgifter, behörighets- och sökbegränsningar, vilka verksamheter som regeringen vill ge möjlighet att ansluta som avsändare infrastrukturen samt villkor för dem.

Utifrån denna föreskriftsrätt föreslår utredningen en tillhörande förordning. Utredningen lämnar förslag utifrån föreskriftsrätten om att det är Skatteverket som ska vara myndigheten som ska tillhandahålla infrastrukturen och få meddela föreskrifter. Slutligen föreslår utredningen även att regeringen i förordningen ska besluta att fri-

skolor, banker, försäkringsföretag, kreditupplysningsföretag, pensionsförvaltare, apotek, bilbesiktningsföretag och bostadsföretag får ansluta som avsändare i infrastrukturen för digital post samt att företag i dessa verksamheter ska ha avtalat om att skicka digital post med leverantörerna av brevlådetjänster för digital post som är anslutna till infrastrukturen.

21.13 Ikraftträdande

Utredningen föreslår:
att lagen om infrastruktur för digital post, lagen om valfrihet om digitala brevlådor och förordningen om infrastruktur för digital post ska träda i kraft den 1 juli 2019.

Med hänsyn till den tid som kan beräknas gå åt för remissförfarande, fortsatt beredning inom Regeringskansliet och riksdagsbehandling bör de bestämmelser utredningen föreslår tidigast kunna träda i kraft den 1 juli 2019.

22 Konsekvensanalyser

22.1 Nollalternativet – finns det ett nollalternativ?

I kommittéhandboken[1] står det att läsa att statsmakternas ställningstagande till ett utredningsförslag oftast underlättas av om förslagets förväntade konsekvenser jämförs med konsekvenserna av att inga förändringar görs, dvs. i jämförelse med ett nollalternativ. Konsekvenserna av ett realistiskt och genomförbart nollalternativ ska därför beräknas och beskrivas. För att kunna bedöma om ett förslag är lönsamt eller inte bör det jämföras med ett eller flera alternativ. Med nollalternativ menas en bedömning av hur situationen blir om förslaget inte genomförs. Nollalternativ behöver inte vara detsamma som den rådande situationen när utredningens förslag lämnas.

Utredningen konstaterar att den digitala utvecklingen har begränsningar vad gäller förutsägbarhet. Utvecklingen styrs, som utredningen inledningsvis konstaterar, i hög grad av multinationella aktörer på en global marknad. Den finns flera exempel på att utvecklingen gått långsammare än som förutspåtts, men att genomslaget när det väl kommit har blivit mer omfattande än vad man förutsett. Avancerade mobiltelefoner, s.k. smarttelefon, är ett exempel på det. Till detta kommer, som utredningen också framhållit, att förslagen måste ses mot bakgrund av andra insatser som regeringen gör eller som, mot bakgrund av förslag som lämnas av parallella utredningar, kan antas komma att genomföras. Att beskriva ett nollalternativ mot denna bakgrund är därför varken möjligt eller meningsfullt.

I tilläggsdirektiv till Digitaliseringskommissionen[2] skrev regeringen för drygt två år sedan att digitaliseringens snabba utveckling gör att strukturomvandlingen går fortare än vid tidigare teknikskiften. Digi-

[1] Ds 2000:1.
[2] Dir. 2015:123, tilläggsdirektiv till Digitaliseringskommissionen den 26 november 2015.

taliseringen påverkar hela samhället och det är viktigt att försäkra sig om att nyttja digitaliseringens fördelar och minimera dess negativa konsekvenser på såväl samhällsnivå som individnivå.

Digitaliseringen kommer sannolikt att gå ännu snabbare i framtiden än vad den hittills har gjort. De stora utmaningarna för samhället kommer att vara att förhålla sig till tekniken. Hur ska den användas, av vem, på vilket sätt och vad blir konsekvenserna för samhället och individen? Det är ett paradigmskifte i så måtto att det för första gången är svårare att följa med i effekterna av den tekniska utvecklingen än det är att ta fram tekniken.

Utredningens förslag till nya bestämmelser kommer att leda till konsekvenser, både för enskilda individer och statliga myndigheter, kommuner och landsting. För individen bedömer utredningen att förslagen bidrar till bättre och säkrare offentlig service i olika delar av landet. Sammantaget innebär förslagen att det blir enklare för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av förvaltningens service. Förslagen bidrar också till att de offentliga myndigheterna kan erbjuda individen en likvärdig service av god kvalitet i stora delar av landet. Bestämmelserna kan i ett inledningsskede innebära ökade kostnader för offentliga myndigheter för anpassning av befintliga it-system eller för investeringar i nya it-system men innebär i förlängningen, enligt utredningens bedömning, väsentliga effektiviseringar och kostnadsminskningar både i ett förvaltningsövergripande perspektiv och för respektive offentlig myndighet som tillhandahåller e-tjänster. Utredningens förslag innebär därmed att samhällets samlade resurser kan användas mer effektivt.

Även företagen gynnas av en effektivare användning av samhällets resurser. Utredningen bedömer att förslagen medför positiva konsekvenser för de företag som verkar inom verksamhetsområden som stagas upp av tydligare reglering, bättre förutsebarhet och ökad säkerhet. Utredningens ambition har samtidigt varit att gynna innovation och företagsamhet. Därför ska regleringen inte medföra hämmande effekter utan tillåta sådan utveckling som kan komma alla till gagn.

22.2 Konsekvenser för den kommunala självstyrelsen

För utredningar i kommittéväsendet gäller att om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, ska konsekvenserna i det avseendet anges i betänkandet. Vid all lagstiftning som kan få betydelse för den kommunala självstyrelsen ska – enligt den så kallade proportionalitetsprincipen – prövas om skälen för regleringen motiverar det intrång i den kommunala självstyrelsen som den kan innebära. Det är i sådana sammanhang viktigt att konsekvenserna för den kommunala självstyrelsen blir föremål för ingående överväganden. Proportionalitetsprincipens huvudsakliga syfte är att åstadkomma en ordning som innebär att intresset av kommunal självstyrelse under beredningen av lagförslag regelmässigt ställs mot de intressen som ligger bakom lagförslaget. Det är av avgörande betydelse att den slutliga bedömningen av om proportionalitetskravet är tillgodosett görs av riksdagen i samband med att den tar ställning till förslaget.[3] Principen om kommunal självstyrelse gäller för all kommunal *verksamhet*.

Av 14 kap. 3 § regeringsformen framgår att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett den.[4]

Utredningens förslag omfattar vare sig statlig eller kommunal verksamhet, dvs. kärnverksamhet eller kommunala angelägenheter. Utredningens uppdrag är att lämna förslag till effektiv styrning av förvaltningsgemensamma digitala funktioner, dvs. medel för offentliga myndigheter att genomföra sin kärnverksamhet eller kommunala angelägenheter. Utredningens förslag omfattar därmed digitala medel för de offentliga myndigheternas genomförande av sina verksamheter.

Inget av utredningens förslag riktar sig enbart till kommuner och/eller till landsting utan omfattar både statliga myndigheter, kommuner och landsting. Av utredningens förslag är det förslagen om att erkänna den statliga elektroniska identitetshandlingen vid elektronisk identifiering och att ansluta sig till valfrihetssystem som digitaliseringsmyndigheten tillhandahåller som innebär en skyldighet för statliga myndigheter, kommuner och landsting att följa bestämmelserna.

[3] Prop. 2009/10:80, bet. 2009/10:KU19, rskr. 2009/10:304 och 305, bet. 2010/11:KU4, rskr. 2010/11:22.
[4] Statskontoret, Kommunalt självstyre och proportionalitet, 2011:17.

Det är utredningens bedömning att förslagen till författningsreglering som berör kommuner och landsting inte går utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett dem och mycket väl motiveras av ett eventuellt intrång i den kommunala självstyrelsen.

22.3 Kommunala finansieringsprincipen

Kommunala finansieringsprincipen innebär att om staten inför nya eller ändrade föreskrifter som ändrar skyldigheter för kommunerna och landstingen kan detta påverka dessas kostnader. För att hantera sådana konsekvenser har i samförstånd mellan staten, kommunerna och landstingen en finansieringsordning utvecklats, den s.k. kommunala finansieringsprincipen.

Den kommunala finansieringsprincipen omfattar enbart statligt beslutade åtgärder som tar sikte på *verksamheter*. Principen innebär att staten inte bör införa nya obligatoriska uppgifter för kommuner och landsting, göra tidigare frivilliga uppgifter obligatoriska, ändra ambitionsnivån på befintliga uppgifter eller göra regeländringar som påverkar kommuners möjligheter att ta ut avgifter utan medföljande finansiering, t.ex. i form av höjda statsbidrag. En förändring som leder till sänkta kostnader för kommunerna och landstingen ska på motsvarande sätt innebära minskade bidrag.

Finansieringsprincipen omfattar inte de så kallade frivilliga verksamheterna. Den omfattar inte heller åtgärder som inte direkt tar sikte på kommunsektorn men som får ekonomiska effekter för sektorn. Hit hör till exempel statliga beslut som påverkar det kommunala skatteunderlaget och därmed skatteintäkterna.

Principen och dess tillämpning är inte lagfäst, men har godkänts av riksdagen.[5] Ekonomiska regleringar enligt den kommunala finansieringsprincipen genomförs i regel på så sätt att det generella statsbidraget till kommuner och landsting justeras.

Utredningen bedömer att förslagen i detta slutbetänkande inte omfattas av den kommunala finansieringsprincipen.

[5] Prop. 1993/94:150 bil. 7 avsnitt 2.5.1, bet. 1993/94:FiU19, rskr. 1993/94:442.

22.4 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Utredningens förslag vad gäller elektronisk identifiering stödjer det brottsförebyggande arbetet. Förslaget till en process för grundidentifieringen skapar en spårbarhet mellan individens identitet och en elektronisk identitetshandling som utfärdas av staten eller en annan aktör. Detta minskar väsentligt risken för missbruk av identitetshandlingar.

En förutsättning för digitaliseringen är att aktörer på marknaden kan vara säkra på vem det är som identifierar sig elektroniskt. Utredningen har konstaterat att det finns ett straffrättsligt skydd för elektroniska urkunder och att elektroniska identitetshandlingar på åtminstone tillitsnivå 3 och 4 är sådana urkunder. Utredningen har vidare konstaterat att det finns kritiska moment i processer för utfärdande av elektroniska identitetshandlingar, och vid användning av dem. Dessa kritiska moment kan utnyttjas i otillbörligt syfte. Ett moment är den identitetskontroll som görs av en person i samband med ansökan om en elektronisk identitetshandling. Genom att föreslå att någon eller några statliga myndigheter ska utfärda en statlig elektronisk identitetshandling som fästs på någon eller några fysiska identitetshandlingar bedömer utredningen att tilliten till att det är rätt individ som får den elektroniska identitetshandlingen kan öka. Risker som att en individ ansöker om och får en elektronisk identitetshandling utfärdad i annans namn minskar när staten ansvarar för att grundidentifiera individer och utfärda elektroniska identitetshandlingar. Därmed kan missbruk i detta sammanhang minska.

Ett annat kritiskt moment är i samband med användningen. De förslag utredningen lämnar om att det måste vara tydligt för individen att han eller hon identifierar sig för inloggning syftar till att öka förståelsen hos individer för att de använder en elektronisk värdehandling. Det kan leda till en ökad kunskap som i sin tur leder till att individen inte låter någon annan identifiera sig i hans eller hennes namn. Därmed kan otillbörlig användning av annans elektroniska identitetshandling minska. Det bygger dock på att individen är aktsam med sin elektroniska identitetshandling. Åtgärder för att verkligen säkerställa att det är rätt individ som använder den elektroniska identitetshandlingen kan vara att tillåta biometri. Utredningen lämnar emellertid inga förslag i denna del, utan har hänvisat till det pågående arbetet i 2017 års ID-kortsutredning.

Utredningens förslag vad gäller elektronisk identifiering stödjer därmed det brottsförebyggande arbetet. Förslaget till reglering av grundidentifieringen skapar en spårbarhet mellan individens identitet och en elektronisk identitetshandling som utfärdas av staten eller en annan aktör. Detta minskar väsentligt risken för missbruk av identitetshandlingar.

Genom eIDAS-förordningen kommer europeiska elektroniska identitetshandlingar att kunna användas för identifiering i svenska e-tjänster. Utfärdandet av dem ska utföras enligt gällande nationella regler i respektive medlemsstat. Detta kan innebära en risk för identitetsstölder, som i avvaktan på gemensamma rutiner, inte kan bortses ifrån. Det är en av orsakerna till att utredningen förordar försiktighet när det gäller att öppna upp e-tjänster för personer som identifierar sig med europeiska elektroniska identitetshandlingar.

Med förslaget till lag om infrastruktur för digital post skapas en kanal där inte bara myndigheter och privata utförare av offentligt finansierad verksamhet utan även andra företag kan kommunicera säkert med kunder och medborgare. Detta minskar möjligheterna för den typ av datorbedrägerier där kriminella utger sig för att vara en myndighet eller ett företag.

22.5 Konsekvenser för sysselsättningen

Utredningen bedömer att förslagen inte får några direkta konsekvenser för sysselsättningen.

22.6 Konsekvenser för jämställdheten mellan kvinnor och män

Utredningen bedömer att förslagen inte får några konsekvenser för jämställdheten mellan kvinnor och män.

22.7 Konsekvenser för att nå de integrationspolitiska målen

Utredningen bedömer att förslagen inte får några negativa konsekvenser för att nå de integrationspolitiska målen.

22.8 Närmare om konsekvenserna

Kapitel 5 – Effektiv styrning av en samverkande förvaltning

Utredningens förslag om samverkansuppgifter för digitaliseringsmyndigheten ligger inom ramen för de förslag till instruktionsenliga uppgifter om samverkan, inklusive finansiering, som utredningen lämnade i delbetänkandet.[6]

Utredningens förslag i detta slutbetänkande om att digitaliseringsmyndigheten ska tilldelas särskilda medel för frivillig samverkan mellan olika aktörer för att främja den offentliga sektorns digitalisering innebär en utgift för myndigheten som inte finns med i beräkningarna i delbetänkandet. Utredningen föreslår att digitaliseringsmyndigheten, på en särskild anslagspost på sitt förvaltningsanslag, tilldelas 20 miljoner kronor i anslagsmedel 2019 för denna uppgift. Utredningen föreslår att Utredningen om inrättande av en myndighet för digitalisering av den offentliga sektorn[7] tar med detta förslag i budgetunderlaget för 2019–2021 som ska lämnas till regeringen senast den 1 mars 2018 och samtidigt bedömer vilka belopp som bör gälla 2020 och 2021.

Utredningen föreslår att anslagsmedlen för denna uppgift ska finansieras genom en permanent överföring av anslagsmedel från ett anslag som redan i dag finansierar innovation och utveckling i ett samhällsövergripande perspektiv. Utredningen föreslår att 20 miljoner kronor förs över från anslaget 1:2 Verket för innovationssystem: Forskning och utveckling inom utgiftsområde 24. Ändamålet för anslaget 1:2 Forskning och utveckling inom utgiftsområde 24 är att anslaget får användas för utgifter för behovsmotiverad forsknings- och utvecklingsverksamhet, utveckling av innovationssystem och programanknutna utgifter. Anslaget får även användas för statsbidrag till SP Sveriges Tekniska Forskningsinstitut AB för riksmätplatser.

[6] Se kapitel 4 (4.4.4 och 4.6) samt kapitel 7.1 i SOU 2013:23 digitalforvaltning.nu.
[7] Dir. 2017:117.

Kapitel 7 – Mål för den offentliga förvaltningens digitaliseringsarbete

Regeringens och de statliga myndigheternas utgifter med anledning av utredningens förslag om mål för den offentliga förvaltningens digitaliseringsarbete samt förslaget om mål för de statliga myndigheternas digitaliseringsarbete finansieras, enligt utredningens bedömning, inom myndigheternas befintliga ramar.

Förslaget att regeringen ska ge digitaliseringsmyndigheten ett särskilt uppdrag att utforma en metod och en process för att stödja regeringens arbete med en samlad analys och bedömning av resultatet av den offentliga sektorns digitaliseringsarbete i förhållande till förslaget till riksdagsbundet mål ligger, enligt utredningens bedömning, inom ramen för uppgifterna i den instruktion för digitaliseringsmyndigheten som utredningen föreslog i delbetänkandet. Även de utgifter som föranleds av förslaget är finansierade genom utredningens förslag till finansiering av digitaliseringsmyndigheten.[8]

Kapitel 9 – Informationssäkerhet – en naturlig del i digitaliseringen

I kapitel 9 föreslår utredningen bl.a. att regeringen ger digitaliseringsmyndigheten i uppdrag att ta fram och mäta nyckeltal för informationssäkerhetsrelaterade aspekter i syfte att följa informationssäkerhetsmognaden i förhållande till digitaliseringen. Detta förslag bedömer utredningen falla inom ramen för det anslag som digitaliseringsmyndigheten får i övrigt för sin verksamhet.

Dessutom föreslår utredningen i samma kapitel att regeringen ger Myndigheten för samhällsskydd och beredskap (MSB) ett uppdrag att utreda hur tillsyn över informationssäkerhetsområdet och incidentrapportering kan genomföras. Detta förslag bedöms falla inom ramen för MSB:s befintliga verksamhet och finansieras inom MSB:s befintliga ram.

[8] Se SOU 2017:23, digitalforvaltning.nu, kapitel 4 och kapitel 7.1.

Kapitel 12 – Statlig elektronisk identitetshandling

Kapitlet innehåller utredningens förslag om att staten ska utfärda en elektronisk identitetshandling till svenska medborgare och folkbokförda i Sverige. Kapitlet innehåller också förslag om att den statliga elektroniska identitetshandlingen ska godtas för elektronisk identifiering hos alla offentliga myndigheter samt att den ska kunna användas för elektronisk identitetskontroll hos andra utfärdare i samband med ansökan om annan elektronisk identitetshandling.

Utredningen bedömer att förslagen får konsekvenser för offentliga myndigheter, för individer och för utfärdare av elektroniska identitetshandlingar.

Förslaget att staten ska utfärda en elektronisk identitetshandling

Förslaget innebär att staten tar på sig ansvaret för att utfärda en elektronisk identitetshandling i samband med utfärdandet av en fysisk identitetshandling. Det är det sätt som utredningen bedömt att staten på bästa sätt skapar förutsättningar för att utnyttja den grundidentifiering som görs i samband med utfärdande av en identitetshandling och att hålla kedjan intakt från grundidentifiering till utfärdande av en elektronisk identitetshandling. Utredningens förslag innehåller varken ställningstagande till vilken myndighet som ska utfärda en statlig elektronisk identitetshandling eller vilken fysisk identitetshandling som den statliga elektroniska identitetshandlingen ska finnas på. Det är frågor som 2017 års ID-kortsutredning ska ta ställning till, och således kommer konsekvenserna av det statliga åtagandet såvitt avser de frågorna att belysas av den utredningen.

Förslaget att statliga myndigheter, kommuner och landsting ska erkänna identifiering med den statliga elektroniska identitetshandlingen

Offentliga myndigheter måste som en följd av förslagen erbjuda individer identifiering med den statliga elektroniska identitetshandlingen. Det innebär att de måste skapa möjlighet att göra identitetskontroller gentemot utfärdaren av den elektroniska identitetshandling som staten utfärdar. Utredningen uttalar sig varken om ansvarig myndighet

eller vilken fysisk identitetshandling som den statliga elektroniska identitetshandlingen ska finnas på. Det är frågor som 2017 års ID-kortsutredning kommer att behandla. Vilken aktör som offentliga myndigheter måste etablera en relation till för att kunna erbjuda identifiering med den statliga elektroniska identitetshandlingen är alltjämt oklart.

Förslaget att den statliga elektroniska identitetshandlingen ska kunna användas som underlag för annan elektronisk identitetshandling

Utredningen bedömer att förslaget medför att leverantörer kan utnyttja den grundidentifiering som staten utför i samband med utfärdandet av den statliga elektroniska identitetshandlingen. Leverantörer, som ofta är privata aktörer, kan således erbjuda sina kunder ett helt elektroniskt ansöknings- och utfärdandeförfarande, åtminstone på vissa tillitsnivåer. Det är ett sätt för privata aktörer att utnyttja de förvaltningsgemensamma digitala funktioner som staten tillhandahåller.

Kapitel 13 – Myndigheters sätt att anskaffa funktioner för elektronisk identitetskontroll

I kapitlet finns utredningens bedömning att det måste vara enkelt för offentliga myndigheter att anskaffa funktioner för elektronisk identitetskontroll.

Utredningens förslag innebär konsekvenser för såväl digitaliseringsmyndigheten som för de offentliga myndigheterna och leverantörerna av funktioner för elektronisk identitetskontroll.

Konsekvenser för digitaliseringsmyndigheten

Utredningen bedömer att den ändring av roll som utredningen föreslår inte innebär några andra uppgifter för digitaliseringsmyndigheten än vad E-legitimationsnämnden har i dag. Det innebär att utredningen bedömer att digitaliseringsmyndighetens arbete i denna del ryms inom befintligt anslag.

Konsekvenser för de offentliga myndigheterna med att ansluta sig till valfrihetssystem

Utredningen bedömer att anvisningen innebär att offentliga myndigheter inte behöver överväga vilken av flera valmöjligheter som de ska använda sig av. Det som kan tillkomma är om offentliga myndigheter bedömer att de har behov utöver valfrihetssystemen, som måste upphandlas särskilt. Sammantaget bedömer emellertid utredningen att det torde innebära lättnader för de offentliga myndigheterna.

Konsekvenser för leverantörerna

Utredningen bedömer att leverantörerna på detta sätt kommer att veta var de finner marknaden för de offentliga myndigheterna. De kommer också att veta på vilka villkor de kan leverera funktioner för elektronisk identitetskontroll till de offentliga myndigheterna.

Konsekvenser av ändrad ersättningsmodell

Utredningen föreslår att dagens ersättningsmodell ska ändras och att leverantörer ska fakturera Kammarkollegiet för alla elektroniska identitetskontroller som offentliga myndigheter har begärt.

Förslaget innebär konsekvenser för såväl de offentliga myndigheterna som för leverantörer och Kammarkollegiet särskilt.

Offentliga myndigheter

De offentliga myndigheterna behöver med den föreslagna ersättningsmodellen inte själva betala för de identitetskontroller som begärs inom ramen för valfrihetssystem. Detta gäller för såväl statliga myndigheter som för kommuner och landsting. Förslaget innebär även en administrativ lättnad för de offentliga myndigheterna.

Leverantörer

Utredningen har beskrivit dagens ersättningsmodell där leverantörerna måste fakturera varje statlig myndighet, kommun eller landsting särskilt. Det förslag som nu lämnas bedömer utredningen kan underlätta för leverantörerna och innebär att leverantörernas administrativa arbete med fakturering effektiviseras.

Kammarkollegiet

Utredningen föreslår att Kammarkollegiets administration av faktureringen ska anslagsfinansieras. Därutöver föreslår utredningen att riksdagen varaktigt anvisar och regeringen tilldelar Kammarkollegiet ett anslag på inledningsvis cirka 29 miljoner kronor för att betala ersättningen för de offentliga myndigheternas elektroniska identitetskontroller. Det beräknade beloppet motsvarar de offentliga myndigheternas andel av BankID:s totala kostnader för elektroniska identitetskontroller 2017. Som en jämförelse kan nämnas att de statliga myndigheternas utgifter för posttjänster 2016 uppgick till 888 657 000 kronor.[9] Utredningen föreslår att det nya anslaget och Kammarkollegiets administration av ersättningen ska finanserias genom en omfördelning av anslagsmedel som frigörs hos de statliga myndigheterna genom de kostnadseffektiviseringar som användningen av de förvaltningsgemensamma digitala funktionerna medför.

Kapitel 14 – En infrastruktur för elektronisk identifiering

Utredningen föreslår i kapitlet att de uppgifter som E-legitimationsnämnden utför i dag ska författningsregleras och att det ska ankomma på digitaliseringsmyndigheten att utveckla och förvalta dessa. De aktuella uppgifterna är tillitsramverket och de tekniska specifikationerna för elektroniska identitetshandlingar samt granskningsförfarandet som leder fram till att en elektronisk identitetshandling får använda kvalitetsmärket Svensk elektronisk identitetshandling. Utredningen föreslår dessutom att det i lag ska regleras att det ska finnas en modell för hur dialogrutor för valbara elektroniska identitetshandlingar ska

[9] SOU 2017:23, digitalforvaltning.nu, s. 158.

se ut, samt att denna modell ska innefatta vilka elektroniska identitetshandlingar som ska visas på ett samlat sätt i en dialogruta.

Konsekvenser för digitaliseringsmyndigheten

Digitaliseringsmyndigheten kommer att inleda sin verksamhet den 1 september 2018. E-legitimationsnämnden avvecklas samtidigt och dess uppgifter tillfaller därefter digitaliseringsmyndigheten. De funktioner som utredningen föreslår ska författningsregleras utför E-legitimationsnämnden redan i dag. Det handlar alltså inte om tillkommande uppgifter utan endast att det synliggörs vilka uppgifter som utgör förvaltningsgemensamma digitala funktioner och som därmed ska omfattas av författningsreglering. Av de funktioner som utredningen föreslår ska regleras är uppgiften att ta fram en modell för dialogrutor beskrivningsmässigt ny. E-legitimationsnämnden har tidigare arbetat med en s.k. anvisningstjänst som var tänkt att fylla samma behov men på ett annat sätt. Utredningen bedömer att den omständigheten att uppgiften nu författningsregleras inte innebär att digitaliseringsmyndigheten får tillkommande uppgifter i förhållande till vad E-legitimationsnämnden har i dag. Det torde alltså rymmas inom befintligt anslag.

Utredningen föreslår att lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling ska träda i kraft den 1 januari 2020. Det som författningsregleras är att digitaliseringsmyndigheten ges i uppdrag att utveckla och förvalta vissa funktioner. Utredningen bedömer emellertid att det inte är en tillkommande uppgift sett i relation till vad E-legitimationsnämnden gör i dag, varför utredningen bedömer att det ryms inom befintligt anslag.

Konsekvenser av kvalitetsmärket Svensk elektronisk identitetshandling för utfärdare

Utredningen har i kapitel 14 bedömt att kvalitetsmärket måste spela en större roll än vad det har gjort så långt. Kvalitetsmärkta elektroniska identitetshandlingar ska vara indikatorer som individer söker efter när de ska ansöka om elektroniska identitetshandlingar. Utred-

ningen bedömer därför i kapitel 13 att kvalitetsmärkningen ska vara ett villkor för leverantörer som vill delta i valfrihetssystem.

Utredningen konstaterar att det i dag är få utfärdare som låtit sina elektroniska identitetshandlingar granskas av E-legitimationsnämnden. De åtgärder som utredningen föreslår är i syfte att fler utfärdare ska låta granska sina elektroniska identitetshandlingar. En utfärdare som låter sin elektroniska identitetshandling granskas måste underkasta sig digitaliseringsmyndighetens bedömning och krav. Eftersom utredningen också föreslår att granskningen ska göras mot de tekniska specifikationerna, kommer det innebära att mer krav ställs på utfärdarna än i dag. För vissa utfärdare kan kraven vara oförenliga med deras egen teknik. Utredningen bedömer dock att det är nödvändigt att ställa ensade krav på utfärdare eftersom det gynnar individer, offentliga myndigheter och utfärdarna som grupp.

Konsekvenser av kvalitetsmärket Svensk elektronisk identitetshandling för individer

Utredningen har bedömt att en kvalitetsmärkning av elektroniska identitetshandlingar tjänar som en viktig signal för både enskilda individer och för de som ska lita på elektroniska identitetshandlingar. Utredningen har vidare bedömt att det är en statlig uppgift att kvalitetsmärka elektroniska identitetshandlingar efter ett ansökningsförfarande. För individer syftar detta till att skapa ökad förståelse och medvetenhet om hur de ska hantera och bedöma elektroniska identitetshandlingar, för de som ska lita på elektroniska identitetshandlingar tjänar det som ett möjligt sätt att ställa krav på utfärdare.

Konsekvenser av kvalitetsmärket Svensk elektronisk identitetshandling för offentliga myndigheter

Utredningen bedömer att kvalitetsmärket Svensk elektronisk identitetshandling kan ha betydelse för offentliga myndigheter, även med beaktande av utredningens förslag att offentliga myndigheter inte längre själva ska tillhandahålla valfrihetssystem utan att det är digitaliseringsmyndigheten som ska göra det och de offentliga myndigheterna ska ansluta sig till de valfrihetssystem som digitaliseringsmyndigheten har. Det kan, såsom utredningen beskrivit i kapitel 13, inte

uteslutas att offentliga myndigheter har behov av att upphandla tjänster för elektronisk identitetskontroll vid sidan om valfrihetssystemen. Utredningen menar att sådana tjänster då inte ska benämnas funktioner, eftersom den förvaltningsgemensamma digitala funktionen är den som regleras i eLOV. Givet att det inte kan uteslutas en vanlig upphandling av sådana tjänster kan kvalitetsmärket spela en viktig roll för upphandlande myndigheter. Utredningen bedömer att det är lämpligt att upphandlande myndigheter ställer krav på att leverantörer ska erbjuda kvalitetsmärkta elektroniska identitetshandlingar, allt med beaktande av att kvalitetsmärket är viktigt för att individer ska kunna göra informerade val av elektroniska identitetshandlingar.

Kapitel 15 – Arbetstagare, student, ställföreträdare – och elektronisk identifiering

Kapitlet innehåller beskrivningar av pågående initiativ för elektronisk identifiering i olika kontexter, dvs. när individer behöver identifiera sig elektroniskt i egenskap av exempelvis arbetstagare, student eller som ställföreträdare för annan.

Utredningen föreslår i avsnitt 15.9 att regeringen ska ge digitaliseringsmyndigheten i uppdrag att närmare bedöma om E-identitet för offentlig sektor (EFOS) skulle kunna användas i hela den offentliga förvaltningen. Som närmare beskrivs i kapitel 15 är EFOS ett pågående samarbetet mellan Inera och Försäkringskassan när det gäller elektroniska identitetshandlingar i tjänsten.

Utredningen bedömer emellertid att det uppdrag som bör ges till digitaliseringsmyndigheten innebär att myndigheten ska bedöma om EFOS kan komma att utvecklas till en förvaltningsgemensam digital funktion, som alltså ska gälla för hela den offentliga förvaltningen. Detta uppdrag bedömer utredningen vara en tillkommande uppgift för digitaliseringsmyndigheten. Skulle digitaliseringsmyndigheten komma fram till att EFOS är en förvaltningsgemensam digital funktion måste det finnas en beredskap för att ta hand om regleringen av denna. Det är viktigt att förslag till sådan reglering börjar tas fram i god tid och parallellt med utvecklingen. Detta bör beaktas i det budgetunderlag som Utredningen om inrättandet av en myndighet för digitalisering av den offentliga sektorn ska lämna till regeringen.

Kapitel 17 – Europeiska elektroniska identitetshandlingar i svenska e-tjänster

Kapitlet handlar till stora delar om vilka konsekvenser som kan väntas av att svenska myndigheter i sina e-tjänster måste erkänna elektroniska identitetshandlingar som är utfärdade i andra europeiska länder. I kapitlet beskrivs myndigheternas förväntningar och vad de praktiskt kommer att ställas inför. I kapitlet beskriver utredningen de verksamhetsmässiga konsekvenser som myndigheterna behöver anpassa sig till.

De ekonomiska konsekvenserna av dessa anpassningar samt av ökad användning av e-tjänster med anledning av eIDAS-förordningen beskrivs nedan. Därefter beskrivs några följder av de rättsliga konsekvenser som eIDAS-förordningen medför.

Ekonomiska konsekvenser för statliga myndigheter, kommuner och landsting

Utredningen bedömer att flödena av identifieringar med elektroniska identitetshandlingar från andra länder till att börja med kommer att vara små. Utredningen bedömer vidare att de ekonomiska konsekvenserna av anpassningarna varierar mycket beroende på myndigheternas verksamhet och digitaliseringsgrad och att de ekonomiska konsekvenserna av ökad användning av e-tjänster bör leda till besparingar.

Utredningen har inte kunnat få någon samlad bild av hur stor användningen av svenska e-tjänster förväntas bli. Den bedömning som gjorts av flera av de svenska myndigheterna är att flödena från andra länder troligtvis först kommer att vara väldigt små. På sikt väntas större volymer. Många offentliga myndigheter har därför inledningsvis intagit en lite avvaktande hållning.

I den enkät som utredningen skickade till vissa myndigheter i oktober 2017 (se avsnitt 17.2.2) fanns några frågor om ekonomiska konsekvenser som myndigheterna har identifierat. De ekonomiska konsekvenserna kan delas upp i konsekvenser av anpassningar och konsekvenser av ökad användning av e-tjänsterna.

Konsekvenser av anpassningar

Flera av myndigheterna som besvarat enkäten kunde inte specificera några särskilda ekonomiska konsekvenser av sina anpassningar de gjort eller planerar att göra med anledning av eIDAS-förordningen. För dessa myndigheter ingår anpassningarna i den normala verksamheten på så sätt att de ändå behöver anpassa sig till framtiden och användares olika behov. Att utveckla e-tjänsterna och på bästa sätt möta omvärldens förväntningar ingår i det arbete som myndigheterna redan bedriver i fråga om sina e-tjänster. Eventuella tillkommande kostnader för dessa myndigheter har bedömts kunna omfattas av deras befintliga ram.

Andra myndigheter har kunnat ge något mer specificerade svar. De grupper av kommuner som gjort gemensamma upphandlingar av it-tjänster beskriver det som ekonomiskt fördelaktigt utan närmare specificering av exakta kostnader.

E-hälsomyndigheten kan inte uttala sig om exakta kostnader men ser behov av att anpassa berörda e-tjänster vilket kräver insatser av befintliga resurser som t.ex. kravanalytiker, experter och utvecklare samt inom informationssäkerhet och juridik. De behöver även titta på behov av eventuella språköversättningar.

Bolagsverket bedömer att kostnaderna för att anpassa verksamt.se inledningsvis kan uppgå till cirka 500 000 kronor. Därefter tillkommer kostnader för att utveckla servicen ytterligare när det gäller språk och bättre information till de som inte ges åtkomst till e-tjänsterna.

Tullverket menar att deras kostnader beror på nivån av skyldigheten. För att tillgodose krav på funktionalitet är det inte fråga om några stora pengar. Om det däremot handlar om funktioner blir det dyrt, t.ex. att bygga om informationsstandarder. Tullverket vill därför ha ett ställningstagande om funktionell interoperabilitet, gärna gällande e-underskrifter inom Sverige och EU.

Skatteverkets bedömda kostnader innehåller anpassningar av myndighetens e-tjänster, utveckling av service till de användare som inte ges tillträde till e-tjänsterna, samt anpassning av den befintliga lösningen för elektronisk identitetskontroll. Det uppskattade beloppet för anpassningar med anledning av eIDAS-förordningen är 25 miljoner kronor.

Pensionsmyndigheten bedömer, vid en första grov skattning, att kostnaderna 2018 blir en miljon kronor och 2019 två miljoner kro-

nor. I bedömningen finns en osäkerhetsfaktor om plus eller minus 50 procent. Kostnaderna inkluderar elektronisk identitetskontroll samt koppling till e-tjänster. För individer som inte har svenskt person- eller samordningsnummer erbjuder Pensionsmyndigheten i dagsläget inga e-tjänster.

Stockholms stad har startat sina förberedelser, t.ex. genom uppladdning av metadata till E-legitimationsnämndens testmiljö. Det har hittills kunnat hanterats inom ordinarie teknisk förvaltning och har inte gett upphov till några extra kostnader för staden.

Konsekvenser av ökad användning av e-tjänster

I de ekonomiska konsekvenserna ingår även att bedöma vad ökad användning av e-tjänster kan leda till på längre sikt i och med att även utländska användare kan ges tillgång till e-tjänsterna.

Myndigheterna har besvarat frågan i samband med deras bedömning av vilka nyttor eIDAS-förordningen kan medföra. Nyttorna innebär möjligheter till besparingar men eftersom myndigheterna själva inte ännu har analyserat verksamheten och den förväntade ökade användningen saknas uppgifter om belopp.

Tullverket har uttryckt att man ur verksamhetsperspektiv bedömer att eIDAS-förordningen konkret och direkt ger myndigheten möjlighet att både billigare och effektivare hantera användare som inte har någon svensk elektronisk identitetshandling. Det ger också möjlighet att utveckla e-tjänster som för användaren blir mer självbetjänande och enklare eftersom det går att bygga användarcentrerade tjänsteportaler – användaren hittar allt från olika leverantörer i en och samma e-tjänst. Detta bygger på att tjänsteleverantörerna har interoperabla funktioner. Som exempel kan myndigheten kanske slippa att kontrollera eller registrera en användare som redan finns betrodd hos någon annan. Digitalisering och automatisering bedöms frigöra personella resurser och myndighetens processpecifika kompetens kan koncentreras till andra delar i en verksamhetsprocess. Med andra ord kan de ekonomiska konsekvenserna innebära att myndigheterna sparar pengar i förlängningen.

Uppbyggnad och förvaltning av noden

Kapitel 17 avslutas med att beskriva de rättsliga konsekvenser som utredningen bedömer nödvändiga för att svenska myndigheter, kommuner och landsting ska kunna uppfylla eIDAS-förordningens krav. De rättsliga konsekvenserna handlar framför allt om uppbyggnaden och förvaltningen av den svenska offentliga noden för gränsöverskridande identifiering. För detta ansvarar i dag E-legitimationsnämnden. E-legitimationsnämndens verksamhet kommer den 1 september 2018 att övertas av den nya digitaliseringsmyndigheten. Utredningen bedömer att den fortsatta uppbyggnaden och förvaltningen av noden i digitaliseringsmyndighetens regi faller inom ramen för det anslag som utredningen föreslog i delbetänkandet.[10]

Incidentrapportering

Utredningen föreslår att alla aktörer som är anslutna till noden utan otillbörligt dröjsmål ska underrätta digitaliseringsmyndigheten om alla händelser som påverkat funktionalitet och säkerhet i noden. Denna incidentrapportering är en ny uppgift för de aktörer som ska utföra den som bör kunna utföras inom ramen för befintliga resurser. Samtidigt är det en nödvändig åtgärd för att digitaliseringsmyndigheten ska kunna sköta uppdraget att tillhandahålla noden och upprätthålla dess säkerhetsnivå.

Konsekvenser av förslaget om tekniska säkerhetsgranskningar av noden

Utredningen föreslår att Försvarets radioanstalt (FRA) ska genomföra tekniska säkerhetsgranskningar av den svenska offentliga noden för gränsöverskridande identifiering som är under uppbyggnad hos E-legitimationsnämnden. Den första granskningen ska genomföras innan noden tas i bruk och därefter ska granskningar begäras av digitaliseringsmyndigheten, som tar över ansvaret för noden i september 2018, vid större förändringar av noden.

[10] SOU 2017:23, digitalforvaltning.nu, s. 261 ff.

Enligt utredningens bedömning ingår sådana tekniska säkerhetsgranskningar i FRA:s uppgifter och bedöms samtidigt kunna hanteras inom ramen för FRA:s anslag.

Kapitel 18 – Anmälan av svenska elektroniska identitetshandlingar

Konsekvenserna av utredningens förslag i detta kapitel handlar främst om individens möjligheter att kunna använda sig av en svensk elektronisk identitetshandling för att sköta sina ärenden inom Europa på distans.

Utredningen föreslår att det ska vara en del av det offentliga åtagandet att Sverige ska anmäla svenska elektroniska identitetshandlingar för gränsöverskridande identifiering enligt eIDAS-förordningen. För att detta ska bli möjligt föreslår utredningen ett öppet förfarande där de svenska elektroniska identitetshandlingar som uppfyller vissa krav ska kunna anmälas. En framtida statlig elektronisk identitetshandling bör utformas med tanke på gränsöverskridande identifiering och när den är redo anmälas till EU-kommissionen i detta syfte.

Konsekvenserna av förslagen för individen blir att det går att som svensk nyttja de möjligheter som eIDAS-förordningen erbjuder genom eventuellt tillträde till europeiska e-tjänster.

Förslagen innebär för företag att det finns möjlighet att ta fram elektroniska identitetshandlingar för gränsöverskridande identifiering för anmälan. På så sätt kan företagen nå hela den inre marknaden inom EU.

Dessutom medför förslagen vissa uppgifter för digitaliseringsmyndigheten. Den nya myndigheten ska enligt utredningens förslag ansvara för anmälan och avanmälan av svenska elektroniska identitetshandlingar. Denna verksamhet bedöms av utredningen falla inom ramen för det anslag som digitaliseringsmyndigheten får i övrigt för verksamheten kopplad till eIDAS-förordningen, noden och gränsöverskridande identifiering.

Kapitel 19 – Betrodda tjänster enligt eIDAS-förordningen

Av eIDAS-förordningen följer bl.a. en skyldighet för svenska myndigheter, kommuner och landsting att erkänna europeiska anmälda elektroniska underskrifter. I kapitel 19 föreslår utredningen att regeringen ska ge digitaliseringsmyndigheten i uppdrag att specificera, tillhandahålla eller upphandla en gemensam valideringstjänst för att statliga myndigheter, kommuner och landsting ska kunna validera elektroniska underskrifter från andra länder. Skälen för detta förslag behandlas närmare i avsnitt 19.5.2. Även detta förslag bedöms av utredningen falla inom ramen för det anslag som digitaliseringsmyndigheten får i övrigt för verksamheten kopplad till eIDAS-förordningen.

Kapitel 20 – Framtida användning av europeiska identitetshandlingar i myndigheternas e-tjänster

Utredningen bedömer i kapitel 20 bl.a. att digitaliseringsmyndigheten bör prioritera deltagande i samarbetsnätverket för elektroniska identitetshandlingar och sakkunnigbedömningar. Det är svårt att uppskatta de ekonomiska konsekvenserna av detta eftersom ingen vet i vilken takt medlemsländerna kommer att anmäla sina elektroniska identitetshandlingar för gränsöverskridande identifiering. Av ett aktivt deltagande bör dock följa insikter om vad som är på väg att hända och kunskaper om de andra medlemsstaternas processer för att ta fram lämpliga elektroniska identitetshandlingar. Vetskap om detta kan underlätta i prioriteringsarbetet och även ge indikationer på om digitaliseringsmyndigheten i sitt budgetunderlag behöver begära ökade anslag för att sköta uppgiften på ett tillfredsställande sätt.

När det gäller konsekvenser av förslaget om kopplingsregister hänvisar utredningen till den konsekvensanalys som har genomförts av Skatteverket i promemorian Koppling mellan europeiska eID-handlingar och svenska personnummer eller styrkta samordningsnummer.[11]

[11] Dnr 131 184020-16/113, s. 68 ff.

Kapitel 21 – En lag om infrastruktur för digital post

För konsekvensanalysen avseende förslaget om lag om infrastruktur för digital post hänvisar utredningen till delbetänkandet[12] och kompletterar här med konsekvenserna av de kompletterande förslag som utredningen lämnar i detta slutbetänkande.

I konsekvenshänseende är det framför allt två viktiga skillnader mellan det tidigare förslaget och det förslag som utredningen nu lämnar. Dels öppnar förslagen för att privata utförare av kommunala angelägenheter ska kunna vara avsändare i infrastrukturen, dels ska även företag inom andra verksamheter kunna vara avsändare i infrastrukturen. Det innebär alltså att fler aktörer kan vara avsändare, fler avtal måste skrivas för att det ska stå klart vad varje aktör ansvarar för och mer uppgifter behöver registreras i förmedlingsadressregistret.

För statliga myndigheter innebär utredningens förslag om en ny lag om Mina meddelanden i detta slutbetänkande inte någon substantiell förändring jämfört med förslaget i delbetänkandet.[13] För kommuner och landsting innebär utredningens förslag i detta slutbetänkande ingen förändring utom i det avseende som gäller möjligheter för privata utförare att ansluta som avsändare i infrastrukturen. Kommunerna och landstingen ska enligt förslaget ansvara för att anmäla de privata utförare som de bedömer ska vara avsändare i infrastrukturen. De ska även avanmäla de privata utförarna när det blir aktuellt och dessutom ansvara för att de privata utförarna använder infrastrukturen till det den ska användas och inte för några andra syften.

Genom förslaget möjliggörs principen om likabehandling som har lyfts fram bl.a. av kommuner och SKL. Det spelar inte längre någon roll om det är en privat utförare som tar hand om den kommunala angelägenheten, den digitala posten kan skickas på precis samma sätt som om det är kommunen eller landstinget som själv utför angelägenheten. För mottagaren blir det ingen skillnad om man har valt en privat utförare eller inte. All digital post från dessa avsändare kan hamna i samma digitala brevlåda.

När det gäller ansvaret för de privata utfärdarna regleras det i kommunallagen att kommunen eller landstinget ska kontrollera och

[12] Kapitel 7.2 i SOU 2017:23 digitalforvaltning.nu.
[13] SOU 2017:23, digitalforvaltning.nu, s. 264 ff.

följa upp verksamheten.[14] Dessutom ska de kommuner och landsting som sluter avtal med en privat utförare, genom avtalet tillförsäkra sig information som gör det möjligt att ge allmänheten insyn i den verksamhet som lämnas över.[15]

Det innebär att kommuner och landsting som sluter avtal med privata utförare redan har ansvar för att kontrollera och följa upp deras verksamhet. De ska också få den information som behövs för insyn i den överlämnade verksamheten. Detta torde även innefatta den analoga postgång som de privata utförarna använder sig av i dag.

Utredningens förslag medför att vissa rutiner kan behöva ändras och kommuner och landsting behöver vara medvetna om att användningen av Mina meddelanden ingår i den verksamhet som de enligt kommunallagen ska kontrollera och följa upp. Samtidigt är detta ett ansvar som kommuner och landsting redan har men som genom förslagen kan få ny inriktning.

Det beskrivna förslaget ska ses som en möjlighet som har efterfrågats av många. De kommuner och landsting som bedömer att de inte kan ta det ansvar som krävs behöver inte anmäla privata utförare som avsändare i infrastrukturen. Ett krav för anmälan är att kommunen eller landstinget också själva ska vara anslutna som avsändare. När de är anslutna och själva använder sig av infrastrukturen får de kunskap i hur det fungerar och kan då lättare avgöra hur de ska kunna ansvara för sina respektive privata utförares användning.

I dag är 17 kommuner anslutna som avsändare i Mina meddelanden med ganska få flöden. Utredningen bedömer att anslutningen av privata utförare inte kommer att bli särskilt omfattande, i vart fall inte i det korta perspektivet. Privata utförare som avsändare kommer antingen att anslutas på grund av att den privata utföraren inför säker e-post till brukare som en del av sitt tjänsteutbud och erbjuder det som en del av paketet, eller att kommunerna kräver det i sin upphandling. Detta talar för att det kommer att ta tid innan det blir någon märkbar volym.

Vad som talar för en anslutning är att företag som är privata utförare kanske inte har byggt ut e-tjänster såsom mina sidor för brukarna. Detta kan särskilt gälla små företag. Mina meddelanden kan därmed uppfattas som ett bra sätt att säkert kommunicera med bru-

[14] 10 kap. 8 § kommunallagen (2017:725).
[15] 10 kap. 9 § kommunallagen (2017:725).

kare. Samtidigt innebär ju den relativt låga anslutningsgraden bland mottagare att företaget inte kan vara säker på att nå alla sina brukare via Mina meddelanden. Detta talar emot ett mer omfattande intresse så länge som inte den större delen av befolkningen kan nås.

Företag och organisationer som utför uppgifter av allmänt intresse

Utredningen föreslår att företag och organisationer som utför uppgifter av allmänt intresse också ska tillåtas ansluta sig som avsändare i infrastrukturen för digital post. Enligt förslaget ska regeringen besluta om vilka typer av verksamheter som ska släppas in i infrastrukturen. Utredningen föreslår att man börjar med friskolor, banker, försäkringsföretag, pensionsförvaltare, kreditupplysningsföretag, apotek, bilbesiktningsföretag och bostadsföretag.

Förslaget bedöms inte medföra några särskilda konsekvenser för vare sig statliga myndigheter, kommuner eller landsting. Förutom de aktuella företag som tillåts skicka digital post genom infrastrukturen påverkar förslagen främst mottagare, alltså individer som har anmält att de vill ha digital post. De kommer kunna samla allt mer post från olika sorters avsändare i samma digitala brevlåda. För de mottagare som exempelvis har barn i olika skolformer, kan de ta emot digital post på samma sätt oavsett om barnet går i kommunal skola eller friskola.

23 Författningskommentar

Utredningen har i föregående kapitel redogjort för de överväganden som ligger bakom de förändringar av bestämmelser som utredningen föreslår i detta betänkande. Av den anledningen är författningskommentarerna begränsade till att i huvudsak avse hänvisningar till de avsnitt i betänkandet där respektive bestämmelse behandlas.

23.1 Förslag till lag om statlig elektronisk identitetshandling

1 §

I denna lag finns bestämmelser om statliga elektroniska identitetshandlingar.

Förslaget behandlas i avsnitt 12.7 och 12.8.

2 §

En statlig elektronisk identitetshandling kan utfärdas till den som är svensk medborgare eller folkbokförd i Sverige enligt folkbokföringslagen (1991:481).

Förslaget behandlas i avsnitt 12.8.

3 §

En statlig elektronisk identitetshandling innehåller följande uppgifter om en individ:

– *nuvarande efternamn*

– *nuvarande förnamn*

– *födelsedatum*

– *personnummer*

Regeringen eller den myndighet som regeringen bestämmer får besluta om att lägga till andra uppgifter om en person i den elektroniska identitetshandlingen.

Förslaget behandlas i avsnitt 12.8.1.

4 §

En statlig elektronisk identitetshandling ska utfärdas på den högsta svenska tillitsnivån enligt tillitsramverket i lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

En statlig elektronisk identitetshandling ska utformas enligt de tekniska specifikationerna i lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

Förslaget behandlas i avsnitt 12.7.2.

5 §

En statlig elektronisk identitetshandling ska finnas på de fysiska identitetshandlingar som regeringen bestämmer.

En statlig elektronisk identitetshandling har samma giltighetstid som den fysiska identitetshandling som den finns på.

Förslaget behandlas i avsnitt 12.7.

6 §

Ansökan om en statlig elektronisk identitetshandling ska göras hos de myndigheter (utfärdande myndigheter) som regeringen bestämmer.

Förslaget behandlas i avsnitt 12.8.3.

7 §

Ansökan om en statlig elektronisk identitetshandling ska göras i samband med ansökan om en fysisk identitetshandling. Uppgifterna i ansökan ska avges på heder och samvete eller under annan sådan försäkran. Sökanden är skyldig att inställa sig personligen.

Förslaget behandlas i avsnitt 12.8.3.

8 §

Sökanden är skyldig att i samband med ansökan om en statlig elektronisk identitetshandling styrka sin identitet och övriga personuppgifter.

Förslaget behandlas i avsnitt 12.8.3.

9 §

En ansökan om en statlig elektronisk identitetshandling ska avslås om förutsättningarna i 8 § inte är uppfyllda eller det som har föreskrivits av regeringen i fråga om ansökan inte har iakttagits och sökanden inte har följt en uppmaning att avhjälpa bristen.

Förslaget behandlas i avsnitt 12.8.3.

10 §

Regeringen eller de myndigheter som regeringen bestämmer får meddela ytterligare föreskrifter om ansökan och utfärdande av statliga elektroniska identitetshandlingar.

Förslaget behandlas i avsnitt 12.8.3.

11 §

Statliga myndigheter, kommuner och landsting ska erkänna identifiering med den statliga elektroniska identitetshandlingen i de e-tjänster där myndigheten, kommunen eller landstinget kräver elektronisk identifiering.

Förslaget behandlas i avsnitt 12.8.4.

12 §

Användare får använda den statliga elektroniska identitetshandlingen som underlag vid ansökan om en annan elektronisk identitetshandling.

Förslaget behandlas i avsnitt 12.8.5.

13 §

Regeringen eller de myndigheter som regeringen bestämmer får uppställa villkor för när en statlig elektronisk identitetshandling får användas som underlag för ansökan om en annan elektronisk identitetshandling.

Förslaget behandlas i avsnitt 12.8.5.

14 §

När en statlig elektronisk identitetshandling används som underlag vid ansökan om en elektronisk identitetshandling hos en annan utfärdare av elektroniska identitetshandlingar ska denne informera den utfärdande myndigheten.

Förslaget behandlas i avsnitt 12.8.6.

15 §

Den utfärdande myndigheten ska registrera vilka andra elektroniska identitetshandlingar som har skapats med den statliga elektroniska identitetshandlingen som underlag.

Förslaget behandlas i avsnitt 12.8.6.

16 §

En statlig elektronisk identitetshandling ska spärras om

- *det fanns hinder mot att utfärda den statliga elektroniska identitetshandlingen vid tiden för utfärdandet och hindret fortfarande består,*
- *någon väsentlig uppgift som framgår av den statliga elektroniska identitetshandlingen är felaktig och inte längre gäller, eller*
- *någon annan än den som den statliga elektroniska identitetshandlingen är utställd till förfogar över den statliga elektroniska identitetshandlingen.*

Förslaget behandlas i avsnitt 12.8.7.

17 §

Om en statlig elektronisk identitetshandling spärras ska den utfärdande myndigheten informera de utfärdare av elektroniska identitetshandlingar, som har använt den statliga elektroniska identitetshandlingen som underlag om detta.

Förslaget behandlas i avsnitt 12.8.7 och 12.8.9.

18 §

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om förfarandet vid spärr av statliga elektroniska identitetshandlingar.

Förslaget behandlas i avsnitt 12.8.7.

19 §

Beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. Prövningstillstånd krävs vid överklagande till kammarrätt.

Förslaget behandlas i avsnitt 12.8.8.

20 §

Beslut enligt denna lag gäller omedelbart, om inte något annat anges i beslutet.

Förslaget behandlas i avsnitt 12.8.8.

23.2 Förslag till lag om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling

1 §

I denna lag finns bestämmelser om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

I infrastrukturen för elektronisk identifiering ingår:

1. tillitsramverk,

2. tekniska specifikationer för elektronisk identifiering,

3. register med utfärdare och förlitande aktörer samt

4. modell för dialogruta med valbara elektroniska identitetshandlingar.

Svensk elektronisk identitetshandling är ett kvalitetsmärke för elektroniska identitetshandlingar som har granskats och godkänts mot tillitsramverket och de tekniska specifikationerna.

Förslaget behandlas i avsnitt 14.3.

2 §

I lagen avses med

1. användare: den som har en elektronisk identitetshandling,

2. elektronisk identitetshandling: en värdehandling som en användare kan använda för att identifiera sig elektroniskt,

3. fysisk bärare: en fysisk identitetshandling, en koddosa eller liknande,

4. mobil bärare: exempelvis en smarttelefon eller en surfplatta,

5. förlitande aktör: den som behöver verifiera en användares uppgifter vid identifiering mot en e-tjänst,

6. utfärdare: den som utfärdar en elektronisk identitetshandling till en användare,

7. tillitsramverk: ett graderat ramverk för tillförlitlighet i utfärdade elektroniska identitetshandlingar,

8. tillitsnivå: en nivå inom tillitsramverket,

9. tekniska specifikationer: tekniska krav som ställs på elektronisk identifiering,

10. modell för dialogruta med valbara elektroniska identitetshandlingar: gruppering av elektroniska identitetshandlingar som har kvalitetsmärket Svensk elektronisk identitetshandling och som presenterar dessa i en dialogruta för användaren när denne ska identifiera sig elektroniskt.

Förslaget behandlas i avsnitt 14.3.1.

Tillitsramverk

3 §

Det ska finnas ett tillitsramverk för elektroniska identitetshandlingar, som löpande ska anpassas till väletablerade standarder och utvecklingen i övrigt samt de hot och risker som kan uppkomma på området.

Förslaget behandlas i avsnitt 14.3.2.

4 §

Den myndighet som regeringen bestämmer ska förvalta och utveckla tillitsramverket enligt 3 §.

Förslaget behandlas i avsnitt 14.3.2. och 14.3.

Tekniska specifikationer

5 §

Det ska finnas tekniska specifikationer för elektronisk identifiering, som löpande ska anpassas till väletablerade standarder, utvecklingen i övrigt, samt de hot och risker som kan uppkomma på området.

Förslaget behandlas i avsnitt 14.3.3.

6 §

Den myndighet som regeringen bestämmer ska förvalta och utveckla tekniska specifikationerna enligt 5 §.

Förslaget behandlas i avsnitt 14.3.3. och 14.3.

Kvalitetsmärket Svensk elektronisk identitetshandling

7 §

Utfärdare av elektroniska identitetshandlingar kan ansöka om att granskas mot tillitsramverket enligt 3 § och de tekniska specifikationerna enligt 5 §. Den som uppfyller kraven på tillitsnivåerna och de tekniska specifikationerna ska godkännas.

Förslaget behandlas i avsnitt 14.3.4.

8 §

Godkända elektroniska identitetshandlingar får som ett tillägg till egen benämning även använda kvalitetsbenämningen Svensk elektronisk identitetshandling.

Förslaget behandlas i avsnitt 14.3.4.

9 §

Ansökan om att granskas mot tillitsramverket och de tekniska specifikationerna ska göras hos den myndighet som regeringen bestämmer. Samma myndighet ska godkänna att en elektronisk identitetshandling får använda kvalitetsbenämningen Svensk elektronisk identitetshandling.

Förslaget behandlas i avsnitt 14.3.4.

Register med utfärdare av elektroniska identitetshandlingar och förlitande aktörer

10 §

Det ska finnas ett register över utfärdare av elektroniska identitetshandlingar med kvalitetsmärket Svensk elektronisk identitetshandling och förlitande aktörer som är anslutna till valfrihetssystem enligt lagen om valfrihetssystem i fråga om funktioner för elektronisk identitetskontroll.

Förslaget behandlas i kapitel 13 samt i avsnitt 14.3.5.

11 §

Den myndighet som regeringen bestämmer ska förvalta och utveckla registret enligt 10 §.

Förslaget behandlas i avsnitt 14.3.5 och 14.3.

12 §

Förlitande aktörer som är ansluta till valfrihetssystem enligt lagen om valfrihetssystem i fråga om funktioner för elektronisk identitetskontroll ska registreras i registret med utfärdare och förlitande aktörer.

Förslaget behandlas i avsnitt 14.3.5

13 §

Det ska finnas en modell för dialogruta med valbara elektroniska identitetshandlingar. En dialogruta med valbara elektroniska identitetshandlingar ska visa de elektroniska identitetshandlingar som ingår i valfrihetssystem som tillhandahålls enligt lagen om valfrihetssystem i fråga om funktioner för elektronisk identitetskontroll samt den statliga elektroniska identitetshandlingen.

Förslaget behandlas i avsnitt 14.3.6.

14 §

Den myndighet som regeringen bestämmer ska förvalta och utveckla modellen enligt 13 §.

Förslaget behandlas i avsnitt 14.3.6.

15 §

Statliga myndigheter, kommuner och landsting ska använda modellen för dialogruta med valbara elektroniska identitetshandlingar i de e-tjänster där den statliga myndigheten, kommunen eller landstinget kräver att individen ska identifiera sig elektroniskt.

Förslaget behandlas i avsnitt 14.3.7.

16 §

Regeringen får besluta om undantag till skyldigheten i 15 § om det finns särskilda skäl.

Förslaget behandlas i avsnitt 14.3.7.

23.3 Förslag till lag om infrastruktur för digital post

Allmänna bestämmelser

1 §

Den myndighet som regeringen bestämmer (myndigheten) ska tillhandahålla en infrastruktur för digital post.

Förslaget behandlas i kapitel 21.

2 §

Denna lag gäller vid behandling av personuppgifter inom infrastrukturen. Vid sådan behandling gäller lagen endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Förslaget behandlas i avsnitt 21.8.

3 §

I denna lag avses med

1. *ankomstkontroll: att leverantören av brevlådetjänster för digital post utför kontroll mot förmedlingsadressregistret att avsändaren är ansluten.*
2. *avsändare: myndighet eller en juridisk person som genom avsändningskontroll skickar digital post till en mottagare inom infrastrukturen.*
3. *avsändningskontroll: att avsändaren utför kontroll mot förmedlingsadressregistret att mottagaren är ansluten till infrastrukturen, i så fall hos vilken leverantör mottagarens brevlådetjänst för digital post finns samt att avsändaren får sända digital post till mottagaren.*
4. *brevlådetjänster för digital post: den del inom infrastrukturen som lagrar digitala post efter att den har gjorts tillgänglig för mottagaren.*
5. *digital post: meddelanden genom digitala kanaler mellan olika aktörer i infrastrukturen.*
6. *förmedlare: en fysisk eller juridisk person som utför uppdrag åt en avsändare genom att vidarebefordra digital post.*
7. *förmedlingsadressregister: det register som innehåller uppgifter, däribland personuppgifter, om de anslutna i infrastrukturen.*
8. *leverantör av brevlådetjänster för digital post: en juridisk person eller en individ som tillhandahåller brevlådetjänster för digital post.*
9. *mottagare: individer och företag som anslutit sig till förmedlingsadressregistret och i sin brevlådetjänst för digital post tar emot digital post inom infrastrukturen.*
10. *privat utförare: en juridisk person eller en individ som har hand om en kommunal angelägenhet.*

I övrigt gäller definitioner i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

Förslaget behandlas i avsnitt 21.2.

4 §

Infrastrukturen utgörs av förmedlingsadressregister, brevlådetjänster för digital post, valfrihetssystem enligt lagen om valfrihet om elektroniska brevlådor samt vad regeringen, eller den myndighet regeringen bestämmer, har beslutat i form av föreskrifter.

Förslaget behandlas i kapitel 21.

5 §

Myndigheten får tillhandahålla brevlådetjänster för digital post till mottagare som enbart tar emot digital post från avsändare enligt 11 §.

Förslaget behandlas i avsnitt 21.3.

6 §

Till stöd för förmedling av digital post får myndigheten föra ett förmedlingsadressregister över anslutna enligt 11–15 §§. Syftet med registret är att ge de som är anslutna till infrastrukturen möjlighet att behandla personuppgifter i sin digitala postverksamhet på ett ändamålsenligt sätt och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Förslaget behandlas i kapitel 21.

Om rätten att få meddelande från myndighet via infrastrukturen

7 §

Om en ansluten mottagare begärt att en statlig myndighet ska sända digital post genom infrastrukturen får detta underlåtas endast om särskilda skäl finns.

Förslaget behandlas i avsnitt 21.4.

Förhållandet till annan lagstiftning

8 §

Denna lag innehåller bestämmelser som kompletterar Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Vid behandling av personuppgifter enligt denna lag gäller lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av denna förordning eller föreskrifter som har meddelats i anslutning till den.

Förslaget behandlas i avsnitt 21.5.

Ändamål

9 §

Personuppgifter får bara behandlas om det behövs för att

1. *hantera digital post i syfte att kunna utföra en arbetsuppgift inom en författningsreglerad verksamhet hos någon av de som anslutit sig till infrastrukturen, eller*
2. *lagra och bearbeta digital post som avses i 1 p. i syfte att erbjuda tilläggstjänster för brevlådeinnehavarna.*

Förslaget behandlas i avsnitt 21.7.

10 §

Personuppgifter som behandlas eller har behandlats enligt 9 § får även behandlas om det behövs för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

I ett enskilt fall får personuppgifter som behandlas eller har behandlats enligt 9 § även behandlas för att tillhandahålla information för något annat ändamål än det som anges, under förutsättning att ända-

målet inte är oförenligt med det ändamål för vilket uppgifterna samlades in.

Förslaget behandlas i avsnitt 21.7.

Anslutning

11 §

Till infrastrukturen ska som avsändare anslutas myndigheter under regeringen om inte regeringen har beslutat annat. Till infrastrukturen får kommuner och landsting ansluta sig som avsändare. Vidare får privata utförare av kommunala angelägenheter ansluta sig som avsändare enligt vad som föreskrivs i denna lag.

Regeringen får besluta att som avsändare får företag och organisationer som utför en uppgift av allmänt intresse ansluta sig. Regeringen får besluta om att denna anslutning ska villkoras med att företaget eller organisationen ska ha avtal med leverantör av brevlådetjänster för digital post.

Förslaget behandlas i avsnitt 21.9 och 21.10.

12 §

Till infrastrukturen får individer ansluta sig som mottagare om de anmält att de vill ta emot digital post från anslutna avsändare. Varje mottagare har genom sin anmälan tillgång till en brevlådetjänst för digital post.

Förslaget behandlas i kapitel 21.

13 §

Till infrastrukturen får leverantör av brevlådetjänster för digital post ansluta sig.

Förslaget behandlas i kapitel 21.

14 §

Den som ansluter sig till infrastrukturen ska registreras i förmedlingsadressregistret.

Förslaget behandlas i kapitel 21.

Avsändnings- och ankomstkontroll

15 §

Avsändare ska före sändning av digital post kontrollera i förmedlingsadressregistret om mottagaren är ansluten till infrastrukturen och i så fall hos vilken leverantör mottagarens brevlådetjänst för digital post finns samt att avsändaren får sända digital post till mottagaren. Om mottagaren inte är ansluten till infrastrukturen eller inte tar emot meddelanden från den aktuella avsändaren får den digitala posten inte sändas via infrastrukturen.

Förslaget behandlas i avsnitt 21.8.1.

16 §

Förmedlare ska före sändning av digital post kontrollera i förmedlingsadressregistret om mottagaren fortfarande är ansluten till infrastrukturen och om avsändaren får sända digital post till mottagaren. Om mottagaren inte är ansluten till infrastrukturen eller inte tar emot meddelanden från den aktuella avsändaren får den digitala posten inte sändas via infrastrukturen.

Förslaget behandlas i avsnitt 21.8.2.

17 §

Leverantör av brevlådetjänster för digital post ska vid ankomst av digital post kontrollera i förmedlingsadressregistret att avsändaren fortfarande är ansluten till infrastrukturen. Om avsändaren inte är ansluten eller

har något civilrättsligt avtal med mottagaren om digital brevlådetjänst ska meddelandet inte mottas.

Förslaget behandlas i avsnitt 21.8.3.

Personuppgiftsansvar

18 §

Myndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför när den tillhandahåller förmedlingsadressregistret.

Förslaget behandlas i avsnitt 21.8.4.

19 §

Avsändaren är personuppgiftsansvarig för behandling av personuppgifter till dess att leverantör av brevlådetjänster för digital post genom ankomstkontroll godkänt mottagandet enligt 17 §.

Avsändaren är vidare personuppgiftsansvarig för behandling av uppgifter som leverantören utför på avsändarens begäran efter att meddelandet gjorts tillgängligt för mottagaren.

Förslaget behandlas i avsnitt 21.8.5.

20 §

Leverantör av brevlådetjänster för digital post är personuppgiftsansvarig för behandling av uppgifter efter att ankomstkontroll genomförts med undantag för förhållanden enligt 19 § andra stycket.

Leverantören är vidare personuppgiftsansvarig för behandling av uppgift som denne erbjuder mottagaren.

Förslaget behandlas i avsnitt 21.8.7.

Anslutning av privata utförare av kommunala uppgifter

21 §

Privata utförare av kommunala angelägenheter får ansluta sig på begäran av kommun eller landsting som är ansluten till infrastrukturen. När utförarens uppdrag har upphört ska kommunen anmäla detta till den myndighet som regeringen beslutar för att ta bort registreringen på den privata utföraren som avsändare i förmedlingsadressregistret.

En förutsättning för anmälan ska vara att kommunen eller landstinget är ansluten samt har kommit överens med utföraren att denne ska använda infrastrukturen.

Kommunen eller landstinget ska kontrollera att utföraren använder infrastrukturen på avsett sätt. Om kommunen eller landstinget finner att utföraren brister härvidlag eller då uppdraget upphör ska anmälan återkallas.

Förslaget behandlas i avsnitt 21.9.1.

Föreskrifter

22 §

Regeringen eller den myndighet som regeringen bestämmer får med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om

1. *inrättande och drift av infrastrukturen,*
2. *den längsta tid under vilken personuppgifter får behandlas,*
3. *säkerhetsåtgärder till skydd för personuppgifter,*
4. *behörighets- och sökbegränsningar, och*
5. *vilka verksamheter som regeringen vill ge möjlighet att ansluta som avsändare i infrastrukturen samt villkor för dem.*

Förslaget behandlas i avsnitt 21.12.1.

Ersättning till leverantör av brevlådetjänster för digital post

23 §

När myndigheten tillämpar lagen om valfrihet om digitala brevlådor ska regeringen eller den myndighet regeringen bestämmer fastställa ersättning till leverantör av brevlådetjänster för digital post anslutna enligt 1 §. Vad som där fastställs ska inte tillämpas för den som anslutits enligt 11 § andra stycket.

Förslaget behandlas i avsnitt 21.12.2.

23.4 Förslag till lag om valfrihet om digitala brevlådor

1 §

Skatteverket får besluta att tillhandahålla valfrihetssystem för digitala brevlådor enligt lagen om infrastruktur för digital post. Med valfrihetssystem menas ett förfarande där mottagaren har rätt att välja den leverantör som ska utföra tjänsten och som Skatteverket har godkänt och tecknat avtal med.

Förslaget behandlas i avsnitt 21.12.2.

2 §

När Skatteverket tillhandahåller valfrihetssystem enligt denna lag ska myndigheten tillämpa lagen (2008:962) om valfrihetssystem. I stället för det som sägs i 2 kap. 3 § första meningen, 6 och 7 §§ lagen om valfrihetssystem ska med

1. *leverantör avses den som på marknaden tillhandahåller tjänster som nämns i 1 §,*
2. *tjänst avses sådan tjänst som nämns i 1 §, och*
3. *upphandlande myndighet avses Skatteverket.*

Förslaget behandlas i avsnitt 21.12.2.

23.5 Förslag till lag om ändring i lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

Noden

9 §

Den myndighet som regeringen utser (nodmyndigheten) ska ansvara för att tillhandahålla en offentlig förbindelsepunkt (nod) för gränsöverskridande elektronisk identifiering och att den fungerar i enlighet med EU:s förordning om elektronisk identifiering och rättsakter som har meddelats med stöd av den förordningen.

Regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om noden.

Paragrafen, som är ny, avser i första stycket att tydliggöra vem som har ansvar för att tillhandahålla Sveriges offentliga nod för mottagande av utländska elektroniska identitetshandlingar och för dirigering av svenska elektroniska identitetshandlingar till och från rätt utfärdare för användning i utländska e-tjänster. Regeln hindrar inte en framtida utveckling av fler noder för mottagande av utländska elektroniska identitetshandlingar.

I andra stycket behandlas föreskriftsrätt genom att regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om noden.

Förslagen behandlas i avsnitt 17.6 och 17.6.1.

10 §

För att användare ska kunna identifieras får nodmyndigheten behandla de personuppgifter som kommer till noden. Vilka personuppgifter som kommer till noden regleras i bilagan till Kommissionens genomförandeförordning (EU) 2015/1501.

Nodmyndigheten är personuppgiftsansvarig för de behandlingar av personuppgifter som utförs i noden.

I paragrafen, som är ny, anges i första stycket att ändamålet med behandling av personuppgifter i noden är att identifiera användare

samt att vilka personuppgifter som får behandlas regleras i bilagan till Kommissionens genomförandeförordning (EU) 2015/1501.

De personuppgifter som får behandlas är enligt bilagan till Kommissionens genomförandeförordning (EU) 2015/1501 följande obligatoriska attribut:

a) nuvarande efternamn,

b) nuvarande förnamn,

c) födelsedatum,

d) en unik identitetsbeteckning som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständiga i tid.

Dessutom får också behandlas följande valfria attribut:

a) förnamn och efternamn vid födseln,

b) födelseort,

c) nuvarande adress, kön.

I andra stycket tilldelas nodmyndigheten enligt 9 § personuppgiftsansvaret för de behandlingar av personuppgifter som myndigheten utför.

Förslagen behandlas i avsnitt 17.6.2.

11 §

Nodmyndigheten får behandla (tekniska) uppgifter för de aktörer vars uppgifter ska behandlas av noden. Myndigheten får även behandla de personuppgifter som är nödvändiga för att säkerställa behörigheter för aktörernas ombud.

I paragrafen, som är ny, regleras att nodmyndigheten får behandla vissa uppgifter. För att noden ska fungera på avsett vis behöver nodmyndigheten föra ett s.k. metadataregister över tekniska uppgifter för de aktörer vars uppgifter ska behandlas av noden. Aktörerna är t.ex. utfärdare av elektroniska identitetshandlingar. Om dessa tekniska uppgifter behöver ändras eller uppdateras behöver nodmyndigheten

veta att rätt person företräder aktören så att det går att lita på att uppgifterna om ändring stämmer. Därför behöver nodmyndigheten ha rätt att behandla de personuppgifter som är nödvändiga för att säkerställa behörigheter för aktörernas ombud.

Förslaget behandlas i avsnitt 17.6.7.

12 §

Alla myndigheter som, för att ge åtkomst till sina nättjänster, omfattas av kraven på elektronisk identifiering enligt EU:s förordning om elektronisk identifiering, ska ansluta till den svenska offentliga noden.

Myndigheter som inte omfattas av förordningens krav får ansluta till den svenska offentliga noden.

I paragrafen, som är ny, behandlas i första stycket att alla myndigheter som har e-tjänster där det krävs att användare loggar in med en elektronisk identitetshandling på minst svensk tillitsnivå 3, omfattas av kravet om erkännande av andra medlemsstaters elektroniska identitetshandlingar enligt eIDAS-förordningen. För att myndigheterna ska kunna ta emot utländska elektroniska identitetshandlingar och uppfylla kravet måste de ansluta till noden.

I andra stycket anges att även de myndigheter som inte omfattas av eIDAS-förordningens krav får ansluta till noden. Om myndigheter vill kunna erkänna utländska elektroniska identitetshandlingar för att ge tillträde till sina e-tjänster ska detta vara möjligt.

Förslaget behandlas i avsnitt 17.6.3.

13 §

Privata aktörer får ansluta till den svenska offentliga noden.

Regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om skyldighet för privata aktörer att betala avgift för att ansluta till noden enligt denna lag.

I paragrafen, som är ny, anges i första stycket att privata aktörer får ansluta till den svenska offentliga noden. För att möjliggöra för privata aktörer att erkänna utländska elektroniska identitetshandlingar i

sina e-tjänster ska även dessa få ansluta till den svenska offentliga noden.

I andra stycket anges att regeringen eller, efter regeringens bemyndigande, nodmyndigheten får meddela föreskrifter om skyldighet för privata aktörer att betala avgift för att ansluta till noden enligt denna lag. Noden föreslås inrättas med offentliga medel för offentliga syften som handlar om att tillgodose den offentliga sektorns behov av stöd för gränsöverskridande identifiering. Det privata användandet av noden kan därför komma att behöva avgiftsbeläggas för att inte offentliga medel ska användas på ett sätt som gynnar vissa privata aktörer.

Förslaget behandlas i avsnitt 17.6.4.

14 §

Alla som är anslutna till noden ska utan otillbörligt dröjsmål underrätta nodmyndigheten om alla händelser som påverkat funktionalitet eller säkerhet i noden.

I paragrafen, som är ny, behandlas incidentrapportering. För att upprätthålla nodens funktionalitet och säkerhet ska alla anslutna aktörer rapportera till nodmyndigheten om eventuella incidenter som inträffar.

Förslaget behandlas i avsnitt 17.6.5.

Anmälan av svenska medel för elektronisk identifiering

15 §

Den myndighet som regeringen utser ansvarar för anmälan av svenska medel för elektronisk identifiering för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering. (anmälande myndighet).

Regeringen eller den myndighet som regeringen bemyndigar får meddela föreskrifter om hur anmälan ska gå till.

I paragrafen, som är ny, anges i första stycket att regeringen utser en myndighet som ansvarar för anmälan av svenska elektroniska

identitetshandlingar för gränsöverskridande identifiering enligt eIDAS-förordningen.

Dessutom får regeringen eller myndigheten enligt andra stycket i föreskrifter besluta mer om hur anmälan ska gå till.

Förslaget behandlas i avsnitt 18.3.

16 §

För att kunna anmälas för gränsöverskridande elektronisk identifiering ska ett svenskt medel för elektronisk identifiering

1. *vara kvalitetsgranskad av digitaliseringsmyndigheten,*
2. *endast utfärdas till medborgare eller folkbokförda i Sverige,*
3. *ingå i valfrihetssystem enligt lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering, och*
4. *vara utfärdat av en aktör som har tecknat försäkring som täcker ersättning för skada som åsamkats fysiska eller juridiska personer avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla de skyldigheter som avses i artikel 7 i EU:s förordning om elektronisk identifiering.*

I paragrafen, som är ny, anges de förutsättningar som behöver vara uppfyllda för att en elektronisk identitetshandling ska kunna anmälas för gränsöverskridande identifiering enligt eIDAS-förordningen.

Kvalitetsmärkningen enligt första punkten är den granskning som staten utför för att kunna anmäla en elektronisk identitetshandling för gränsöverskridande identifiering i Sveriges namn och veta att den håller tillräcklig kvalitet för det avsedda syftet.

För att få anmälas för gränsöverskridande identifiering får den elektroniska identitetshandlingen bara utfärdas till medborgare eller folkbokförda i Sverige. Innehavarna av den elektroniska identitetshandlingen behöver ha personnummer för att Sverige med säkerhet ska kunna veta att de personidentifieringsuppgifter som förmedlas genom den elektroniska identitetshandlingen tillskrivs den fysiska person som avses vid tidpunkten för utfärdandet samt att den elektroniska identitetshandlingen faktiskt tilldelas den person som avses.

Kravet att ingå i valfrihetssystem är ett sätt att garantera att alla privata utfärdare av elektroniska identitetshandlingar får samma ersättning från staten för den levererade tjänsten samtidigt som användarna har möjlighet att styra genom sina val vilka elektroniska identitetshandlingar som ska kunna användas.

Utfärdare behöver även ha tecknat försäkring som täcker ersättning för eventuella skador som orsakas av de elektroniska identitetshandlingarna.

Förslaget behandlas i avsnitt 18.3.2.

17 §

Anmälande myndighet ansvarar även för att tillfälligt upphäva, återkalla, återinföra och dra tillbaka elektroniska identitetshandlingar vid säkerhetsincidenter enligt artikel 10 i EU:s förordning om elektronisk identifiering.

I paragrafen, som är ny, anges att samma myndighet som anmäler elektroniska identitetshandlingar måste också ha möjlighet att tillfälligt upphäva, återkalla, återinföra och dra tillbaka dem när det krävs enligt eIDAS-förordningen.

Förslaget behandlas i avsnitt 18.3.3.

Ikraftträdandebestämmelse

Lagen ska träda i kraft den 29 september 2018 som är det datum från vilket europeiska elektroniska identitetshandlingar ska erkännas i svenska myndigheters e-tjänster.

Förslaget behandlas i avsnitt 17.6.8.

23.6 Förslag till lag om ändring i lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering

1 §

I denna lag finns bestämmelser om tillämpning av valfrihetssystem i fråga om funktioner för elektronisk identitetskontroll.

Den myndighet som regeringen bestämmer (den upphandlade myndigheten) ska tillhandahålla valfrihetssystem för funktioner för elektronisk identitetskontroll.

Myndigheter, kommuner och landsting med behov av funktioner för elektronisk identitetskontroll ska ansluta sig till valfrihetssystem som den upphandlande myndigheten tillhandahåller.

Regeringen får besluta om undantag från skyldigheten i andra stycket om det föreligger särskilda skäl.

Förslaget behandlas i avsnitt 13.6.

2 §

Med valfrihetssystem avses i denna lag ett förfarande där individen har rätt att välja den leverantör som ska utföra identitetskontrollen och som den upphandlande myndigheten har godkänt och tecknat kontrakt med.

Termerna upphandlingsdokument, kontrakt och upphandlande myndighet har i denna lag samma betydelse som i lagen (2016:1145) om offentlig upphandling.

Förslaget, som innebär att begreppet tjänst för elektronisk identifiering byts till funktion för elektronisk identitetskontroll samt att en upphandlande myndighet ersätts av den upphandlande myndigheten, behandlas i avsnitt 13.6.1 och 13.6.3.

4 §

När den upphandlande myndigheten har beslutat att inrätta eller förändra ett valfrihetssystem ska det annonseras på en nationell webbplats som har upprättats för ändamålet. Ansökningar ska löpande begäras in genom sådan annonsering.

Upphandlingsdokumenten ska finnas tillgängliga på webbplatsen tillsammans med annonsen.

Förslaget, som innebär att en upphandlande myndighet ersätts av den upphandlande myndigheten, behandlas i avsnitt 13.6.3.

11 §

Den upphandlande myndigheten får begära att sökanden visar att det inte finns någon grund för att utesluta denne med stöd av 10 § första stycket 1, 2 eller 5.

Den upphandlande myndigheten ska som bevis för att det inte finns grund för att utesluta en sökande godta utdrag ur ett officiellt register eller annan likvärdig handling när det gäller ett förhållande som avses i 10 § första stycket 1 eller 2 och intyg från en behörig myndighet när det gäller ett förhållande som avses i 10 § första stycket 5.

Om, i fråga om en sökande som inte är medborgare i eller bosatt i Sverige, sådana handlingar eller intyg som avses i andra stycket inte utfärdas i sökandens hemland eller ursprungsland, eller inte omfattar samtliga de fall som avses i 10 § första stycket 1, 2 och 5, får de ersättas med en utsaga som har avgetts på heder och samvete eller av en liknande försäkran. En sådan sökande får också föreläggas att visa att det inte finns grund för att utesluta denne med stöd av 10 § första stycket 3 eller andra stycket.

Om en sökande är registrerad i en officiell förteckning över godkända tillhandahållare av identitetskontroll i ett land inom Europeiska ekonomiska samarbetsområdet, ska den upphandlande myndigheten utgå från att sökanden inte kan uteslutas som leverantör enligt 10 § första stycket 1–5.

Förslaget innebär att begreppet tjänstetillhandahållare ersätts av tillhandahållare av identitetskontroll. Begreppet tjänst byts ut i lagen mot funktion och denna ändring är således en följdändring.

Förslaget behandlas i avsnitt 13.6.1.

16 §

En leverantör som gör gällande att den upphandlande myndigheten har brutit mot en bestämmelse i denna lag, får ansöka om rättelse hos allmän förvaltningsdomstol.

Endast den sökande som inte har godkänts får ansöka om rättelse av beslut enligt 12 §.

En ansökan om rättelse ska vara skriftlig.

Förslaget, som innebär att en upphandlande myndighet ersätts av den upphandlande myndigheten behandlas i avsnitt 13.6.3.

19 §

Om den upphandlande myndigheten inte har följt bestämmelserna i denna lag ska myndigheten ersätta sökanden för därigenom uppkommen skada.

Talan om skadestånd ska väckas vid allmän domstol.

En skadeståndstalan som grundar sig på ett beslut att inte godkänna en sökande ska väckas inom ett år från dagen för beslutet. Väcks inte talan i tid, är rätten till skadestånd förlorad.

Förslaget, som innebär att begreppet en upphandlande myndighet ersätts av den upphandlande myndigheten, behandlas i avsnitt 13.6.3.

22 §

Den myndighet som regeringen bestämmer utövar tillsyn över att denna lag följs.

Tillsynsmyndigheten får inhämta sådana upplysningar som är nödvändiga för tillsynen från den upphandlande myndigheten och från den myndighet som avses i 1 § tredje stycket. Upplysningarna ska i första hand inhämtas genom ett skriftligt förfarande. Om det på grund av materialets omfång, brådska eller något annat förhållande är lämpligare, får upplysningarna i stället inhämtas genom besök hos den upphandlande myndigheten eller den myndighet som avses i 1 § tredje stycket.

Den upphandlande myndigheten och den myndighet som avses i 1 § tredje stycket är skyldig att tillhandahålla de upplysningar som tillsynsmyndigheten begär för sin tillsyn.

Förslaget innebär att en upphandlande myndighet ersätts med den upphandlande myndigheten vilket då syftar på digitaliseringsmyndigheten. Förslaget innebär vidare att tillsynsmyndigheten får inhämta upplysningar från statliga myndigheter, kommuner eller landsting. Digitaliseringsmyndighetens uppdrag att tillhandahålla valfrihetssystem behandlas i avsnitt 13.6.3.

23.7 Förslag till förordning med mål för de statliga myndigheternas digitaliseringsarbete

Förordningens tillämpningsområde

1 §

Denna förordning gäller för myndigheterna under regeringen.

Förslaget behandlas i avsnitt 7.3.3.

Mål för de statliga myndigheternas digitaliseringsarbete

2 §

Målet för de statliga myndigheternas digitaliseringsarbete är att den statliga förvaltningens användning av digitala medel ska leda till att det blir så enkelt som möjligt för så många som möjligt att utöva sina rättigheter och fullgöra sina skyldigheter samt ta del av den statliga förvaltningens service. De statliga myndigheternas användning av digitala medel ska vara säker samt öka kvaliteten och effektiviteten i den offentliga förvaltningen som helhet.

Förslaget behandlas i avsnitt 7.3.3.

Redovisning

3 §

Myndigheterna ska i sin årsredovisning redovisa sina resultat i förhållande till regeringens mål i 2 § i denna förordning för de statliga myndigheternas digitaliseringsarbete. Resultatredovisningen ska lämnas enligt 3 kap. 1 § förordningen (2000:605) om årsredovisning och budgetunderlag.

Förslaget behandlas i avsnitt 7.3.3.

23.8 Förslag till förordning om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling

1 §

Digitaliseringsmyndigheten ska förvalta och utveckla tillitsramverket enligt 3 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

Förslaget behandlas i avsnitt 14.3.2.

2 §

Digitaliseringsmyndigheten ska förvalta och utveckla de tekniska specifikationerna enligt 5 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

Förslaget behandlas i avsnitt 14.3.3.

3 §

Digitaliseringsmyndigheten granskar elektroniska identitetshandlingar enligt 8 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling elektroniska identitetshandlingar samt godkänner att en elektronisk identitetshandling som

tillägg till sitt eget namn får använda benämningen Svensk elektronisk identitetshandling.

Förslaget behandlas i avsnitt 14.3.4.

4 §

Digitaliseringsmyndigheten ska förvalta och utveckla registret med utfärdare av elektroniska identitetshandlingar och förlitande aktörer enligt 9 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

Förslaget behandlas i avsnitt 14.3.5.

5 §

Digitaliseringsmyndigheten ska förvalta och utveckla modellen för dialogruta med valbara elektroniska identitetshandlingar enligt 12 § lagen om infrastruktur för elektronisk identifiering och kvalitetsmärket Svensk elektronisk identitetshandling.

Förslaget behandlas i avsnitt 14.3.6.

23.9 Förslag till förordning om infrastruktur för digital post

1 §

Skatteverket ska tillhandahålla en infrastruktur för digital post och vara myndigheten enligt lagen om infrastruktur för digital post.

Förslaget behandlas i avsnitt 21.12.3.

2 §

Skatteverket får meddela föreskrifter enligt 23 § lagen om infrastruktur för digital post.

Förslaget behandlas i avsnitt 21.12.3.

3 §

Som avsändare i infrastrukturen för digital post får enligt 24 § 4 p. lagen om infrastruktur för digital post friskolor, banker, försäkringsföretag, pensionsförvaltare, kreditupplysningsföretag, apotek, bilbesiktningsföretag och bostadsföretag ansluta sig.

Förslaget behandlas i avsnitt 21.12.3.

4 §

De avsändare som ansluts enligt 3 § denna förordning ska ha avtalat om att skicka digital post med leverantörerna av brevlådetjänster för digital post som är anslutna till infrastrukturen.

Förslaget behandlas i avsnitt 21.12.3.

23.10 Förslag till förordning om ändring i förordningen (2016:576) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

6 §

Digitaliseringsmyndigheten ska vara nodmyndighet enligt 9 § lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering.

Digitaliseringsmyndigheten ska vara kontaktpunkt för Europeiska kommissionen i frågor som rör gränsöverskridande elektronisk identifiering.

Förslaget behandlas i avsnitt 17.6.1.

7 §

Digitaliseringsmyndigheten får meddela föreskrifter om

1. *hur aktörer ska ansluta till noden, och*
2. *rapportering av händelser som påverkat funktionaliteten eller säkerheten i noden.*

Förslaget behandlas i avsnitt 17.6.1.

8 §

Digitaliseringsmyndigheten ska ansvara för anmälningar till kommissionen av svenska medel för elektronisk identifiering för gränsöverskridande elektronisk identifiering enligt EU:s förordning om elektronisk identifiering.

Förslaget behandlas i avsnitt 18.3.

9 §

Digitaliseringsmyndigheten ska vid större förändringar av det system som den svenska noden omfattar, begära en teknisk säkerhetsgranskning av Försvarets radioanstalt. Granskningsförfarandet får ta max tre månader från det att digitaliseringsmyndigheten ansökt om granskning.

Förslaget behandlas i avsnitt 17.6.6.

23.11 Förslag till förordning om ändring i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte (I)

2 a §

Myndigheter får samverka utanför sina verksamhetsområden i frågor om digitalisering av den offentliga förvaltningen.

Förslaget behandlas i avsnitt 5.1.

23.12 Förslag till förordning om ändring i förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte (II)

Härigenom föreskrivs att 5 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte ska upphöra att gälla den 1 juli 2019.

Förslaget behandlas i avsnitt 21.13.

Kommittédirektiv 2016:39

Effektiv styrning av nationella digitala tjänster i en samverkande förvaltning (N 2016:01)

Beslut vid regeringssammanträde den 19 maj 2016

Sammanfattning

En särskild utredare ska analysera och ge förslag till effektiv styrning av utveckling, införande och förvaltning av nationella digitala tjänster. Utredaren ska, med utgångspunkt i de nationella digitala tjänsterna Mina meddelanden och Svensk e-legitimation, analysera tjänsterna och lämna förslag till utformning av:

- organisering och ansvarsfördelning för de nationella digitala tjänsterna,
- åtgärder och incitament för att uppnå en ökad användning av de nationella digitala tjänsterna, och
- samverkan mellan offentlig och privat sektor i tillhandahållandet av de nationella digitala tjänsterna.

Vidare ska utredaren analysera och lämna förslag som rör vissa specifika frågor inom ovanstående områden för Svensk e-legitimation och Mina meddelanden samt återstående frågor om den nationella tillämpningen av EU-förordningen om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen).

Uppdraget ska, när det gäller följande frågor om Mina meddelanden, redovisas i ett delbetänkande senast den 15 mars 2017:

- hur privata utförare av offentligfinansierad verksamhet ska kunna ansluta som avsändare inom Mina meddelanden,
- hur en övergång för privatpersoner och företag till digital myndighetspost kan genomföras i praktiken, och
- förslag till utformning av en ersättningsmodell för de brevlådeoperatörer som tillhandahåller brevlådor inom ramen för Mina meddelanden.

Uppdraget i övrigt ska redovisas senast den 31 oktober 2017.

Samverkan inom gemensamma digitala lösningar

Digitala tjänster ska, så långt det är möjligt och där det är relevant, vara förstahandsval i den offentliga sektorns kontakter med medborgare, organisationer och företag (prop. 2015/16:1, utg.omr. 22, s. 120). Genom fler innovativa lösningar i offentlig tjänsteproduktion bör ytterligare effektivitetsvinster kunna göras. Det finns en stor effektiviseringspotential att ta till vara med hjälp av tekniken och den ska också bidra till att förstärka förvaltningens öppenhet (prop. 2009/10:175 s. 27).

Digitaliseringskommissionen har konstaterat att digitaliseringen ändrar förutsättningarna för de offentligt finansierade verksamheterna genom att den erbjuder stora möjligheter till effektivisering och rationalisering och högre kvalitet för individen i de tjänster som tillhandahålls (SOU 2015:91). Kommissionen har vidare funnit att detta ställer nya krav på den offentliga sektorns kärnverksamhet, på dem som arbetar med människor inom vård, skola och omsorg samt på transparens och interaktion i den service och information som ges. Verksamhetsutveckling i offentlig sektor handlar alltmer om att använda digitaliseringens möjligheter för att möta utvecklingen i omvärlden.

E-delegationen och Statskontoret har i olika utredningar framfört att Sverige börjat tappa placeringar och uppvisa sämre resultat i internationella mätningar, efter att länge ha varit en av de ledande nationerna på e-förvaltningsområdet. E-delegationen har i sitt slutbetänkande konstaterat att offentlig sektor behöver mobilisera samverkan kring gemensamma digitala lösningar (SOU 2015:66). Delega-

tionen pekade på att utvecklingen i andra länder i hög grad bygger på gemensamma identifieringslösningar, säker infrastruktur för kommunikation, registerhantering och lagstiftning kopplad till dessa lösningar samt, inte minst, gemensamma sammanhållna kundmöten i livshändelser. Statskontoret delar denna bild och har konstaterat att bristen på samordning bl.a. leder till att medborgare i vissa fall måste vända sig till flera olika aktörer för ett och samma ärende och att offentlig sektor sällan följer upp om enskilda digitala tjänster levererar utlovade effekter i form av medborgarnytta eller effektivisering (Statskontoret, Delegerad digitalisering, 2014:12).

Det finns därför behov av att stödja utveckling och användning av gemensamma digitala lösningar. Gemensamma digitala lösningar kan utgöras av lösningar som används av hela den offentliga sektorn, sektorspecifika lösningar och lösningar som utvecklas i samverkan mellan ett fåtal myndigheter. Med nationella digitala tjänster avses de gemensamma digitala lösningar som är av infrastrukturkaraktär och som utgör en avgörande förutsättning för offentlig e-tjänstutveckling i sin helhet. De nationella digitala tjänsterna ska kunna användas inom hela den offentliga sektorn och syftar till att underlätta elektronisk hantering av ärenden och kontakter med enskilda. Exempel på sådana befintliga tjänster är Mina meddelanden och Svensk e-legitimation. Tjänsterna ska utvecklas utifrån medborgarnas behov, vilket förutsätter en bred och omfattande samverkan mellan statliga myndigheter, mellan kommunala myndigheter, mellan stat och kommun samt mellan offentlig och privat sektor.

Mina meddelanden är en infrastruktur för att skicka säkra elektroniska försändelser från myndigheter till enskilda. Skatteverket ansvarar för infrastrukturen, som 2016 finansieras av 14 statliga myndigheter i frivillig samverkan. Regeringen har satt upp målet att stora och mellanstora myndigheter ska ha anslutit relevanta meddelandeflöden till Mina meddelanden senast 2017. Skatteverket erbjuder inom infrastrukturen för Mina meddelanden även den digitala brevlådan Min myndighetspost till privatpersoner och företag. Privata brevlådeoperatörer kan ansluta till infrastrukturen om de uppfyller fastställda krav. Privatpersoner väljer vilken brevlåda de vill ha sin myndighetspost till när de anmäler sig till Mina meddelanden.

Svensk e-legitimation är en infrastruktur för elektronisk legitimering som är under utveckling. Den senaste versionen omfattar bl.a. kvalitetsmärkning, teknisk arkitektur och samordnad försörj-

ning av tjänster för elektronisk legitimering och underskrift. En särskild lag, lagen (2013:311) om valfrihetssystem i fråga om tjänster för elektronisk identifiering, har stiftats för att reglera offentlig sektors försörjning av tjänsterna. E-legitimationsnämnden ansvarar för infrastrukturen. Myndigheter ansluter sig på frivillig basis genom att teckna avtal med E-legitimationsnämnden. Infrastrukturen finansieras genom avgifter från anslutande myndigheter. Regeringen har satt upp målet att Svensk e-legitimation ska vara infört 2016.

Uppdraget att analysera och ge förslag till effektiv styrning av utveckling, införande och förvaltning av nationella digitala tjänster

Digitaliseringen skapar nya möjligheter för statsförvaltningen att bli mer innovativ och samverkande. Genom att myndigheterna samverkar digitalt kan kontakterna med medborgarna förenklas och innovation och delaktighet stödjas, samtidigt som statsförvaltningens effektivitet och kvaliteten på dess arbete kan höjas (se Med medborgaren i centrum – regeringens strategi för en digital samverkande statsförvaltning, dnr N2012/06402/ITP).

Digitaliseringskommissionen, E-delegationen och Statskontoret har i olika utredningar bedömt att potentialen i de nationella digitala tjänsterna fortfarande till stora delar är outnyttjad. Detta anses framför allt bero på olösta frågor kring styrning, organisering och finansiering av införandet av digitala tjänster. Organiseringen och styrningen inom området har hanterats på ett decentraliserat sätt som bygger på samverkan och en hög grad av frivillighet från myndigheternas sida. De enskilda myndigheterna ansvarar för utveckling, införande och förvaltning samtidigt som regeringens organisering och styrning av de nationella digitala tjänsterna uppfattas som otydlig.

En annan avgörande framgångsfaktor för de nationella digitala tjänsterna är anslutningsgraden. Mina meddelanden innebär, vid hög anslutningsgrad av både avsändare och mottagare, stor nytta för såväl avsändare som mottagare. Möjligheten att ansluta frivilligt har emellertid hittills resulterat i en anslutningsgrad som är så låg att nyttan är starkt begränsad för både avsändare och mottagare, varför åtgärder och incitament för ökad användning måste övervägas. Motsvarande problembild finns även för Svensk e-legitimation, där anslutningsgraden alltjämt är låg bland såväl myndigheter som leveran-

törer, vilket bl.a. resulterat i behov av temporära övergångslösningar för att tillgodose offentlig sektors försörjning av e-legitimationstjänster.

Både Mina meddelanden och Svensk e-legitimation bygger på samverkan mellan offentlig och privat sektor. Privat sektors medverkan i utveckling och leverans av digitala tjänster kan bidra till ökad användarnytta, tillväxt och innovation. Det finns dock vissa specifika frågor för respektive tjänst som behöver utredas för att säkerställa att samverkan tillgodoser användarnas behov, krav på säkerhet och tillgänglighet samt regeringens mål på området.

Analysera och föreslå organisering, ansvarsfördelning och reglering av nationella digitala tjänster

I dag är ansvaret för enskilda nationella digitala tjänster fördelat mellan olika statliga myndigheter. Samverkan och ansvarsfördelning för de olika tjänsterna har utformats på olika sätt. Det finns därför behov av att analysera om det är mer ändamålsenligt med en enhetlig modell för organisering och ansvarsfördelning avseende tjänsterna, och hur en sådan modell kan utformas, för att säkerställa en mer effektiv styrning av de nationella digitala tjänsterna.

Utredaren ska därför, bl.a. med utgångspunkt i Mina meddelanden och Svensk e-legitimation, analysera skillnaderna mellan hur ansvaret för olika befintliga nationella digitala tjänster är fördelat i dag och alternativ till detta. Analysen ska utgå från ett livscykelperspektiv för de nationella digitala tjänsterna där hela kedjan från utveckling till avveckling ska beaktas. Analysen ska särskilt behandla för- och nackdelar med olika alternativ till hur ansvaret för nationella digitala tjänster ska fördelas inom offentlig sektor och om ansvaret även fortsättningsvis ska fördelas på flera myndigheter eller om det i stället bör placeras hos en och samma myndighet. Utredaren ska utifrån slutsatserna av analysen ge förslag till lämplig organisering, ansvarsfördelning och reglering av nationella digitala tjänster från utveckling till avveckling.

Utredaren ska också ge förslag till hur samverkan om t.ex. kravställning eller vidareutveckling av nationella digitala tjänster inom offentlig sektor som helhet bör ske.

Mina meddelanden regleras i dag i 5 § förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte. Enligt

1 § gäller förordningen för myndigheter under regeringen. Sedan 2013 får även kommunala myndigheter anslutas. Stora delar av kommunal verksamhet utförs i privat regi. Privata utförare har dock, med dagens reglering, inte möjlighet att ansluta som avsändare till Mina meddelanden. Utredaren ska därför ta fram förslag, inklusive eventuella författningsförslag, på hur privata utförare av offentligfinansierad verksamhet ska kunna ansluta som avsändare inom Mina meddelanden så att alla utförare av offentligfinansierad verksamhet har möjlighet att erbjuda offentlig service med hjälp av digitala tjänster på lika villkor.

För Svensk e-legitimation ska utredaren i denna del analysera och lämna förslag på organisering och ansvarsfördelning vad gäller utveckling, införande och förvaltning av attribut- och behörighetstjänster som medger att e-legitimationer kan användas i olika roller, särskilt vad gäller e-legitimation i tjänsten.

Analysera och föreslå åtgärder och incitament för ökad användning

Anslutningstakten till befintliga nationella digitala tjänster är för långsam, såväl när det gäller statliga och kommunala myndigheter som slutanvändare i form av privatpersoner och företag. Behov av åtgärder och incitament, exempelvis krav på obligatorisk anslutning eller användning, har förts fram i olika sammanhang, bl.a. i Digitaliseringskommissionens betänkande (SOU 2015:91). Flera nordiska länder har vidtagit åtgärder och genom dessa uppnått en snabbare anslutningstakt och bredare genomslag i samhället för gemensamma digitala tjänster i jämförelse med svensk förvaltning.

Utredaren ska därför analysera nytta och konsekvenser av sådana åtgärder, bl.a. obligatorisk anslutning eller avgiftsfri användning, och föreslå åtgärder för att åstadkomma en ökad användning av nationella digitala tjänster bland myndigheter, leverantörer och slutanvändare. Utredaren ska i sin analys ta hänsyn till de särskilda förutsättningar som råder för olika typer av utförare, som statliga myndigheter, kommuner och landsting samt privata utförare av offentlig verksamhet.

Utredaren ska, bl.a. med beaktande av förslaget i Digitaliseringskommissionens betänkande (SOU 2015:91) och Skatteverkets förslag om obligatorisk anslutning till Mina meddelanden för aktiebolag

(se Skatteverkets rapport Rapportering av Skatteverkets uppdrag att följa statliga myndigheters anslutning till Mina meddelanden och att verka för företags anslutningar) analysera och lämna förslag till hur en övergång till digital myndighetspost till mottagare kan genomföras i praktiken.

Offentliga digitala tjänster bör utformas på ett sådant sätt att alla människor, med olika förutsättningar och behov, kan ta del av dem. Det gäller t.ex. nedsättning av syn, hörsel och kognitiva förmågor. En annan viktig målsättning bör vara att utvecklingen av digitala tjänster bidrar till att både kvinnor och män är nöjda med och nyttjar tjänsterna i likvärdig utsträckning. Utredaren ska därför ta hänsyn till dessa målsättningar vid utformningen av förslagen.

Analysera och föreslå utformning av samverkan mellan offentlig och privat sektor

Privat sektors medverkan i utveckling och leverans av digitala tjänster är en nyckelfaktor för tillväxt och innovation samt för att tillvarata teknikens möjligheter. Ett positivt samspel mellan offentlig och privat sektor kan starkt bidra till förnyelse i offentlig verksamhet och samtidigt leda till innovation och internationell konkurrenskraft i näringslivet.

När det gäller e-legitimationsområdet har samverkan mellan privat och offentlig sektor haft positiva effekter på utvecklingen. Sverige har en mycket hög spridning och användning av säkra e-legitimationer till en förhållandevis låg kostnad i jämförelse med många andra länder. Det finns dock utmaningar i den etablerade marknadssituationen, med en stark marknadsaktör och begränsade förutsättningar för effektiv konkurrens på grund av bl.a. höga inträdesbarriärer. Mindre prioriterade användargrupper riskerar att inte inkluderas och motstridiga intressen mellan privat och offentlig sektor kan leda till att den fulla potentialen i e-legitimationen som verktyg inte kan utnyttjas. Det finns därför behov av att närmare analysera omfattningen av det offentliga åtagandet i förhållande till de privata aktörernas roll och lämna förslag på vidareutveckling av modellen för e-legitimationer för att långsiktigt tillgodose offentlig sektors och användares behov, krav på säkerhet och tillgänglighet samt regeringens mål på området. Regeringen har gett E-legitimationsnämnden i uppdrag att analysera och vid behov ompröva den modell som valts för Svensk

e-legitimation (dnr N2015/07943/EF). Uppdraget ska slutredovisas den 17 oktober 2016. Regeringsuppdraget utgör en viktig utgångspunkt för utredaren att förhålla sig till i utredningsarbetet i denna del. Utredaren ska:

- lämna förslag på långsiktig utformning av det offentliga åtagandet när det gäller ansvarsfördelningen mellan offentlig och privat sektor i processen för grundidentifiering och utfärdande av e-legitimationer så att tillgången till enkla och säkra e-legitimationer för alla säkerställs,
- analysera och lämna förslag på hur konkurrens och innovation på den privata marknaden för utfärdande av e-legitimationer kan främjas på lång sikt,
- analysera och lämna förslag på åtgärder, för såväl företag på den privata marknaden som privata utförare av offentligt finansierad verksamhet, som främjar och stöder privat sektors användning av e-legitimation, särskilt när det gäller att nyttja offentlig sektors infrastruktur.

Inom Mina meddelanden finns möjlighet för privata brevlådeoperatörer att ansluta till infrastrukturen och erbjuda sina mottagare att ta emot myndighetspost digitalt. De privata brevlådeoperatörerna får dock endast tillhandahålla brevlådor till privatpersoner. Samtidigt erbjuder Skatteverket brevlådan Min myndighetpost till både privatpersoner och företag. Brevlådeoperatörer måste uppfylla de villkor och säkerhetskrav som gäller för Mina meddelanden. Kraven medför kostnader för brevlådeoperatörerna samtidigt som de i dagsläget inte får någon ersättning för sin medverkan inom infrastrukturen. Som exempel kan nämnas kostnader till följd av kravet på inloggning med e-legitimation. Avsaknad av såväl ersättningsmodell som begränsningar i mottagarkretsen och konkurrenssituationen medför risk att de privata aktörernas medverkan, och därmed den innovation de bidrar med, hämmas. Utredaren ska därför lämna förslag, inklusive eventuella författningsförslag, på en ersättningsmodell, t.ex. i form av valfrihetssystem, för de brevlådeoperatörer som tillhandahåller brevlådor inom ramen för Mina meddelanden.

Utredaren ska även analysera om det finns generella principer som kan tillämpas för utformningen av ansvarsfördelning och samverkan mellan offentlig och privat sektor när det gäller att tillhanda-

hålla nationella digitala tjänster. Frågor att analysera inom ramen för denna del av uppdraget är t.ex.:

- vikten av medverkan från privata leverantörer av digitala tjänster för att möta förvaltningens behov över tid av bl.a. innovation och teknikutveckling,
- konkurrens och statsstöd, och
- hur kontroll och uppföljning kan ske och om civilrättslig avtalsreglering är tillräcklig och lämplig.

Hantering av vissa centrala frågeställningar vid tillämpningen av eIDAS-förordningen

Svenska myndigheter har från och med den 29 september 2018 en skyldighet att erkänna anmälda e-legitimationer från andra medlemsstater i EU i sina nationella e-tjänster. Skyldigheten följer av den s.k. eIDAS-förordningen, dvs. Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. Regeringen har föreslagit en ny lag med kompletterande bestämmelser till EU-förordningen (prop. 2015/16:72). Regeringen har även gett E-legitimationsnämnden och Skatteverket uppdrag när det gäller området elektronisk identifiering i eIDAS-förordningen. Uppdraget till E-legitimationsnämnden (dnr N2016/02305/EF) är att påbörja utvecklingen av den centrala teknisk arkitektur (nod) som krävs för att kunna hantera utländska e-legitimationer i svenska digitala tjänster enligt eIDAS--förordningen. Uppdraget till Skatteverket (dnr N2016/02307/EF) är att utreda behoven av och förutsättningarna för en samordnad tjänst för koppling mellan en utländsk e-legitimation och en individs svenska personnummer eller styrkta samordningsnummer. Regeringsuppdragen utgör viktiga utgångspunkter för utredaren att förhålla sig till i utredningsarbetet i denna del.

Det återstår dock ett antal mer komplexa frågor att utreda, bl.a. när det gäller de konsekvenser som förordningen för med sig ur ett svenskt perspektiv i fråga om erkännande av europeiska e-legitimationer och anmälan av en svensk e-legitimation, och ytterligare kompletterande åtgärder kan därför behöva vidtas. Exempelvis med-

för den svenska modellen med privata utfärdare av e-legitimation särskilda utmaningar när det gäller ansvarsfördelning och samverkan vid anmälan av en e-legitimation enligt eIDAS-förordningen. En annan utmaning är det nationella beroendet av svenskt person- eller samordningsnummer i nationella e-tjänster i förhållande till de minimipersonidentifieringsuppgifter som förmedlas via den europeiska e-legitimationen.

Utredaren ska därför utreda rättsliga, ekonomiska och verksamhetsmässiga konsekvenser för svenska myndigheter av skyldigheten att erkänna anmälda europeiska e-legitimationer och elektroniska underskrifter i nationella e-tjänster. Vidare ska utredaren analysera och lämna förslag på sådana ytterligare åtgärder som krävs för att säkerställa att Sverige kan uppfylla sina åtaganden enligt förordningen, ta till vara nytta och potential samt tillgodose svenska myndigheters behov och krav på säkerhet, spårbarhet och tillgänglighet i förhållande till förordningen. Utredaren ska särskilt analysera omfattningen av kravet på erkännande av anmälda europeiska e-legitimationer i nationella e-tjänster och vilka nödvändiga anpassningar av nationella e-tjänster som kravet i detta avseende föranleder. Utredaren ska även analysera och lämna förslag, inklusive eventuella författningsförslag, på följande specifika frågor:

- hur processen för tilldelning av samordningsnummer till utländska medborgare på distans genom e-legitimation kan möjliggöras och automatiseras,
- hur personuppgiftsansvaret bör fördelas mellan parterna, personuppgiftsansvarets omfattning samt frågor kring lämpliga persondataskyddande åtgärder och säkerställande av den personliga integriteten i kedjan av hantering av utländska personidentifieringsuppgifter,
- hur e-tjänster i privat sektor kan ges förutsättningar att använda den offentliga centrala infrastrukturen.

Utredaren ska även utreda behoven av och förutsättningarna för anmälan av svenska e-legitimationer enligt eIDAS-förordningen. Utredaren ska i denna del analysera om offentlig sektor bör ha ett åtagande när det gäller att säkerställa att svenska privatpersoner och företag kan använda e-legitimationer i utländska e-tjänster för identifiering och underskrift. Utredaren ska redovisa för- och nackdelar

med olika alternativ avseende omfattningen av ett sådant åtagande, särskilt i förhållande till den privata marknadens möjlighet och förutsättningar att tillgodose identifierade behov. Utredaren ska även analysera ekonomiska och rättsliga risker för offentlig sektor samt processuella frågor vid anmälan och efterföljande användning av en anmäld svensk e-legitimation. Vidare ska utredaren lämna förslag på lämplig ansvarsfördelning inom offentlig sektor samt mellan offentlig sektor och privata utfärdare av e-legitimation vid anmälan av en svensk e-legitimation. Utredaren ska även analysera och lämna förslag, inklusive eventuella författningsförslag, på följande specifika frågor:

- hur privata utfärdare av e-legitimation kan ersättas vid användning av en anmäld e-legitimation i utländska e-tjänster, såväl i förhållande till offentlig som privat sektor, och
- om svenska personnummer och samordningsnummer bör överföras vid användning av en svensk e-legitimation i utländska e-tjänster och möjligheten och lämpligheten att i stället använda en pseudonym.

Utredaren ska även översiktligt kartlägga vilka svenska tjänster som kan komma att omfattas av eIDAS-förordningens krav på betrodda tjänster och offentlig förvaltnings förväntade framtida behov av sådana tjänster.

Konsekvensbeskrivningar

Utredaren ska utifrån de förslag som lämnas redovisa de konsekvenser och kostnader som uppstår för staten, för övrig offentlig sektor, för företag och för enskilda. Om förslagen påverkar kostnaderna eller intäkterna för staten, ska en beräkning redovisas. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas. När det gäller ökade kostnader och minskade intäkter för staten ska utredaren föreslå en finansiering av dessa. Om något av förslagen påverkar det kommunala självstyret ska, utöver dess konsekvenser, också de överväganden som lett fram till förslagen redovisas.

Utredaren ska i redovisningen även behandla konsekvenser för användbarhet och tillgänglighet samt integritet och säkerhet.

Samråd och redovisning av uppdraget

Utredaren ska samråda med E-legitimationsnämnden och Skatteverket samt med andra lämpliga myndigheter, företag och organisationer. Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och i EU.

Utredaren ska även ta hänsyn till pågående digitaliseringsarbeten inom olika sektorer och ta in erfarenheter från andra nationella digitala tjänster.

Uppdraget ska, när det gäller följande frågor om Mina meddelanden, redovisas i ett delbetänkande senast den 15 mars 2017:

- hur privata utförare av offentligfinansierad verksamhet ska kunna ansluta som avsändare inom Mina meddelanden,
- hur en övergång för privatpersoner och företag till digital myndighetspost kan genomföras i praktiken och
- förslag till utformning av en ersättningsmodell för de brevlådeoperatörer som tillhandahåller brevlådor inom ramen för Mina meddelanden.

Uppdraget i övrigt ska redovisas senast den 31 oktober 2017.

(Näringsdepartementet)

Kommittédirektiv 2016:97

Tilläggsdirektiv till Utredningen om effektiv styrning av nationella digitala tjänster i en samverkande förvaltning (N 2016:01)

Beslut vid regeringssammanträde den 24 november 2016

Utvidgning av och förlängd tid för uppdraget

Regeringen beslutade den 19 maj 2016 att ge en särskild utredare i uppdrag att analysera och lämna förslag till effektiv styrning av utveckling, införande och förvaltning av nationella digitala tjänster (dir. 2016:39).

Utredaren ges nu i uppdrag att analysera hur digitaliseringen i den offentliga sektorn kan stärkas genom att, inom ramen för den befintliga myndighetsstrukturen, samla ansvaret för dessa frågor till en myndighet. Utredaren ska med utgångspunkt i analysen lämna förslag till nödvändiga författningsändringar och övriga åtgärder som krävs för att en myndighet så snart som möjligt ska kunna ges den aktuella uppgiften. Uppdraget ska i denna del redovisas senast den 15 mars 2017.

Utredaren ges vidare i uppdrag att lämna förslag till en reglering som innebär en skyldighet för lämpliga statliga och kommunala myndigheter att ansluta sig till tjänsten Mina meddelanden.

Utredningstiden förlängs. Uppdraget ska, med undantag för de deluppdrag som ska redovisas senast den 15 mars 2017, i stället slutredovisas senast den 31 december samma år.

Ett samlat ansvar för digitaliseringen i den offentliga sektorn

Styrningen av digitaliseringen i den offentliga sektorn är komplex, då den omfattar fristående statliga myndigheter samt kommuner och landsting. Regeringen har hittills styrt utvecklingen genom att delegera ansvaret till kommittéer, råd och de enskilda statliga myndigheterna. Riksrevisionen har i sin granskningsrapport Den offentliga förvaltningens digitalisering – En enklare, öppnare och effektivare förvaltning? bl.a. konstaterat att detta till viss del har varit ändamålsenligt, men också lett till att utvecklingen på området inte har hanterats på ett kostnadseffektivt sätt (RiR 2016:14). E-delegationen har i flera betänkanden (SOU 2009:86, SOU 2013:75 och SOU 2015:66) framhållit behovet av ytterligare styrning. Samma behov har även identifierats av Statskontoret (Statskontoret 2014:12), Digitaliseringskommissionen (SOU 2015:91) och Ekonomistyrningsverket (ESV 2016:25).

För att stärka styrningen av samarbetet och samverkan över myndighetsgränserna på det aktuella området har regeringen i budgetpropositionen för 2017 anfört att den överväger att utse en aktör med ett samlat ansvar för digitaliseringen i den offentliga sektorn (prop. 2016/17:1 utg.omr. 22 avsnitt 4.5.1).

Genom att samla ansvaret i en myndighet kan styrningen av digitaliseringen i den offentliga sektorn effektiviseras, samtidigt som förutsättningarna för en medborgarcentrerad, innovativ och effektiv verksamhetsutveckling förbättras.

Utredaren ges mot denna bakgrund i uppdrag att

- analysera hur digitaliseringen i den offentliga sektorn kan stärkas genom att, inom ramen för den befintliga myndighetsstrukturen, samla ansvaret för dessa frågor till en myndighet,
- redovisa för- och nackdelar med ett samlat ansvar samt överväga och redogöra för när ansvaret som tidigast kan överföras,
- utifrån ovanstående analys lämna förslag till myndighetens nya uppgift och befogenheter, och i samband med detta överväga om det finns anledning att ändra myndighetens ledningsform,
- lämna förslag till finansiering av den nya verksamheten, och
- lämna förslag till nödvändiga författningsändringar och övriga åtgärder som krävs för att myndigheten så snart som möjligt ska kunna ges den aktuella uppgiften.

Anslutningen till tjänsten Mina meddelanden

Anslutningen till den nationella digitala tjänsten Mina meddelanden är enligt regeringen för låg för att tjänsten ska vara effektiv (prop. 2016/17:1 utg.omr. 22 avsnitt 4.4.2). Enligt de ursprungliga direktiven ska utredaren lämna förslag till utformning av åtgärder och incitament för att uppnå en ökad användning av de nationella digitala tjänsterna bland myndigheter, leverantörer och slutanvändare, dvs. alla befintliga aktörer inom Mina meddelanden. Utredaren ska också lämna förslag till hur en övergång till digital myndighetspost ska ske för privatpersoner och företag. Införandet av en skyldighet för kommuner och landsting att ansluta sig till Mina meddelanden skulle dock innebära ett nytt åtagande för dem, vilket kräver stöd i lag.

Utredaren ges mot denna bakgrund i uppdrag att

- lämna förslag till en reglering som innebär en skyldighet för lämpliga statliga och kommunala myndigheter att ansluta sig till tjänsten,
- göra urvalet av myndigheter utifrån en helhetsbedömning av bl.a. omfattningen av myndigheternas kontakter med privatpersoner och företag, och
- i sin analys av urvalet ta hänsyn till de olika förutsättningar som gäller för statliga myndigheter, kommuner och landsting samt beakta och redovisa sina överväganden med anledning av regleringen i 14 kap. 3 § regeringsformen om inskränkningar i den kommunala självstyrelsen.

Samråd och redovisning av uppdraget

Den del av uppdraget som avser att samla ansvaret för digitaliseringen i den offentliga sektorn ska redovisas senast den 15 mars 2017.

Utredningstiden förlängs. Uppdraget ska, med undantag för de deluppdrag som ska redovisas senast den 15 mars 2017, i stället slutredovisas senast den 31 december samma år.

(Finansdepartementet)

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) nr 910/2014

av den 23 juli 2014

om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande [1],

i enlighet med det ordinarie lagstiftningsförfarandet [2], och

av följande skäl:

(1) Att bygga upp förtroendet för nätmiljön är avgörande för den ekonomiska och sociala utvecklingen. Bristande förtroende, särskilt på grund av upplevd brist på rättssäkerhet, gör att konsumenter, företag och offentliga myndigheter tvekar att utföra transaktioner på elektronisk väg och att använda nya tjänster.

(2) Syftet med denna förordning är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag och offentliga myndigheter, och därigenom öka effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen.

(3) Europaparlamentet och rådets direktiv 1999/93/EG [3] gällde elektroniska underskrifter utan att skapa ett heltäckande, gräns- och sektorsöverskridande regelverk för säkra, pålitliga och lättanvända elektroniska transaktioner. Genom denna förordning stärks och utvidgas det direktivets regelverk.

(4) I kommissionens meddelande av den 26 augusti 2010 med titeln *En digital agenda för Europa* utpekades fragmenteringen av den digitala marknaden, bristen på interoperabilitet och den ökande it-brottsligheten som viktiga hinder för en positiv spiral för den digitala ekonomin. I sin rapport om EU-medborgarskapet 2010 med titeln *Att undanröja hindren för EU-medborgarnas möjligheter att utöva sina rättigheter* betonade kommissionen ytterligare vikten av att undanröja de största hindren för att unionsmedborgarna ska kunna utnyttja fördelarna med en digital inre marknad och gränsöverskridande digitala tjänster.

(5) I sina slutsatser av den 4 februari 2011 och den 23 oktober 2011 uppmanade Europeiska rådet kommissionen att se till att en digital inre marknad skapas senast 2015, att göra snabba framsteg på centrala områden inom den digitala ekonomin och att främja en fullständigt integrerad digital inre marknad genom att underlätta gränsöverskridande användning av nättjänster, med särskild fokus på att underlätta säker elektronisk identifiering och autentisering.

[1] EUT C 351, 15.11.2012, s. 73.
[2] Europaparlamentets ståndpunkt av den 3 april 2014 (ännu ej offentliggjord i EUT) och rådets beslut av den 23 juli 2014.
[3] Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12).

(6) I sina slutsatser av den 27 maj 2011 uppmanade rådet kommissionen att bidra till den digitala marknaden genom att skapa lämpliga förhållanden för ömsesidigt gränsöverskridande erkännande av grundläggande funktioner såsom elektronisk identifiering, elektroniska dokument, elektroniska underskrifter och elektroniska leveranstjänster samt för interoperabla e-förvaltningstjänster i hela EU.

(7) Europaparlamentet betonade, i sin resolution av den 21 september 2010 om fullbordandet av den inre marknaden för e-handel ([1]), betydelsen av säkerhet i elektroniska tjänster, särskilt i elektroniska underskrifter, och behovet av att skapa en infrastruktur för kryptering med öppen nyckel (PKI) i hela Europa samt uppmanade kommissionen att inrätta en europeisk nätverkssport för valideringsmyndigheter för att garantera gränsöverskridande interoperabilitet för elektroniska underskrifter och öka säkerheten i samband med transaktioner som görs via internet.

(8) Enligt Europaparlamentets och rådets direktiv 2006/123/EG ([2]) ska medlemsstaterna inrätta "gemensamma kontaktpunkter" för att se till att alla förfaranden och formaliteter som är nödvändiga för tillträde till en tjänsteverksamhet och för att utöva den kan fullgöras enkelt, på distans och på elektronisk väg, via den lämpliga gemensamma kontaktpunkten och med behöriga myndigheter. Många nättjänster som är tillgängliga via gemensamma kontaktpunkter kräver elektronisk identifiering, autentisering och underskrift.

(9) I de flesta fall kan medborgare inte använda sin elektroniska identifiering för att autentisera sig i en annan medlemsstat därför att de nationella systemen för elektronisk identifiering i deras land inte är erkända i andra medlemsstater. Detta elektroniska hinder utestänger tillhandahållare av tjänster från möjligheten att fullt ut utnyttja fördelarna med den inre marknaden. Ömsesidigt erkända medel för elektronisk identifiering kommer att underlätta tillhandahållandet av en rad olika tjänster över gränserna på den inre marknaden och ge företagen möjlighet att verka över gränserna utan att stöta på en mängd hinder i sina kontakter med myndigheter.

(10) Genom Europaparlamentets och rådets direktiv 2011/24/EU ([3]) inrättades ett nätverk av nationella myndigheter som är ansvariga för e-hälsa. I syfte att öka säkerheten och kontinuiteten i gränsöverskridande hälso- och sjukvård ska nätverket utarbeta riktlinjer om tillgång till elektroniska hälso- och sjukvårdsuppgifter samt tjänster, inklusive genom att stödja "gemensamma åtgärder för identifiering och autentisering för att underlätta överförbara uppgifter i gränsöverskridande hälso- och sjukvård". Ömsesidigt erkännande av elektronisk identifiering och autentisering är en förutsättning för att gränsöverskridande sjukvård ska kunna bli verklighet för Europas befolkning. Om personer reser för att söka vård måste deras sjukjournaler vara tillgängliga i behandlingslandet. Detta förutsätter robusta, säkra och tillförlitliga ramar för elektronisk identifiering.

(11) Denna förordning bör tillämpas i full överensstämmelse med de principer om skydd av personuppgifter som föreskrivs i Europaparlamentets och rådets direktiv 95/46/EG ([4]). Vad gäller principen om ömsesidigt erkännande som fastställs genom denna förordning bör autentisering för en nättjänst endast avse behandling av den identifieringsinformation som är adekvat, relevant och som inte går utöver vad som är nödvändigt för att få tillgång till den aktuella nättjänsten. Därtill bör kraven i direktiv 95/46/EG om sekretess och säkerhet vid behandling följas av tillhandahållaren av betrodda tjänster och tillsynsorgan.

(12) Ett av målen för denna förordning är att undanröja befintliga hinder för den gränsöverskridande användningen av medel för elektronisk identifiering som används i medlemsstaterna för autentisering för åtminstone offentliga tjänster. Denna förordning syftar inte till att ingripa i fråga om elektroniska identitetshanteringssystem och tillhörande infrastrukturer som inrättats i medlemsstaterna. Syftet med denna förordning är att se till att säker elektronisk identifiering och autentisering för åtkomst till gränsöverskridande nättjänster som erbjuds av medlemsstaterna är möjlig.

([1]) EUT C 50 E, 21.2.2012, s. 1.
([2]) Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (EUT L 376, 27.12.2006, s. 36).
([3]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).
([4]) Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

(13) Medlemsstaterna bör även fortsättningsvis ha rätt att för elektronisk identifiering använda eller införa medel för åtkomst till nättjänster. De bör även ha möjlighet att själva bestämma om de vill engagera den privata sektorn i tillhandahållandet av dessa medel. Medlemsstaterna bör inte vara skyldiga att anmäla sina system för elektronisk identifiering till kommissionen. Det ankommer på medlemsstaterna att välja om de till kommissionen vill anmäla alla, några eller inga av de elektroniska identifieringssystem som används på nationell nivå för att få åtkomst till åtminstone offentliga nättjänster eller särskilda nättjänster.

(14) I förordningen bör vissa villkor fastställas rörande vilka medel för elektronisk identifiering som måste erkännas och hur systemen för elektronisk identifiering bör anmälas. Dessa villkor bör hjälpa medlemsstaterna att bygga upp det förtroende som krävs för varandras system för elektronisk identifiering samt att ömsesidigt erkänna medel för elektronisk identifiering som ingår i deras anmälda system. Principen om ömsesidigt erkännande bör gälla om den anmälande medlemsstatens system för elektronisk identifiering uppfyller villkoren för anmälan och om anmälan har offentliggjorts i *Europeiska unionens officiella tidning*. Principen om ömsesidigt erkännande bör dock endast avse autentisering för en nättjänst. Åtkomsten till dessa nättjänster och deras slutliga leverans till den sökande bör vara nära kopplad till rätten att ta emot sådana tjänster enligt villkoren i nationell lagstiftning.

(15) Skyldigheten att erkänna medel för elektronisk identifiering bör enbart avse medel vars identifieringstillitsnivå motsvarar en nivå som är lika hög eller högre än den nivå som krävs för den aktuella nättjänsten. Den skyldigheten bör dessutom endast tillämpas när det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till den nättjänsten. Medlemsstaterna bör ha rätt att, i enlighet med unionsrätten, erkänna medel för elektronisk identifiering med lägre identifieringstillitsnivåer.

(16) Tillitsnivåerna bör återge graden av tillit till ett medel för elektronisk identifiering vid fastställande av en persons identitet och skapa visshet om att den person som gör anspråk på en viss identitet faktiskt är den person som har tilldelats denna identitet. Tillitsnivån beror på den grad av tillit detta medel för elektronisk identifiering ger i fråga om en persons påstådda eller styrkta identitet med beaktande av olika processer (t.ex. styrkande och kontroll av identitet, och autentisering), förvaltningsverksamhet (t.ex. den enhet som utfärdar medel för elektronisk identifiering och förfaranden för att utfärda sådana medel) och de tekniska kontroller som tillämpas. Det finns olika tekniska definitioner och beskrivningar av tillitsnivåer tack vare unionsfinansierade storskaliga pilotprojekt, standardiseringsarbete och internationell verksamhet. Det storskaliga pilotprojektet Stork och ISO 29115 avser, bland annat, nivåerna 2, 3 och 4, som bör tas under noggrant övervägande vid fastställandet av minsta tekniska krav, standarder och förfaranden för tillitsnivåerna låg, väsentlig och hög enligt denna förordning, samtidigt som en konsekvent tillämpning av denna förordning säkerställs med särskilt hänseende på tillitsnivån hög i samband med styrkande av identitet för utfärdande av kvalificerade certifikat. De fastställda kraven ska vara teknikneutrala. Det ska vara möjligt att uppnå de nödvändiga tekniska kraven med hjälp av olika tekniklösningar.

(17) Medlemsstaterna bör uppmana den privata sektorn att frivilligt använda medel för elektronisk identifiering inom ramen för ett anmält system för identifieringsändamål när detta behövs för nättjänster eller elektroniska transaktioner. Genom möjligheten att använda sådana medel för elektronisk identifiering kan den privata sektorn förlita sig på elektronisk identifiering och autentisering som redan i stor utsträckning används i många medlemsstater för åtminstone offentliga tjänster, samtidigt som det blir lättare för företag och medborgare att få åtkomst till sina gränsöverskridande nättjänster. För att göra det lättare för den privata sektorn att använda sådana gränsöverskridande medel för elektronisk identifiering bör den autentiseringsmöjlighet som tillhandahålls av en medlemsstat vara tillgänglig för de förlitande parter i den privata sektorn som är etablerade utanför denna medlemsstats territorium på samma villkor som för de förlitande parter i den privata sektorn som är etablerade i denna medlemsstat. Med hänsyn till förlitande parter i den privata sektorn får den anmälande medlemsstaten fastställa villkor för åtkomst till medlen för autentisering. Sådana villkor för åtkomst kan innehålla uppgift om huruvida medlen för autentisering för det anmälda systemet för närvarande är tillgängliga för förlitande parter i den privata sektorn.

(18) I denna förordning bör det föreskrivas skadeståndsansvar för den anmälande medlemsstaten, den part som utfärdar medlet för elektronisk identifiering och den part som handhar autentiseringsförfarandet vid underlåtenhet att uppfylla relevanta skyldigheter enligt denna förordning. Denna förordning bör dock tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar. Den ska därför inte påverka tillämpningen av dessa nationella bestämmelser om t.ex. definition av skada eller relevanta tillämpliga förfaranderegler, inbegripet regler om bevisbörda.

(19) Säkerheten i system för elektronisk identifiering är avgörande för ett tillförlitligt gränsöverskridande ömsesidigt erkännande av medel för elektronisk identifiering. Mot denna bakgrund bör medlemsstaterna samarbeta med avseende på säkerheten och interoperabiliteten i systemen för elektronisk identifiering på unionsnivå. När system för elektronisk identifiering kräver att förlitande parter på nationell nivå använder särskild maskinvara eller programvara förutsätter den gränsöverskridande interoperabiliteten att dessa medlemsstater inte inför sådana krav och därtill hörande kostnader för förlitande parter som är etablerade utanför deras territorium. I så fall bör lämpliga lösningar diskuteras och utvecklas inom interoperabilitetsramverkets räckvidd. Tekniska krav som har sin grund i de inneboende specifikationerna för nationella medel för elektronisk identifiering som sannolikt berör innehavarna av sådana elektroniska medel (t.ex. smartkort) är däremot oundvikliga.

(20) Medlemsstaternas samarbete bör underlätta den tekniska interoperabiliteten för de anmälda systemen för elektronisk identifiering i syfte att främja en hög nivå av förtroende och en säkerhetsnivå som är anpassad till risknivån. Ett utbyte av information och bästa praxis mellan medlemsstaterna med sikte på ömsesidigt erkännande bör bidra till detta samarbete.

(21) Genom denna förordning bör även ett allmänt regelverk för användningen av betrodda tjänster upprättas. Någon allmän skyldighet att använda dem eller att installera en accesspunkt för alla befintliga betrodda tjänster bör dock inte skapas. I synnerhet bör den inte gälla tillhandahållande av tjänster som endast används inom slutna system mellan en avgränsad uppsättning deltagare, och som inte påverkar tredje man. Exempelvis system som inrättats i företag eller offentlig förvaltning för hantering av interna förfaranden där betrodda tjänster används bör inte omfattas av kraven i denna förordning. Endast betrodda tjänster som tillhandahålls för allmänheten och som påverkar tredje man bör uppfylla de krav som fastställs i denna förordning. Denna förordning bör inte heller gälla frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser om nationell rätt eller unionsrätten föreskriver vissa formkrav. Den bör inte heller inverka på nationella formkrav avseende offentliga register, i synnerhet inte kommersiella register eller fastighetsregister.

(22) För att bidra till deras allmänna gränsöverskridande användning bör det vara möjligt att använda betrodda tjänster som bevis vid rättsliga förfaranden i alla medlemsstater. Rättsverkan av betrodda tjänster ska definieras i nationell rätt, om inte annat föreskrivs i denna förordning.

(23) I den mån denna förordning medför en skyldighet att erkänna en betrodd tjänst, får en sådan betrodd tjänst ogillas endast om skyldighetens adressat av tekniska skäl bortom adressatens direkta kontroll är oförmögen att läsa eller kontrollera den. Denna skyldighet bör dock inte i sig medföra att ett offentligt organ är tvunget att anskaffa den maskinvara och programvara som krävs för teknisk läsbarhet för alla befintliga betrodda tjänster.

(24) Medlemsstaterna får behålla eller införa nationella bestämmelser, i överensstämmelse med unionsrätten, avseende betrodda tjänster så länge dessa tjänster inte har harmoniserats fullständigt genom denna förordning. Betrodda tjänster som överensstämmer med denna förordning bör dock omfattas av fri rörlighet på den inre marknaden.

(25) Utöver de tjänster som ingår i den fasta förteckning över betrodda tjänster som avses i denna förordning bör medlemsstaterna ha frihet att fastställa andra typer av betrodda tjänster för erkännande på nationell nivå som kvalificerade betrodda tjänster.

(26) På grund av den snabba tekniska utvecklingen bör denna förordning omfatta en strategi som är öppen för innovation.

(27) Denna förordning bör vara teknikneutral. Den rättsliga verkan som den medför bör vara möjlig att uppnå med alla typer av tekniska medel, förutsatt att kraven i denna förordning är uppfyllda.

(28) För att framför allt öka små och medelstora företags samt konsumenternas förtroende för den inre marknaden och för att främja användningen av betrodda tjänster och produkter, bör begreppen kvalificerade betrodda tjänster och kvalificerad tillhandahållare av betrodda tjänster införas i syfte att ange krav och skyldigheter som säkerställer hög grad av säkerhet oavsett vilken typ av kvalificerad betrodd tjänst eller produkt som används eller tillhandahålls.

(29) I linje med de skyldigheter som följer av Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning, som godkändes genom rådets beslut 2010/48/EG ([1]), särskilt artikel 9 i konventionen, bör personer med funktionshinder kunna använda betrodda tjänster och slutanvändarprodukter som används vid tillhandahållandet av dessa tjänster på samma villkor som andra konsumenter. När det är genomförbart bör därför betrodda tjänster som tillhandahålls och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster göras tillgängliga för personer med funktionsnedsättning. Genomförbarhetsbedömningen bör inbegripa tekniska och ekonomiska överväganden.

(30) Medlemsstaterna bör utse ett eller flera tillsynsorgan för genomförandet av tillsynsverksamheten enligt denna förordning. Medlemsstaterna bör också kunna fatta beslut, efter ömsesidig överenskommelse med en annan medlemsstat, om att utse ett tillsynsorgan på den andra medlemsstatens territorium.

(31) Tillsynsorgan bör samarbeta med dataskyddsmyndigheter, t.ex. genom att informera dem om resultatet av granskningar av kvalificerade tillhandahållare av betrodda tjänster, när det förefaller ha skett en överträdelse av reglerna om skydd för personuppgifter. Bestämmelsen om information bör särskilt gälla säkerhetstillbud och personuppgiftsöverträdelser.

(32) För att öka användarnas förtroende för den inre marknaden bör det åligga alla tillhandahållare av betrodda tjänster att tillämpa goda säkerhetsförfaranden som är lämpliga i förhållande till de risker som deras verksamhet är förenad med.

(33) Bestämmelser om användningen av pseudonymer i certifikat bör inte hindra medlemsstaterna från att kräva identifiering av personer i enlighet med unionsrätten eller nationell rätt.

(34) För att säkerställa en jämförbar säkerhetsnivå i fråga om kvalificerade betrodda tjänster bör alla medlemsstater följa gemensamma grundläggande tillsynskrav. För att underlätta enhetlig tillämpning av dessa krav i hela unionen bör medlemsstaterna införa jämförbara förfaranden och utbyta information om sin tillsynsverksamhet och bästa praxis på området.

(35) Alla tillhandahållare av betrodda tjänster bör omfattas av kraven i denna förordning, särskilt de som gäller säkerhet och skadeståndsansvar, för att säkerställa vederbörlig noggrannhet, insyn och ansvarighet i sina verksamheter och tjänster. Med tanke på den typ av tjänster som de tillhandahåller bör det emellertid med avseende på dessa krav göras åtskillnad mellan kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster.

(36) Inrättandet av ett tillsynssystem för alla tillhandahållare av betrodda tjänster bör säkerställa lika villkor för säkerheten och tillförlitligheten i deras åtgärder och tjänster, och därigenom bidra till användarskyddet och till en fungerande inre marknad. Icke-kvalificerade tillhandahållare av betrodda tjänster bör omfattas av mindre omfattande, förebyggande tillsynsverksamhet i efterhand som är anpassad till arten av deras tjänster och åtgärder. Tillsynsorganet bör därför inte ha någon allmän skyldighet att utöva tillsyn av icke-kvalificerade tillhandahållare av betrodda tjänster. Tillsynsorganet bör endast vidta åtgärder när det har informerats (t.ex. av den icke-kvalificerade tillhandahållaren av betrodda tjänster själv, av ett annat tillsynsorgan, genom anmälan från en användare eller en affärspartner eller på grundval av en egen utredning) om att en icke-kvalificerad tillhandahållare av betrodda tjänster inte uppfyller kraven i denna förordning.

([1]) Rådets beslut 2010/48/EG av den 26 november 2009 om ingående från Europeiska gemenskapens sida av Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning (EUT L 23, 27.1.2010, s. 35).

(37) Denna förordning bör föreskriva skadeståndsansvar för alla tillhandahållare av betrodda tjänster. Den fastställer särskilt det system för skadeståndsansvar enligt vilket alla tillhandahållare av betrodda tjänster bör ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person genom underlåtenhet att uppfylla kraven i denna förordning. För att underlätta bedömningen av den ekonomiska risk som tillhandahållare av betrodda tjänster kan vara tvungna att bära eller som de bör täcka genom försäkring, tillåts tillhandahållare av betrodda tjänster genom denna förordning att på vissa villkor fastställa begränsningar för användningen av de tjänster de tillhandahåller, varvid de inte ska hållas ansvariga för skada som uppkommit genom sådan användning av tjänster som överskrider dessa begränsningar. Kunder bör vederbörligen informeras i förväg om begränsningarna. Sådana begränsningar bör vara igenkännliga för tredje man, t.ex. genom att information om begränsningarna bifogas villkoren för den tillhandahållna tjänsten eller genom andra igenkännliga medel. För att dessa principer ska kunna genomföras bör denna förordning tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar. Denna förordning påverkar därför inte dessa nationella bestämmelser om t.ex. definitionen av skada, avsikt, oaktsamhet eller relevanta tillämpliga procedurregler.

(38) Det är mycket viktigt att säkerhetsincidenter och bedömningar av säkerhetsrisker anmäls så att berörda parter kan förses med tillräcklig information i händelse av en säkerhetsincident eller en integritetsförlust.

(39) För att kommissionen och medlemsstaterna ska kunna bedöma hur effektiv den mekanism för anmälan av överträdelser som införs genom denna förordning är, bör tillsynsorganen vara skyldiga att överlämna sammanfattande information till kommissionen och till Europeiska byrån för nät- och informationssäkerhet (Enisa).

(40) För att kommissionen och medlemsstaterna ska kunna bedöma hur effektiv den förstärkta tillsynsmekanism som införs genom denna förordning är, bör tillsynsorganen vara skyldiga att rapportera om sin verksamhet. Detta skulle kraftigt bidra till att underlätta utbytet av god praxis mellan tillsynsorganen och säkerställa kontrollen av att väsentliga tillsynskrav genomförs på ett enhetligt och verkningsfullt sätt i alla medlemsstater.

(41) För att säkerställa att kvalificerade betrodda tjänster är hållbara och varaktiga samt för att öka användarnas förtroende för kontinuiteten i dessa tjänster, bör tillsynsorganen kontrollera befintlighet och korrekt tillämpning av bestämmelser om planer för verksamhetens upphörande när kvalificerade tillhandahållare av betrodda tjänster upphör med sin verksamhet.

(42) För att underlätta tillsynen av kvalificerade tillhandahållare av betrodda tjänster, t.ex. när en sådan tillhandahåller sina tjänster i en annan medlemsstat och inte omfattas av tillsyn där, eller när en tillhandahållares datorer är placerade i en annan medlemsstat än den där tillhandahållaren är etablerad, bör ett system för ömsesidigt bistånd mellan medlemsstaternas tillsynsorgan inrättas.

(43) För att säkerställa att kvalificerade tillhandahållare av betrodda tjänster och de tjänster de tillhandahåller uppfyller de krav som fastställs i denna förordning bör en bedömning av överensstämmelse utföras av organ för bedömning av överensstämmelse, och de rapporter om överensstämmelsebedömning dessa resulterar i bör av den kvalificerade tillhandahållaren av betrodda tjänster lämnas in till tillsynsorganet. Om tillsynsorganet begär att en kvalificerad tillhandahållare av betrodda tjänster ska lämna in en särskild rapport om överensstämmelsebedömning, bör tillsynsorganet särskilt respektera principen om god förvaltning, inbegripet skyldigheten att motivera beslut, samt proportionalitetsprincipen. Tillsynsorganet bör därför vederbörligen motivera sitt beslut om krav på särskild överensstämmelsebedömning.

(44) Målet med denna förordning är att säkerställa ett konsekvent ramverk i syfte att tillhandahålla en hög nivå av säkerhet och rättssäkerhet för betrodda tjänster. I detta avseende bör kommissionen när den behandlar bedömning av överensstämmelse av produkter och tjänster i tillämpliga fall söka synergier med befintliga relevanta europeiska och internationella system så som Europaparlamentets och rådets förordning (EG) nr 765/2008 [1] om krav för ackreditering av organ för bedömning av överensstämmelse och marknadskontroll av produkter.

[1] Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

(45) För att få till stånd en effektiv initieringsprocess, som bör leda till att kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster de tillhandahåller införs i förteckningar över betrodda tjänsteleverantörer, bör man uppmuntra inledande kontakter mellan potentiella kvalificerade tillhandahållare av betrodda tjänster och behöriga tillsynsorgan, i syfte att underlätta den *due diligence*-granskning som ska leda fram till tillhandahållandet av kvalificerade betrodda tjänster.

(46) Förteckningar över betrodda tjänsteleverantörer kan vara viktiga för att hjälpa till att bygga upp förtroendet bland aktörer på marknaden, eftersom de visar att tillhandahållaren av tjänster vid tidpunkten för tillsynen hade status som kvalificerad.

(47) För att användare ska kunna dra full nytta av och veta att de kan förlita sig på nättjänster är det nödvändigt att de har förtroende för nättjänsterna och att dessa är lättillgängliga. Det bör därför inrättas ett EU-förtroendemärke för att identifiera kvalificerade betrodda tjänster som tillhandhålls av kvalificerade tillhandahållare av betrodda tjänster. Ett sådant EU-förtroendemärke av kvalificerade betrodda tjänster skulle göra tydlig åtskillnad mellan kvalificerade betrodda tjänster och andra betrodda tjänster och på så sätt bidra till insynen på marknaden. Det bör vara frivilligt för kvalificerade tillhandahållare av betrodda tjänster att använda sig av ett EU-förtroendemärke och detta bör inte medföra några andra krav än de som föreskrivs i denna förordning.

(48) Det krävs en hög tillitsnivå för att säkerställa ömsesidigt erkännande av elektroniska underskrifter, men i vissa fall, som t.ex. inom ramen för kommissionens beslut 2009/767/EG [1] bör även elektroniska underskrifter med en lägre säkerhetsgrad godtas.

(49) Denna förordning bör fastställa principen om att en elektronisk underskrift inte bör förvägras rättslig verkan på grund av att den har elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk underskrift. Den rättsliga verkan av elektroniska underskrifter ska emellertid definieras i nationell rätt, med undantag för kraven i denna förordning på att en kvalificerad elektronisk underskrift ska ha samma rättsliga verkan som en handskriven underskrift.

(50) Eftersom behöriga myndigheter i medlemsstaterna för närvarande använder olika avancerade elektroniska underskrifter av olika format för att underteckna sina dokument elektroniskt är det nödvändigt att se till att åtminstone ett visst antal format av avancerade elektroniska underskrifter kan stödjas tekniskt av medlemsstaterna när de erhåller dokument som undertecknats elektroniskt. På samma sätt skulle det när behöriga myndigheter i medlemsstaterna använder avancerade elektroniska stämplar vara nödvändigt att se till att de stöder åtminstone ett visst antal format av avancerade elektroniska stämplar.

(51) Det bör vara möjligt för undertecknare att anförtro anordningar för skapande av kvalificerade elektroniska underskrifter till tredje man, förutsatt att lämpliga mekanismer och förfaranden tillämpas för att se till att undertecknaren har användningen av sina uppgifter för skapande av elektroniska underskrifter uteslutande under sin egen kontroll och att kraven för kvalificerade elektroniska underskrifter uppfylls genom anordningens användning.

(52) Om miljön för skapande av elektroniska underskrifter styrs av en tillhandahållare av betrodda tjänster på uppdrag av undertecknaren, kommer elektroniska underskrifter på distans med säkerhet att utvecklas på grund av sina många ekonomiska fördelar. För att säkerställa att dessa elektroniska underskrifter får samma rättsliga erkännande som elektroniska underskrifter som skapas i en miljö som helt och hållet styrs av användaren bör emellertid tillhandahållare av tjänster för elektroniska underskrifter på distans tillämpa särskilda säkerhetsförfaranden för förvaltning och administration samt använda tillförlitliga system och produkter, bland annat säkra elektroniska kommunikationskanaler, för att säkerställa en tillförlitlig miljö för skapande av elektroniska underskrifter som undertecknaren använder uteslutande under sin egen kontroll. För en kvalificerad elektronisk underskrift som skapas med en anordning för skapande av elektroniska underskrifter på distans bör de krav som gäller för kvalificerade tillhandahållare av betrodda tjänster och som anges i denna förordning tillämpas.

[1] Kommissionens beslut 2009/767/EG av den 16 oktober 2009 om åtgärder som underlättar användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden (EUT L 274, 20.10.2009, s. 36).

(53) Tillfälligt upphävande av kvalificerade certifikat är etablerad operativ praxis för tillhandahållare av betrodda tjänster i ett antal medlemsstater som skiljer sig från återkallande och medför en tillfällig förlust av giltighet för ett certifikat. Rättsäkerheten kräver att ett certifikats status som tillfälligt upphävt alltid ska anges klart och tydligt. Tillhandahållare av betrodda tjänster bör därför ansvara för att klart och tydligt ange ett certifikats status och, om detta upphävs, den exakta tidsperiod under vilket certifikatet har tillfälligt upphävts. Denna förordning bör inte ålägga tillhandahållare av betrodda tjänster eller medlemsstater att använda sig av tillfälligt upphävande men bör tillhandahålla transparensregler för när och hur en sådan möjlighet finns.

(54) Gränsöverskridande erkännande av kvalificerade elektroniska underskrifter förutsätter gränsöverskridande interoperabilitet och erkännande av kvalificerade certifikat. Därför bör inte kvalificerade certifikat omfattas av några obligatoriska krav som går utöver kraven i denna förordning. På nationell nivå bör man dock få inkludera särskilda egenskaper, t.ex. unika identifierare, i kvalificerade certifikat, under förutsättning att sådana särskilda egenskaper inte hindrar gränsöverskridande interoperabilitet och erkännande av kvalificerade certifikat och elektroniska underskrifter.

(55) It-säkerhetscertifiering som bygger på internationella standarder, såsom ISO 15408 och besläktade utvärderingsmetoder och arrangemang för ömsesidigt erkännande, utgör ett viktigt verktyg för att kontrollera säkerheten hos kvalificerade anordningar för skapande av elektroniska underskrifter och bör främjas. Innovativa lösningar och tjänster, såsom undertecknande via mobil och datamoln, förlitar sig emellertid på tekniska och organisatoriska lösningar för kvalificerade anordningar för skapande av elektroniska underskrifter, för vilka det eventuellt ännu inte finns tillgängliga säkerhetsstandarder eller för vilka den första it-säkerhetscertifieringen pågår. Säkerhetsnivån för sådana kvalificerade anordningar för skapande av elektroniska underskrifter skulle kunna utvärderas genom alternativa processer endast om sådana säkerhetsstandarder inte finns tillgängliga eller om den första it-säkerhetscertifieringen pågår. De processerna bör vara jämförbara med standarderna för it-säkerhetscertifiering i den mån deras säkerhetsnivåer är likvärdiga. Förfarandena skulle dessutom kunna underlättas av en sakkunnighetsbedömning.

(56) I denna förordning bör det fastställas krav på kvalificerade anordningar för skapande av elektroniska underskrifter för att säkerställa de avancerade elektroniska underskrifternas funktionalitet. Denna förordning bör inte omfatta hela den systemmiljö där sådana anordningar används. Därför bör omfattningen av certifieringen av kvalificerade anordningar för skapande av elektroniska underskrifter begränsas till den hårdvara och systemprogramvara som används för att hantera och skydda uppgifterna för skapande av underskrifter som skapas, lagras eller behandlas i anordningen för skapande av underskrifter. I enlighet med vad som fastställs i relevanta standarder bör certifieringsskyldigheterna inte omfatta tillämpningar för skapande av underskrifter.

(57) För att säkerställa rättssäkerheten avseende en underskrifts giltighet är det nödvändigt att specificera vilka komponenter i en kvalificerad elektronisk underskrift som bör bedömas av den förlitande part som utför valideringen. Genom att specificera kraven på kvalificerade tillhandahållare av betrodda tjänster som kan tillhandahålla en kvalificerad valideringstjänst till förlitande parter som inte själva vill eller kan utföra valideringen av kvalificerade elektroniska underskrifter bör dessutom privat och offentlig sektor stimuleras att investera i sådana tjänster. Sammantaget bör dessa krav göra kvalificerad validering av elektroniska underskrifter enkel och bekväm för alla parter på unionsnivå.

(58) När en transaktion kräver en kvalificerad elektronisk stämpel från en juridisk person bör en kvalificerad elektronisk underskrift från ett behörigt ombud för den juridiska personen vara lika godtagbar.

(59) Elektroniska stämplar bör utgöra bevis för att ett elektroniskt dokument har utfärdats av en juridisk person och säkerställa visshet om dokumentets ursprung och integritet.

(60) Tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat för elektroniska stämplar bör vidta de åtgärder som krävs för att kunna fastställa identiteten för den fysiska person som representerar den juridiska person som har fått ett kvalificerat certifikat för en elektronisk stämpel, om sådan identifiering krävs på nationell nivå inom ramen för juridiska eller administrativa förfaranden.

(61) Genom denna förordning bör långsiktigt bevarande av uppgifter säkerställas, för att säkerställa den rättsliga giltigheten hos elektroniska underskrifter och elektroniska stämplar över längre tidsperioder och garantera att de kan valideras oavsett kommande tekniska förändringar.

(62) I syfte att säkerställa säkerheten hos kvalificerad elektronisk tidsstämpling bör det i denna förordning krävas att man använder en avancerad elektronisk stämpel eller en avancerad elektronisk underskrift eller andra likvärdiga metoder. Sannolikt kan innovation leda till ny teknik som kan säkerställa en likvärdig säkerhetsnivå för tidsstämpling. Vid användning av någon annan metod än avancerade elektroniska stämplar eller avancerade elektroniska underskrifter bör det åligga tillhandahållaren av betrodda tjänster att i rapporten om bedömning av överensstämmelse visa att denna metod säkerställer en likvärdig säkerhetsnivå och att den är förenlig med skyldigheterna i denna förordning.

(63) Elektroniska dokument är viktiga för vidareutveckling av gränsöverskridande elektroniska transaktioner på den inre marknaden. Denna förordning bör fastställa principen om att ett elektroniskt dokument inte bör förvägras rättslig verkan på grund av att det har elektronisk form, för att säkerställa att elektroniska transaktioner inte kommer att ogillas enbart på grund av att ett dokument har elektronisk form.

(64) När kommissionen behandlar formaten för avancerade elektroniska underskrifter och stämplar ska den bygga vidare på den praxis, de standarder och den lagstiftning som redan finns, i synnerhet kommissionens beslut 2011/130/EU ([1]).

(65) Elektroniska stämplar kan användas för att autentisera ett dokument som utfärdats av en juridisk person, men även för att autentisera en juridisk persons digitala tillgångar, t.ex. programvarukoder eller servrar.

(66) Det är av avgörande betydelse att det föreskrivs en rättslig ram för att främja gränsöverskridande erkännande mellan befintliga nationella rättssystem för elektroniska tjänster för rekommenderade leveranser. Den ramen skulle också kunna öppna nya marknadsmöjligheter för unionens tillhandahållare av betrodda tjänster att erbjuda nya paneuropeiska tjänster för elektroniska tjänster för rekommenderade leveranser.

(67) Tjänster för autentisering av webbplatser innebär möjlighet för en besökare på en webbplats att försäkra sig om att en verklig och legitim enhet står bakom webbplatsen. Dessa tjänster bidrar till att bygga upp förtroendet för näthandeln, eftersom användarna kommer att ha förtroende för en webbplats som har autentiserats. Tillhandahållande och användning av tjänster för autentisering av webbplatser är fullständigt frivilligt. För att autentiseringen av webbplatser ska kunna bli ett sätt att stärka förtroendet, ge användaren en bättre upplevelse och främja tillväxten på den inre marknaden bör man emellertid i denna förordning föreskriva minimiskyldigheter vad gäller säkerhet och skadeståndsansvar för tillhandahållarna och deras tjänster. Därför har hänsyn tagits till resultaten av befintliga initiativ ledda av industrin, t.ex. forumet för certifieringsinstanser och försäljare av webbläsare – CA/B Forum. Dessutom bör denna förordning inte hindra användning av andra sätt eller metoder för att autentisera webbplatser som inte omfattas av denna förordning och förordningen bör inte heller hindra tillhandahållare av autentiseringstjänster i tredjeland från att tillhandahålla sina tjänster till kunder i unionen. En tillhandahållare från ett tredjeland bör dock endast kunna få sina tjänster för autentisering av webbplatser erkända som kvalificerade i enlighet med denna förordning om ett internationellt avtal mellan unionen och det land i vilket tillhandahållaren är etablerad har ingåtts.

(68) Begreppet *juridisk person* enligt bestämmelserna om etablering i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) ger aktörer möjlighet att fritt välja den juridiska form de anser vara lämplig för att bedriva sin verksamhet. Följaktligen omfattar begreppet *juridisk person* enligt EUF-fördraget alla enheter, oberoende av juridisk form, som bildats i enlighet med eller som omfattas av rätten i en medlemsstat.

(69) Unionens institutioner, organ och byråer uppmanas att erkänna elektronisk identifiering och betrodda tjänster som omfattas av denna förordning för administrativt samarbete som drar nytta av framför allt befintlig god praxis och resultaten av pågående projekt på de områden som omfattas av denna förordning.

([1]) Kommissionens beslut 2011/130/EU av den 25 februari 2011 om fastställande av minimikrav för behandling över gränserna av dokument som signerats elektroniskt av behöriga myndigheter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden (EUT L 53, 26.2.2011, s. 66).

(70) I syfte att på ett flexibelt och snabbt sätt kunna komplettera vissa detaljerade tekniska aspekter av denna förordning bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på de kriterier som ska uppfyllas av organ med ansvar för certifieringen av kvalificerade anordningar för skapande av elektroniska underskrifter. Det är av särskild betydelse att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. När kommissionen förbereder och utarbetar delegerade akter bör den se till att relevanta handlingar översänds samtidigt till Europaparlamentet och rådet och att detta sker så snabbt som möjligt och på lämpligt sätt.

(71) För att säkerställa enhetliga villkor för genomförandet av denna förordning, bör kommissionen tilldelas genomförandebefogenheter, särskilt för att ange referensnummer till standarder vilkas användning skulle skapa presumtion för överensstämmelse med vissa krav i denna förordning. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([1]).

(72) När kommissionen antar delegerade akter eller genomförandeakter bör den ta vederbörlig hänsyn till de standarder och tekniska specifikationer som utarbetats av europeiska och internationella standardiseringsorgan, särskilt Europeiska standardiseringskommittén (CEN), Europeiska institutet för telekommunikationsstandarder (Etsi), Internationella standardiseringsorganisationen (ISO) och Internationella teleunionen (ITU), i syfte att säkerställa en hög nivå av säkerhet och interoperabilitet när det gäller elektronisk identifiering och betrodda tjänster.

(73) Av rättssäkerhets- och tydlighetsskäl bör direktiv 1999/93/EG upphävas.

(74) För att säkerställa rättssäkerheten för marknadsoperatörer som redan använder kvalificerade certifikat som utfärdas för fysiska personer i enlighet med direktiv 1999/93/EG är det nödvändigt att föreskriva en tillräckligt lång övergångsperiod. Övergångsåtgärder bör även fastställas för säkra anordningar för skapande av underskrifter vars överensstämmelse har fastställts i enlighet med direktiv 1999/93/EG samt för tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat före den 1 juli 2016. Slutligen är det också nödvändigt att göra det möjligt för kommissionen att anta genomförandeakter och delegerade akter före det datumet.

(75) De tillämpningsdagar som anges i denna förordning påverkar inte medlemsstaternas befintliga skyldigheter enligt unionsrätten, särskilt direktiv 2006/123/EG.

(76) Eftersom målen för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

(77) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 ([2]) och avgav ett yttrande den 27 september 2012 ([3]).

([1]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

([2]) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

([3]) EUT C 28, 30.1.2013, s. 6.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte

I syfte att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster fastställs i denna förordning

a) de villkor på vilka medlemsstaterna erkänner medel för elektronisk identifiering av fysiska och juridiska personer som omfattas av ett anmält system för elektronisk identifiering hos en annan medlemsstat,

b) regler för betrodda tjänster, i synnerhet för elektroniska transaktioner, och

c) en rättslig ram för elektroniska underskrifter, elektroniska stämplar, elektronisk tidsstämpling, elektroniska dokument, elektroniska tjänster för rekommenderade leveranser och certifikattjänster för autentisering av webbplatser.

Artikel 2

Tillämpningsområde

1. Denna förordning gäller system för elektronisk identifiering som har anmälts av en medlemsstat, och tillhandahållare av betrodda tjänster som är etablerade inom unionen.

2. Denna förordning gäller inte tillhandahållande av betrodda tjänster som till följd av nationell rätt eller avtal mellan en avgränsad uppsättning deltagare endast används inom slutna system.

3. Denna förordning påverkar inte nationell rätt eller unionsrätt som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *elektronisk identifiering:* en process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används.

2. *medel för elektronisk identifiering:* en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster.

3. *personidentifieringsuppgifter:* en uppsättning uppgifter som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person.

4. *system för elektronisk identifiering:* ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person.

5. *autentisering:* en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form.

6. *förlitande part:* en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster.

7. *offentligt organ:* en statlig, regional eller lokal myndighet, ett organ som lyder under offentlig rätt eller en sammanslutning som bildats av en eller flera sådana myndigheter eller ett eller flera sådana offentligrättsliga organ, eller en privat enhet som av minst en av dessa myndigheter, enheter eller sammanslutningar har bemyndigats att tillhandahålla offentliga tjänster när de agerar i enlighet med ett sådant bemyndigande.

8. *offentligrättsligt organ:* ett organ enligt definitionen i artikel 2.1.4 i Europaparlamentets och rådets direktiv 2014/24/EU ([1]).

9. *undertecknare:* en fysisk person som skapar en elektronisk underskrift.

10. *elektronisk underskrift:* uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.

11. *avancerad elektronisk underskrift:* en elektronisk underskrift som uppfyller kraven enligt artikel 26.

12. *kvalificerad elektronisk underskrift:* en avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter.

13. *uppgifter för skapande av elektroniska underskrifter:* unika uppgifter som undertecknaren använder för att skapa en elektronisk underskrift.

14. *certifikat för elektroniska underskrifter:* ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk underskrift till en fysisk person och bekräftar åtminstone namnet eller pseudonymen på den personen.

15. *kvalificerat certifikat för elektroniska underskrifter:* ett certifikat för elektroniska underskrifter som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga I.

16. *betrodd tjänst:* en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

    a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

    b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

    c) bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

17. *kvalificerad betrodd tjänst:* en betrodd tjänst som uppfyller tillämpliga krav i denna förordning.

([1]) Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EU (EUT L 94, 28.3.2014, s. 65).

18. *organ för bedömning av överensstämmelse:* ett organ enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008 som i enlighet med den förordningen är ackrediterat för överensstämmelsebedömning av en kvalificerad tillhandahållare av en betrodd tjänst och den kvalificerade betrodda tjänst som denne tillhandahåller.

19. *tillhandahållare av betrodda tjänster:* en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster.

20. *kvalificerad tillhandahållare av betrodda tjänster:* en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet.

21. *produkt:* maskinvara eller programvara, eller relevanta komponenter i maskinvara eller programvara, som är avsedda att användas för tillhandahållande av betrodda tjänster.

22. *anordning för underskriftframställning:* en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift.

23. *kvalificerad anordning för underskriftframställning:* en anordning för skapande av elektroniska underskrifter som uppfyller kraven i bilaga II.

24. *skapare av en stämpel:* en juridisk person som skapar en elektronisk stämpel.

25. *elektronisk stämpel:* uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form för att säkerställa de senares ursprung och integritet.

26. *avancerad elektronisk stämpel:* en elektronisk stämpel som uppfyller kraven enligt artikel 36.

27. *kvalificerad elektronisk stämpel:* en avancerad elektronisk stämpel som skapas med hjälp av en kvalificerad anordning för skapande av elektroniska stämplar och som är baserat på ett kvalificerat certifikat för elektroniska stämplar.

28. *uppgifter för skapande av elektroniska stämplar:* unika uppgifter som skaparen av den elektroniska stämpeln använder för att skapa en elektronisk stämpel.

29. *certifikat för elektroniska stämplar:* ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk stämpel till en juridisk person och bekräftar namnet på den personen.

30. *kvalificerat certifikat för elektroniska stämplar:* ett certifikat för en elektronisk stämpel som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga III.

31. *anordning för skapande av elektroniska stämplar:* en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk stämpel.

32. *kvalificerad anordning för skapande av elektroniska stämplar:* en anordning för skapande av elektroniska stämplar som efter nödvändig anpassning uppfyller kraven i bilaga II.

33. *elektronisk tidsstämpling:* uppgifter i elektronisk form som binder andra uppgifter i elektronisk form till en viss tidpunkt och därmed utgör bevis för att de senare uppgifterna existerade vid den tidpunkten.

34. *kvalificerad elektronisk tidsstämpling:* en elektronisk tidsstämpling som uppfyller de krav som fastställs i artikel 42.

35. *elektroniskt dokument:* innehåll lagrat i elektronisk form, i synnerhet som ljud-, bild- eller audiovisuell inspelning.

36. *elektronisk tjänst för rekommenderad leverans:* en tjänst som gör det möjligt att överföra uppgifter mellan tredje män på elektronisk väg och tillhandahåller bevis avseende de överförda uppgifternas hantering, inklusive bevis för uppgifternas sändning och mottagande, och som skyddar överförda uppgifter mot risken för förlust, stöld, skada eller otillåtna ändringar.

37. *kvalificerad elektronisk tjänst för rekommenderad leverans:* en elektronisk tjänst för rekommenderad leverans som uppfyller de krav som fastställs i artikel 44.

38. *certifikat för autentisering av webbplatser*: ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för.

39. *kvalificerat certifikat för autentisering av webbplatser*: ett certifikat för autentisering av webbplatser som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga IV.

40. *valideringsuppgifter:* uppgifter som används för att validera en elektronisk underskrift eller en elektronisk stämpel.

41. *validering:* en process genom vilken en elektronisk underskrifts giltighet kontrolleras och bekräftas.

Artikel 4

Inremarknadsprincipen

1. Tillhandahållande av betrodda tjänster i en medlemsstat som utförs av en tillhandahållare av betrodda tjänster som är etablerad i en annan medlemsstat får inte begränsas av skäl som omfattas av de områden som regleras i denna förordning.

2. Produkter och betrodda tjänster som överensstämmer med denna förordning ska omfattas av fri rörlighet på den inre marknaden.

Artikel 5

Behandling och skydd av uppgifter

1. Personuppgifter ska behandlas i enlighet med direktiv 95/46/EG.

2. Utan att det påverkar rättsverkan av pseudonymer enligt nationell rätt ska användningen av pseudonymer vid elektroniska transaktioner inte förbjudas.

KAPITEL II

ELEKTRONISK IDENTIFIERING

Artikel 6

Ömsesidigt erkännande

1. När det enligt nationell rätt eller enligt nationella administrativa förfaranden krävs en elektronisk identifiering där medel för elektronisk identifiering och autentisering används för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ i en medlemsstat, ska de medel för elektronisk identifiering som utfärdats i en annan medlemsstat erkännas i den första medlemsstaten för gränsöverskridande autentisering för den tjänsten via internet, förutsatt att

a) medlet för elektronisk identifiering är utfärdat inom ramen för ett system för elektronisk identifiering som ingår i den förteckning som offentliggjorts av kommissionen enligt artikel 9,

b) tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög som eller högre än den tillitsnivå som det berörda offentliga organet kräver för åtkomst till denna nättjänst i den första medlemsstaten, förutsatt att tillitsnivån för detta medel för elektronisk identifiering motsvarar tillitsnivån väsentlig eller hög,

c) det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.

Ett sådant erkännande ska ske senast tolv månader efter det att kommissionen offentliggör den förteckning som avses i led a i första stycket.

2. Ett medel för elektronisk identifiering som utfärdats inom ramen för ett system för elektronisk identifiering som ingår i den förteckning som kommissionen offentliggjort enligt artikel 9 och som motsvarar tillitsnivån låg får erkännas av offentliga organ för gränsöverskridande autentisering för den tjänst som tillhandahålls via internet av dessa organ.

Artikel 7

Berättigande till anmälan av system för elektronisk identifiering

Ett system för elektronisk identifiering ska vara berättigat till anmälan enligt artikel 9.1 om samtliga följande villkor är uppfyllda:

a) Medlet för elektronisk identifiering inom ramen för systemet för elektronisk identifiering ska vara utfärdat

i) av den anmälande medlemsstaten,

ii) på uppdrag av den anmälande medlemsstaten, eller

iii) oberoende av den anmälande medlemsstaten och erkännas av den medlemsstaten.

b) Medlet för elektronisk identifiering inom systemet för elektronisk identifiering ska kunna användas för att få åtkomst till åtminstone en tjänst som tillhandahålls av ett offentligt organ och som kräver elektronisk identifiering i den anmälande medlemsstaten.

c) Systemet för elektronisk identifiering och det medel för elektronisk identifiering som utfärdats inom ramen för det ska uppfylla kraven för åtminstone en av de tillitsnivåer som anges i den genomförandeakt som avses i artikel 8.3.

d) Den anmälande medlemsstaten ska se till att de personidentifieringsuppgifter som unikt representerar personen i fråga, i enlighet med de tekniska specifikationer, standarder och förfaranden för den relevanta tillitsnivå som anges i den genomförandeakt som avses i artikel 8.3, tillskrivs den fysiska eller juridiska person som avses i artikel 3.1 vid tidpunkten för utfärdandet av medlet för elektronisk identifiering inom detta system.

e) Den part som utfärdar medlet för elektronisk identifiering inom detta system ska se till att medlet för elektronisk identifiering tilldelas den person som avses i led d i denna artikel i enlighet med de tekniska specifikationer, standarder och förfaranden för den relevanta tillitsnivå som anges i den genomförandeakt som avses i artikel 8.3.

f) Den anmälande medlemsstaten ska se till att autentisering är tillgänglig via internet så att alla förlitande parter som är etablerade på någon annan medlemsstats territorium kan bekräfta de personidentifieringsuppgifter som tas emot i elektronisk form.

För andra förlitande parter än offentliga organ får den anmälande medlemsstaten fastställa tillträdesvillkoren för autentiseringen. Sådan gränsöverskridande autentisering ska tillhandahållas kostnadsfritt när den utförs i samband med en nättjänst som tillhandahålls av ett offentligt organ.

Medlemsstaterna får inte ålägga förlitande parter som har för avsikt att utföra en sådan autentisering oproportionella tekniska krav om sådana krav skulle hindra eller avsevärt försvåra kompatibiliteten mellan anmälda system för elektronisk identifiering.

g) Minst sex månader före anmälan enligt artikel 9.1 ska den anmälande medlemsstaten när det gäller den skyldighet som anges i artikel 12.5 förse andra medlemsstater med en beskrivning av detta system i enlighet med de förfaranden som fastställts genom de genomförandeakter som avses i artikel 12.7.

h) System för elektronisk identifiering ska uppfylla kraven i den genomförandeakt som avses i artikel 12.8.

Artikel 8

Tillitsnivåer för system för elektronisk identifiering

1. I ett system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 ska tillitsnivåerna låg, väsentlig och/eller hög specificeras för medel för elektronisk identifiering som har utfärdats inom det systemet.

2. Tillitsnivåerna låg, väsentlig och hög ska uppfylla följande kriterier för respektive nivå:

a) Tillitsnivå låg ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en begränsad grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att väsentligt minska risken för missbruk eller ändring av identiteten.

b) Tillitsnivå väsentlig ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en väsentlig grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att väsentligt minska risken för missbruk eller ändring av identiteten.

c) Tillitsnivå hög ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en högre grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet än tillitsnivån väsentlig, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att förhindra risken för missbruk eller ändring av identiteten.

3. Senast den 18 september 2015, med beaktande av relevanta internationella standarder, och om inte annat följer av punkt 2, ska kommissionen genom genomförandeakter fastställa tekniska minimispecifikationer, standarder och förfaranden genom vilka tillitsnivåerna låg, väsentlig och hög specificeras för medel för elektronisk identifiering för tillämpningen av punkt 1.

Dessa tekniska minimispecifikationer, standarder och förfaranden ska fastställas med hänvisning till tillförlitligheten och kvaliteten i följande delar:

a) Förfarandet för att styrka och kontrollera identiteten på fysiska eller juridiska personer som ansöker om utfärdande av medel för elektronisk identifiering.

b) Förfarandet för att utfärda det begärda medlet för elektronisk identifiering.

c) Den autentiseringsmekanism genom vilken den fysiska eller juridiska personen använder medlet för elektronisk identifiering för att bekräfta sin identitet för en förlitande part.

d) Den enhet som utfärdar medlen för elektronisk identifiering.

e) Varje annat organ som deltar i ansökningen om utfärdande av medel för elektronisk identifiering.

f) De tekniska och säkerhetsrelaterade specifikationerna för de utfärdade medlen för elektronisk identifiering.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 9

Anmälan

1. Den anmälande medlemsstaten ska till kommissionen anmäla följande uppgifter samt utan onödigt dröjsmål anmäla eventuella senare ändringar av dessa:

a) En beskrivning av systemet för elektronisk identifiering, inbegripet dess tillitsnivåer och av utfärdaren eller utfärdarna av medel för elektronisk identifiering inom systemet.

b) Det tillämpliga systemet för tillsyn och information om systemet för skadeståndsansvar med avseende på följande:

i) Den part som utfärdar medlet för elektronisk identifiering.

ii) Den part som handhar autentiseringsförfarandet.

c) Den myndighet eller de myndigheter som ansvarar för systemet för elektronisk identifiering.

d) Information om den enhet eller de enheter som hanterar registreringen av de unika personidentifieringsuppgifterna.

e) En beskrivning av hur kraven i den genomförandeakt som avses i artikel 12.8 har uppfyllts.

f) En beskrivning av den autentisering som avses i artikel 7 f.

g) System för tillfälligt upphävande eller återkallelse av det anmälda systemet för elektronisk identifiering eller autentisering eller av de berörda utsatta delarna.

2. Kommissionen ska ett år från dagen för tillämpning av de genomförandeakter som avses i artiklarna 8.3 och 12.8 offentliggöra en förteckning över de system för elektronisk identifiering som anmälts enligt punkt 1 i den här artikeln och de grundläggande uppgifterna om dessa i *Europeiska unionens officiella tidning*.

3. Om kommissionen tar emot en anmälan efter utgången av den period som avses i punkt 2 ska den i *Europeiska unionens officiella tidning* offentliggöra ändringarna i den förteckning som avses i punkt 2 inom två månader från den dag då anmälan mottogs.

4. En medlemsstat får lämna in en begäran till kommissionen om att ta bort ett system för elektronisk identifiering som anmälts av medlemsstaten från den förteckning som avses i punkt 2. Kommissionen ska offentliggöra motsvarande ändringar i förteckningen i *Europeiska unionens officiella tidning* inom en månad från den dag då medlemsstatens begäran mottogs.

5. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden för de anmälningar som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 10

Säkerhetsincidenter

1. Om antingen det system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 eller den autentisering som avses i artikel 7 f utsätts för intrång eller delvis äventyras på ett sätt som påverkar tillförlitligheten i systemets gränsöverskridande autentisering ska den anmälande medlemsstaten utan dröjsmål tillfälligt upphäva eller återkalla denna gränsöverskridande autentisering eller de berörda utsatta delarna och informera andra medlemsstater och kommissionen.

2. När en incident eller ett äventyrande som avses i punkt 1 har åtgärdats ska den anmälande medlemsstaten återinföra den gränsöverskridande autentiseringen och utan onödigt dröjsmål informera andra medlemsstater och kommissionen om detta.

3. Om en incident eller ett äventyrande som avses i punkt 1 inte åtgärdas inom tre månader från det tillfälliga upphävandet eller återkallelsen, ska den anmälande medlemsstaten till övriga medlemsstater och kommissionen anmäla att systemet för elektronisk identifiering har dragits tillbaka.

Kommissionen ska utan onödigt dröjsmål offentliggöra motsvarande ändringar i den förteckning som avses i artikel 9.2 i *Europeiska unionens officiella tidning*.

Artikel 11

Skadeståndsansvar

1. Den anmälande medlemsstaten ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom dess underlåtenhet att uppfylla sina skyldigheter enligt artikel 7 d och f vid en gränsöverskridande transaktion.

2. Den part som utfärdat medlet för elektronisk identifiering ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla den skyldighet som avses i artikel 7 e vid en gränsöverskridande transaktion.

3. Den part som handhar autentiseringsförfarandet ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att säkerställa korrekt handhavande av den autentisering som avses i artikel 7 f vid en gränsöverskridande transaktion.

4. Punkterna 1, 2 och 3 ska tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar.

5. Punkterna 1, 2 och 3 påverkar inte det skadeståndsansvar enligt nationell rätt som gäller för parter i en transaktion där de använda medlen för elektronisk identifiering omfattas av det system för elektronisk identifiering som anmälts i enlighet med artikel 9.1.

Artikel 12

Samarbete och interoperabilitet

1. De nationella system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 ska vara interoperabla.

2. Med avseende på tillämpningen av punkt 1 ska ett interoperabilitetsramverk fastställas.

3. Interoperabilitetsramverket ska uppfylla följande kriterier:

a) Det ska ha som mål att vara teknikneutralt och ska inte diskriminera mellan särskilda nationella tekniska lösningar för elektronisk identifiering i en medlemsstat.

b) Det ska, när det är möjligt, följa europeiska och internationella standarder.

c) Det ska främja tillämpningen av principen om ett inbyggt integritetsskydd.

d) Det ska säkerställa att personuppgifter behandlas i enlighet med direktiv 95/46/EG.

4. Interoperabilitetsramverket ska bestå av följande:

a) Hänvisning till tekniska minimikrav avseende tillitsnivåerna i artikel 8.

b) Sammankoppling av nationella tillitsnivåer för anmälda system för elektronisk identifiering med tillitsnivåerna enligt artikel 8.

c) Hänvisning till tekniska minimikrav för interoperabilitet.

d) Hänvisning till en minimuppsättning personidentifieringsuppgifter som är unika för en fysisk eller juridisk person och som är tillgänglig via system för elektronisk identifiering.

e) Förfaranderegler.

f) Arrangemang för tvistlösning.

g) Gemensamma standarder för driftsäkerhet.

5. Medlemsstaterna ska samarbeta med avseende på följande:

a) Interoperabiliteten i de system för elektronisk identifiering som anmälts enligt artikel 9.1 och de system för elektronisk identifiering som medlemsstaterna avser att anmäla.

b) Säkerheten i systemen för elektronisk identifiering.

6. Samarbetet mellan medlemsstaterna ska bestå av följande:

a) Utbyte av information, erfarenhet och god praxis när det gäller system för elektronisk identifiering och särskilt i fråga om tekniska krav avseende interoperabilitet och tillitsnivåer.

b) Utbyte av information, erfarenheter och god praxis när det gäller arbete med tillitsnivåer för system för elektronisk identifiering enligt artikel 8.

c) Sakkunnigbedömning av system för elektronisk identifiering som omfattas av denna förordning.

d) Bedömning av relevant utveckling inom sektorn för elektronisk identifiering.

7. Senast den 18 mars 2015 ska kommissionen genom genomförandeakter fastställa nödvändiga förfaranden för att underlätta det samarbete mellan medlemsstaterna som avses i punkterna 5 och 6 i syfte att främja en hög nivå av förtroende och säkerhet som står i proportion till risknivån.

8. Senast den 18 september 2015 ska kommissionen, i enlighet med de kriterier som fastställs i punkt 3 och med beaktande av resultaten av samarbetet mellan medlemsstaterna, för att fastställa enhetliga villkor för tillämpningen av kraven i punkt 1 anta genomförandeakter om det interoperabilitetsramverk som anges i punkt 4.

9. De genomförandeakter som avses i punkterna 7 och 8 i denna artikel ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

KAPITEL III

BETRODDA TJÄNSTER

AVSNITT 1

Allmänna bestämmelser

Artikel 13

Skadeståndsansvar och bevisbörda

1. Utan att det påverkar tillämpningen av punkt 2 ska tillhandahållare av betrodda tjänster ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla kraven i denna förordning.

Bevisbördan för avsikt eller oaktsamhet hos en icke-kvalificerad tillhandahållare av betrodda tjänster ska vila på den fysiska eller juridiska person som gör gällande sådan skada som avses i första stycket.

Avsikt eller oaktsamhet hos en kvalificerad tillhandahållare av betrodda tjänster ska anses föreligga såvida inte en kvalificerad tillhandahållare av betrodda tjänster bevisar att den skada som avses i första stycket har uppstått utan avsikt eller oaktsamhet hos den kvalificerade tillhandahållaren av betrodda tjänster.

2. Om en tillhandahållare av betrodda tjänster vederbörligen informerar sina kunder i förväg om de begränsningar som gäller för användningen av de tjänster de tillhandahåller och dessa begränsningar är möjliga för tredje man att ta del av, ska tillhandahållarna av betrodda tjänster inte ha skadeståndsansvar för skador som uppstår vid sådan användning av tjänster som överskrider de angivna begränsningarna.

3. Punkterna 1 och 2 ska tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar.

Artikel 14

Internationella aspekter

1. Betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster som är etablerade i ett tredjeland ska erkännas som rättsligt likvärdiga med kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen, under förutsättning att de betrodda tjänsterna från tredjelandet är erkända enligt ett avtal som ingåtts mellan unionen och det berörda tredjelandet eller en internationell organisation i enlighet med artikel 218 i EUF-fördraget.

2. Avtal som avses i punkt 1 ska särskilt säkerställa att

a) de krav som är tillämpliga på kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen och de kvalificerade betrodda tjänster som de tillhandahåller uppfylls av tillhandahållarna av betrodda tjänster i det tredjeland eller den internationella organisation med vilket eller vilken avtalet ingås och av de betrodda tjänster som de tillhandahåller,

b) de kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen erkänns som rättsligt likvärdiga med betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster i det tredjeland eller den internationella organisation med vilket eller vilken avtalet ingås.

Artikel 15

Tillgänglighet för personer med funktionshinder

När det är genomförbart ska betrodda tjänster som tillhandahålls och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster göras tillgängliga för personer med funktionshinder.

Artikel 16

Sanktioner

Medlemsstaterna ska fastställa bestämmelser om de sanktioner som ska tillämpas vid överträdelser av denna förordning. Sanktionerna ska vara effektiva, proportionella och avskräckande.

AVSNITT 2

Tillsyn

Artikel 17

Tillsynsorgan

1. Medlemsstaterna ska utse ett tillsynsorgan som är etablerat inom deras territorium eller, efter ömsesidig överenskommelse med en annan medlemsstat, ett tillsynsorgan som är etablerat i den andra medlemsstaten. Det organet ska ansvara för tillsynsuppgifter i den medlemsstat som utsett organet.

Tillsynsorgan ska tilldelas nödvändiga befogenheter och adekvata resurser för utövande av sina uppgifter.

2. Medlemsstaterna ska meddela kommissionen namn på och adress till sina respektive utsedda tillsynsorgan.

3. Tillsynsorganet ska ha följande roll:

a) Utöva tillsyn över kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts för att genom tillsynsverksamhet på förhand och i efterhand se till att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning.

b) Vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts genom tillsynsverksamhet i efterhand om de tar del av påståenden att dessa icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i denna förordning.

4. Vid tillämpningen av punkt 3 och med förbehåll för de begränsningar som anges däri ska tillsynsorganets uppgifter särskilt innefatta följande:

a) Samarbete med andra tillsynsorgan och bistånd till dem i enlighet med artikel 18.

b) Analys av de rapporter om överensstämmelsebedömning som avses i artiklarna 20.1 och 21.1.

c) Information till andra tillsynsorgan samt allmänheten om säkerhetsincidenter eller integritetsförluster i enlighet med artikel 19.2.

d) Rapportering till kommissionen om sin huvudverksamhet i enlighet med punkt 6 i denna artikel.

e) Granskningsverksamhet eller framställningar till ett organ för bedömning av överensstämmelse om att detta ska göra en överensstämmelsebedömning av kvalificerade tillhandahållare av betrodda tjänster i enlighet med artikel 20.2.

f) Samarbete med dataskyddsmyndigheterna, främst genom att utan onödigt dröjsmål informera dem om resultatet av granskningar av kvalificerade tillhandahållare av betrodda tjänster, när det förefaller ha skett en överträdelse av reglerna för skydd för personuppgifter.

g) Beviljande av status som kvalificerad tillhandahållare av betrodda tjänster och till de tjänster som de tillhandahåller samt återkallande av denna status i enlighet med artiklarna 20 och 21.

h) Information till det organ som är ansvarigt för den nationella förteckning över betrodda tjänsteleverantörer som avses i artikel 22.3 om sina beslut om beviljande eller återkallande av status som kvalificerad, såvida inte det organet även är tillsynsorganet.

i) Kontroll av befintlighet och korrekt tillämpning av bestämmelser om planer för verksamhetens upphörande i sådana fall när den kvalificerade tillhandahållaren av betrodda tjänster upphör med sin verksamhet, inbegripet hur information hålls tillgänglig i enlighet med artikel 24.2 h.

j) Åläggande av krav på tillhandahållare av betrodda tjänster att åtgärda varje underlåtenhet att uppfylla kraven i denna förordning.

5. Medlemsstaterna får kräva att tillsynsorganet ska inrätta, underhålla och uppdatera en infrastruktur för betrodda tjänster i enlighet med villkoren i nationell rätt.

6. Senast den 31 mars varje år ska varje tillsynsorgan till kommissionen överlämna en rapport om det föregående kalenderårets huvudverksamhet tillsammans med en sammanfattning av överträdelseanmälningar som har inkommit från tillhandahållare av betrodda tjänster i enlighet med artikel 19.2.

7. Kommissionen ska göra den årsrapport som avses i punkt 6 tillgänglig för medlemsstaterna.

8. Kommissionen får genom genomförandeakter fastställa format och förfaranden för den rapport som avses i punkt 6. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 18

Ömsesidigt bistånd

1. Tillsynsorganen ska samarbeta med sikte på att utbyta god praxis.

Ett tillsynsorgan ska, efter att ha mottagit en motiverad begäran från ett annat tillsynsorgan, ge det organet bistånd så att deras åtgärder kan vidtas på ett enhetligt sätt. Det ömsesidiga biståndet kan bland annat omfatta begäranden om information och tillsynsåtgärder, t.ex. begäranden om att utföra inspektioner avseende de rapporter om överensstämmelsebedömning som avses i artiklarna 20 och 21.

2. Ett tillsynsorgan som tar emot en begäran om bistånd får vägra att tillmötesgå denna begäran på grundval av något av följande skäl:

a) Tillsynsorganet är inte behörigt att tillhandahålla det bistånd som begärs.

b) Det begärda biståndet står inte i proportion till den tillsynsverksamhet som tillsynsorganet utför i enlighet med artikel 17.

c) Det skulle stå i strid med denna förordning att tillhandahålla det begärda biståndet.

3. Där så är lämpligt får medlemsstaterna bemyndiga sina respektive tillsynsorgan att vidta gemensamma åtgärder där personal från andra medlemsstaters tillsynsorgan deltar. De berörda medlemsstaterna ska besluta om och inrätta arrangemangen och förfarandena för sådana gemensamma åtgärder i enlighet med sin nationella rätt.

Artikel 19

Säkerhetskrav på tillhandahållare av betrodda tjänster

1. Kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa att säkerhetsnivån står i proportion till graden av risk. I synnerhet ska åtgärder vidtas för att förhindra eller minimera säkerhetsincidenters inverkan samt för att informera berörda parter om de negativa effekterna av eventuella sådana incidenter.

2. Kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster ska, utan otillbörligt dröjsmål och under alla omständigheter inom 24 timmar efter upptäckt, underrätta tillsynsorganet och i förekommande fall andra relevanta organ, såsom det behöriga nationella organet för informationssäkerhet eller dataskyddsmyndigheten, om alla säkerhetsincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller på de personuppgifter som ingår i denna.

När det är troligt att säkerhetsincidenten eller integritetsförlusten kommer att ha negativ inverkan på en fysisk eller juridisk person till vilken den betrodda tjänsten har tillhandahållits, ska tillhandahållaren av betrodda tjänster utan onödigt dröjsmål även underrätta den fysiska eller juridiska personen om säkerhetsincidenten eller integritetsförlusten.

När så är lämpligt, särskilt om säkerhetsincidenten eller integritetsförlusten rör två eller flera medlemsstater, ska det underrättade tillsynsorganet informera tillsynsorganen i övriga berörda medlemsstater samt Enisa.

Det underrättade tillsynsorganet ska informera allmänheten eller kräva att tillhandahållaren av betrodda tjänster gör det, om den slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten ligger i allmänhetens intresse.

3. Tillsynsorganet ska en gång om året till Enisa överlämna en sammanfattning av de anmälningar om säkerhetsincidenter eller som inkommit från tillhandahållare av betrodda tjänster.

4. Kommissionen får, genom genomförandeakter,

a) ytterligare specificera de åtgärder som avses i punkt 1, och

b) fastställa format och förfaranden, inklusive tidsfrister, som ska vara tillämpliga för de ändamål som avses i punkt 2.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 3

Kvalificerade betrodda tjänster

Artikel 20

Tillsyn över kvalificerade tillhandahållare av betrodda tjänster

1. Kvalificerade tillhandahållare av betrodda tjänster ska minst en gång vartannat år och på egen bekostnad granskas av ett organ för bedömning av överensstämmelse. Syftet med denna granskning ska vara att bekräfta att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. De kvalificerade tillhandahållarna av betrodda tjänster ska lämna in den resulterande rapporten om överensstämmelsebedömning till tillsynsorganet inom en period av tre arbetsdagar efter mottagande av denna.

2. Tillsynsorganet får, utan att det påverkar tillämpningen av punkt 1, när som helst granska eller begära att ett organ för bedömning av överensstämmelse gör en överensstämmelsebedömning av de kvalificerade tillhandahållarna av betrodda tjänster på dessa tillhandahållare av betrodda tjänsters egen bekostnad för att bekräfta att dessa och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. Vid misstänkta överträdelser av reglerna om skydd för personuppgifter ska tillsynsorganet informera dataskyddsmyndigheterna om sina granskningsresultat.

3. När tillsynsorganet begär att den kvalificerade tillhandahållaren av betrodda tjänster ska åtgärda en underlåtenhet att uppfylla kraven i denna förordning och när tillhandahållaren inte gör detta, och i tillämpliga fall inom den tidsfrist som fastställts av tillsynsorganet, får tillsynsorganet med beaktande av i synnerhet underlåtenhetens omfattning, varaktighet och följder återkalla den tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad samt informera det organ som avses i artikel 22.3 för att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 ska kunna uppdateras. Tillsynsorganet ska informera den kvalificerade tillhandahållaren av betrodda tjänster om återkallandet av dess eller den berörda tjänstens status som kvalificerad.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till följande standarder:

a) Ackreditering av organ för bedömning av överensstämmelse och för den rapport om överensstämmelsebedömning som avses i punkt 1.

b) Granskningsregler som organen för bedömning av överensstämmelse ska följa vid sina överensstämmelsebedömningar av kvalificerade tillhandahållare av betrodda tjänster som avses i punkt 1.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 21

Igångsättande av en kvalificerad betrodd tjänst

1. När tillhandahållare av betrodda tjänster som inte har status som kvalificerade har för avsikt att börja tillhandahålla kvalificerade betrodda tjänster, ska de anmäla sin avsikt till tillsynsorganet och samtidigt lämna in en rapport om överensstämmelsebedömning som utfärdats av ett organ för bedömning av överensstämmelse.

2. Tillsynsorganet ska kontrollera huruvida tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller kraven i denna förordning, och i synnerhet kraven för kvalificerade tillhandahållare av betrodda tjänster och för de kvalificerade betrodda tjänster som de tillhandahåller.

Om tillsynsorganet kommer fram till att tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller de krav som avses i första stycket, ska det bevilja status som kvalificerad till tillhandahållare av betrodda tjänster och de betrodda tjänster som denne tillhandahåller samt informera det organ som avses i artikel 22.3 för att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 ska kunna uppdateras, senast tre månader efter anmälan i enlighet med punkt 1 i denna artikel.

Om kontrollen inte har slutförts inom tre månader från anmälan, ska tillsynsorganet informera tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.

3. Kvalificerade tillhandahållare av betrodda tjänster får börja tillhandahålla den kvalificerade betrodda tjänsten efter det att status som kvalificerad har angetts i de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1.

4. Kommissionen får genom genomförandeakter fastställa format och förfaranden för de ändamål som avses i punkterna 1 och 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 22

Förteckningar över betrodda tjänsteleverantörer

1. Varje medlemsstat ska upprätta, underhålla och offentliggöra förteckningar med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som den ansvarar för, tillsammans med uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller.

2. Medlemsstaterna ska på ett säkert sätt upprätta, underhålla och offentliggöra elektroniskt undertecknade eller förseglade förteckningar som avses i punkt 1 i en form som lämpar sig för automatiserad behandling.

3. Medlemsstaterna ska utan onödigt dröjsmål till kommissionen lämna information om det organ som ansvarar för att upprätta, underhålla och offentliggöra nationella förteckningar över betrodda tjänsteleverantörer, samt närmare uppgifter om var dessa förteckningar offentliggörs, de certifikat som används för att underteckna eller försegla förteckningarna över betrodda tjänsteleverantörer och eventuella ändringar i dem.

4. Kommissionen ska se till att den information som avses i punkt 3 genom en säker kanal görs tillgänglig för allmänheten i elektroniskt undertecknad eller förseglad form som lämpar sig för automatiserad behandling.

5. Senast den 18 september 2015 ska kommissionen genom genomförandeakter ange den information som avses i punkt 1 och fastställa de tekniska specifikationer och format som ska gälla för förteckningar över betrodda tjänsteleverantörer för de ändamål som avses i punkterna 1–4. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 23

EU-förtroendemärke för kvalificerade betrodda tjänster

1. Efter det att den kvalificerade status som avses i artikel 21.2 andra stycket har angetts i den förteckning över betrodda tjänsteleverantörer som avses i artikel 22.1, får kvalificerade tillhandahållare av betrodda tjänster använda sig av EU-förtroendemärket för att på ett enkelt, igenkännligt och tydligt sätt ange de kvalificerade betrodda tjänster som de tillhandahåller.

2. Vid användning av det EU-förtroendemärke som avses i punkt 1 ska kvalificerade tillhandahållare av betrodda tjänster se till att en länk till den relevanta förteckningen över betrodda tjänsteleverantörer finns på deras webbplats.

3. Senast den 1 juli 2015 ska kommissionen genom genomförandeakter fastställa specifikationer med avseende på formatet för EU-förtroendemärket för kvalificerade betrodda tjänster och särskilt för dess presentation, sammansättning, storlek och utformning. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 24

Krav på kvalificerade tillhandahållare av betrodda tjänster

1. En kvalificerad tillhandahållare av betrodda tjänster ska, när den utfärdar ett kvalificerat certifikat för en betrodd tjänst, på lämpligt sätt och i enlighet med nationell rätt kontrollera identiteten och i förekommande fall eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet utfärdas.

Den information som avses i första stycket ska kontrolleras av den kvalificerade tillhandahållaren av betrodda tjänster antingen direkt eller via tredje man i enlighet med nationell rätt på något av följande sätt:

a) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen.

b) På distans, med hjälp av medel för elektronisk identifiering, där en fysisk närvaro av den fysiska personen eller en behörig företrädare för den juridiska personen vid tidpunkt före utfärdandet av det kvalificerade certifikatet säkerställs och som uppfyller kraven i artikel 8 när det gäller tillitsnivåerna väsentlig eller hög.

c) Genom ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel som utfärdats i enlighet med led a eller b.

d) Med hjälp av andra identifieringsmetoder som erkänns på nationell nivå och som erbjuder garantier som är likvärdiga med fysisk närvaro. Likvärdiga garantier ska bekräftas av ett organ för bedömning av överensstämmelse.

2. En kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade betrodda tjänster ska

a) informera tillsynsorganet om alla ändringar av tillhandahållandet av dess kvalificerade betrodda tjänster, och om den har för avsikt att upphöra med denna verksamhet,

b) ha personal, och i förekommande fall underleverantörer, som har den sakkunskap, den tillförlitlighet samt de erfarenheter och kvalifikationer som behövs och som har genomgått lämplig utbildning om regler för säkerhet och skydd för personuppgifter och ska tillämpa förfaranden för administration och förvaltning som överensstämmer med europeiska eller internationella standarder,

c) när det gäller risken för ansvar vid skador i enlighet med artikel 13 förfoga över tillräckliga ekonomiska medel och/eller skaffa sig lämplig ansvarsförsäkring i enlighet med nationell rätt,

d) innan den ingår ett avtalsförhållande på ett tydligt och uttömmande sätt informera de personer som vill använda en kvalificerad betrodd tjänst om de exakta villkor som gäller för användning av den tjänsten, inbegripet om eventuella begränsningar av användningen,

e) använda tillförlitliga system och produkter som är skyddade mot ändringar och säkerställa den tekniska säkerheten och tillförlitligheten hos den process som stöds av dessa,

f) använda tillförlitliga system för att lagra uppgifter som har lämnats till den, i en form som kan kontrolleras så att

i) de är offentligt tillgängliga för hämtning endast i de fall där samtycke från den person som uppgifterna rör har erhållits,

ii) endast behöriga personer kan föra in uppgifter och göra ändringar i de lagrade uppgifterna, och

iii) uppgifternas äkthet kan kontrolleras,

g) vidta lämpliga åtgärder mot förfalskning och stöld av uppgifter,

h) under en lämplig tidsperiod registrera och hålla tillgänglig, även efter det att den kvalificerade tillhandahållaren av betrodda uppgifter har upphört med sin verksamhet, all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster har utfärdat och tagit emot, särskilt för att vid rättsliga förfaranden kunna lägga fram bevis och för att säkerställa tjänstens kontinuitet; registreringen får göras elektroniskt,

i) ha en uppdaterad plan för verksamhetens upphörande i syfte att säkerställa tjänstens kontinuitet i enlighet med bestämmelser som kontrollerats av tillsynsorganet i enlighet med artikel 17.4 i,

j) säkerställa laglig behandling av personuppgifter i enlighet med direktiv 95/46/EG,

k) då det är fråga om kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat, upprätta och uppdatera en certifikatdatabas,

3. Om en kvalificerad tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat beslutar att återkalla ett certifikat, ska den registrera ett sådant återkallande i sin certifikatdatabas och offentliggöra återkallandet av statusen för certifikatet i god tid och i alla händelser inom 24 timmar efter mottagandet av begäran. Återkallandet ska få verkan omedelbart efter offentliggörandet.

4. Med avseende på punkt 3 ska kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat informera eventuella förlitande parter om giltigheten eller statusen som återkallad hos de kvalificerade certifikat som de utfärdat. Informationen ska, åtminstone på certifikatnivå, när som helst och utöver certifikatets giltighetsperiod göras tillgängligt på ett automatiskt sätt som är tillförlitligt, kostnadsfritt och effektivt.

5. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för tillförlitliga system och produkter, vilka uppfyller kraven i punkt 2 e och f i denna artikel. Överensstämmelse med kraven i denna artikel ska förutsättas när tillförlitliga system och produkter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 4

Elektroniska underskrifter

Artikel 25

Rättslig verkan av elektroniska underskrifter

1. En elektronisk underskrift får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att underskriften har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska underskrifter.

2. En kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift.

3. En kvalificerad elektronisk underskrift som är baserad på ett kvalificerat certifikat som utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk underskrift i alla andra medlemsstater.

Artikel 26

Krav med avseende på avancerade elektroniska underskrifter

En avancerad elektronisk underskrift ska uppfylla följande krav:

a) Den ska vara unikt knuten till undertecknaren.

b) Undertecknaren ska kunna identifieras genom den.

c) Den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll.

d) Den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Artikel 27

Elektroniska underskrifter i offentliga tjänster

1. Om en medlemsstat kräver en avancerad elektronisk underskrift för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska medlemsstaten erkänna avancerade elektroniska underskrifter, avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat för elektroniska underskrifter och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i de genomförandeakter som avses i punkt 5.

2. Om en medlemsstat kräver en avancerad elektronisk underskrift som är baserad på ett kvalificerat certifikat för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska medlemsstaten erkänna avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i de genomförandeakter som avses i punkt 5.

3. Medlemsstaterna ska för gränsöverskridande användning av nättjänster som erbjuds av ett offentligt organ inte kräva en elektronisk underskrift med en högre säkerhetsnivå än den som gäller för kvalificerade elektroniska underskrifter.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för avancerade elektroniska underskrifter. Överensstämmelse med de krav på avancerade elektroniska underskrifter som avses i punkterna 1 och 2 i denna artikel samt i artikel 26 ska förutsättas när en avancerad elektronisk underskrift uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

5. Kommissionen ska senast den 18 september 2015 och med beaktande av befintliga rutiner, standarder och unionsrättsakter, genom genomförandeakter, fastställa referensformat för avancerade elektroniska underskrifter eller referensmetoder i de fall alternativa format används. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 28

Kvalificerade certifikat för elektroniska underskrifter

1. Kvalificerade certifikat för elektroniska underskrifter ska uppfylla kraven i bilaga I.

2. Kvalificerade certifikat för elektroniska underskrifter ska inte omfattas av några obligatoriska krav som går utöver kraven i bilaga I.

3. Kvalificerade certifikat för elektroniska underskrifter får omfatta extra, icke-obligatoriska, särskilda attribut. Dessa attribut ska inte påverka kvalificerade elektroniska underskrifters kompatibilitet eller erkännande.

4. Om ett kvalificerat certifikat för elektroniska underskrifter har återkallats efter den ursprungliga aktiveringen, ska det förlora sin giltighet från och med tidpunkten för återkallandet, och dess status som giltigt ska inte under några omständigheter återgå.

5. På följande villkor får medlemsstaterna fastställa nationella bestämmelser för tillfälligt upphävande av ett kvalificerat certifikat för elektroniska underskrifter:

a) Om ett kvalificerat certifikat för en elektronisk underskrift tillfälligt har upphävts, ska certifikatet vara ogiltigt under tiden för det tillfälliga upphävandet.

b) Perioden för det tillfälliga upphävandet ska tydligt anges i certifikatdatabasen och certifikatets status som tillfälligt upphävt ska under perioden för det tillfälliga upphävandet vara synlig genom den tjänst som tillhandahåller information om certifikatets status.

6. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska underskrifter. Överensstämmelse med kraven i bilaga I ska förutsättas när ett kvalificerat certifikat för elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 29

Krav på anordningar för skapande av kvalificerade elektroniska underskrifter

1. Anordningar för skapande av kvalificerade elektroniska underskrifter ska uppfylla kraven i bilaga II.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för anordningar för skapande av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i bilaga II ska förutsättas när en anordning för skapande av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 30

Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter

1. Lämpliga offentliga eller privata organ som utsetts av medlemsstaterna ska certifiera att anordningar för skapande av kvalificerade elektroniska underskrifter överensstämmer med kraven i bilaga II.

2. Medlemsstaterna ska underrätta kommissionen om namnet på och adressen till det offentliga eller privata organ som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för medlemsstaterna.

3. Den certifiering som avses i punkt 1 ska bygga på något av följande:

a) Ett förfarande för säkerhetsutvärdering som utförts i enlighet med någon av de standarder för säkerhetsutvärdering av informationsteknikprodukter som finns med i den förteckning som fastställts i enlighet med andra stycket.

b) Ett annat förfarande än det som avses i led a, förutsatt att det omfattar jämförbara säkerhetsnivåer och att det offentliga eller privata organ som avses i punkt 1 underrättar kommissionen om förfarandet. Detta förfarande får endast användas vid avsaknad av sådana standarder som avses i led a eller medan en sådan säkerhetsutvärdering som avses i led a pågår.

Kommissionen ska genom genomförandeakter upprätta en förteckning över standarder för den säkerhetsbedömning av informationsteknikprodukter som avses i led a. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

4. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 47 rörande fastställandet av särskilda kriterier som ska uppfyllas av de utsedda organ som avses i punkt 1 i den här artikeln.

Artikel 31

Offentliggörande av en förteckning över certifierade anordningar för skapande av kvalificerade elektroniska underskrifter

1. Medlemsstaterna ska utan onödigt dröjsmål och senast en månad efter det att certifieringen slutförts till kommissionen lämna information om anordningar för skapande av kvalificerade elektroniska underskrifter som har certifierats av de organ som avses i artikel 30.1. De ska utan onödigt dröjsmål och senast en månad efter det att en certifiering har upphört att gälla även informera kommissionen om anordningar för skapande av elektroniska underskrifter som inte längre är certifierade.

2. Kommissionen ska på grundval av den information som inkommit upprätta, offentliggöra och underhålla en förteckning över certifierade anordningar för skapande av kvalificerade elektroniska underskrifter.

3. Kommissionen får genom genomförandeakter fastställa format och förfaranden som ska vara tillämpliga för de ändamål som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 32

Krav på validering av kvalificerade elektroniska underskrifter

1. Genom valideringsförfarandet för en kvalificerad elektronisk underskrift ska den kvalificerade elektroniska underskriftens giltighet bekräftas under förutsättning att

a) det certifikat som stöder underskriften vid tidpunkten för undertecknandet var ett kvalificerat certifikat för elektroniska underskrifter som överensstämmer med bilaga I,

b) det kvalificerade certifikatet har utfärdats av en kvalificerad tillhandahållare av betrodda tjänster och var giltigt vid tidpunkten för undertecknandet,

c) valideringsuppgifterna för underskriften överensstämmer med de uppgifter som lämnats till den förlitande parten,

d) certifikatets unika uppsättning uppgifter som avser undertecknaren har tillhandahållits den förlitande parten på rätt sätt,

e) användningen av en eventuell pseudonym tydligt har angetts för den förlitande parten om en pseudonym användes vid tidpunkten för undertecknandet,

f) den elektroniska underskriften har skapats med hjälp av en anordning för skapande av kvalificerade elektroniska underskrifter,

g) integriteten hos de undertecknade uppgifterna inte har äventyrats,

h) kraven i artikel 26 var uppfyllda vid tidpunkten för undertecknandet.

2. Det system som används för att validera den kvalificerade elektroniska underskriften ska ge den förlitande parten det korrekta resultatet av valideringsförfarandet och ska göra det möjligt för den förlitande parten att upptäcka eventuella problem som är relevanta för säkerheten.

3. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för validering av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när valideringen av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 33

Kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter

1. En kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter får endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som

a) tillhandahåller validering i enlighet med artikel 32.1, och

b) gör det möjligt för förlitande parter att erhålla resultaten av valideringsförfarandet på ett automatiskt sätt som är tillförlitligt, effektivt och försett med en avancerad elektronisk underskrift eller en avancerad elektronisk stämpel från tillhandahållaren av den kvalificerade valideringstjänsten.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för den kvalificerade valideringstjänst som avses i punkt 1. Överensstämmelse med kraven i punkt 1 ska förutsättas när valideringstjänsten för kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 34

Kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter

1. En kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter får endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som använder förfaranden och tekniker som gör det möjligt att förlänga den kvalificerade elektroniska underskriftens tillförlitlighet utöver perioden för teknisk giltighet.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när systemen för de kvalificerade tjänsterna för bevarande av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 5

Elektroniska stämplar

Artikel 35

Rättslig verkan av elektroniska stämplar

1. En elektronisk stämpel får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form eller att det inte uppfyller kraven för kvalificerade elektroniska stämplar.

2. En kvalificerad elektronisk stämpel ska omfattas av en presumtion om integritet hos de uppgifter som den kvalificerade elektroniska stämpeln är kopplad till och om att de har korrekt ursprung.

3. En kvalificerad elektronisk stämpel som är baserat på ett kvalificerat certifikat som har utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk stämpel i alla andra medlemsstater.

Artikel 36

Krav med avseende på avancerade elektroniska stämplar

En elektronisk stämpel ska uppfylla följande krav:

a) Den ska vara knuten uteslutande till skaparen av stämpeln.

b) Skaparen av stämpeln ska kunna identifieras genom det.

c) Det ska vara skapat på grundval av uppgifter för skapande av elektroniska stämplar som stämpelns skapare med hög grad av tillförlitlighet under sin kontroll kan använda för skapande av elektroniska stämplar.

d) Den ska vara kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Artikel 37

Elektroniska stämplar i offentliga tjänster

1. Om en medlemsstat kräver en avancerad elektronisk stämpel för användningen av en nättjänst som erbjuds av ett offentligt organ eller för organets räkning ska medlemsstaten erkänna avancerade elektroniska stämplar, avancerade elektroniska stämplar som är baserade på ett kvalificerat certifikat för elektroniska stämplar och kvalificerade elektroniska stämplar i åtminstone de format eller med användning av de metoder som anges i de genomförandeakter som avses i punkt 5.

2. Om en medlemsstat kräver en avancerad elektronisk stämpel som är baserad på ett kvalificerat certifikat för användningen av en nättjänst som erbjuds av ett offentligt organ eller för organets räkning, ska medlemsstaten erkänna avancerade elektroniska stämplar som är baserade på ett kvalificerat certifikat och kvalificerade elektroniska stämplar i åtminstone de format eller med användning av de metoder som anges i de genomförandeakter som avses i punkt 5.

3. Medlemsstaterna ska för gränsöverskridande användning av en nättjänst som erbjuds av ett offentligt organ inte kräva en elektronisk stämpel på en högre säkerhetsnivå än den som gäller för den kvalificerade elektroniska stämpeln.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för avancerade elektroniska stämplar. Överensstämmelse med de krav på avancerade elektroniska stämplar som avses i punkterna 1 och 2 i denna artikel samt i artikel 36 ska förutsättas när en avancerad elektronisk stämpel uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

5. Kommissionen ska senast den 18 september 2015, och med beaktande av befintliga rutiner, standarder och unionsrättsakter genom genomförandeakter fastställa referensformat för avancerade elektroniska stämplar eller referensmetoder i de fall alternativa format används. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 38

Kvalificerade certifikat för elektroniska stämplar

1. Kvalificerade certifikat för elektroniska stämplar ska uppfylla kraven i bilaga III.

2. Kvalificerade certifikat för elektroniska stämplar ska inte omfattas av några obligatoriska krav som går utöver kraven i bilaga III.

3. Kvalificerade certifikat för elektroniska stämplar får omfatta extra, icke-obligatoriska, särskilda attribut. Dessa attribut ska inte påverka kvalificerade elektroniska stämplars interoperabilitet eller erkännande.

4. Om ett kvalificerat certifikat för en elektronisk stämpel har återkallats efter den ursprungliga aktiveringen ska det förlora sin giltighet från och med tidpunkten för återkallandet och dess status ska inte under några omständigheter återgå.

5. På följande villkor får medlemsstaterna fastställa nationella bestämmelser för tillfälligt upphävande av kvalificerade certifikat för elektroniska stämplar:

a) Om ett kvalificerat certifikat för elektroniska stämplar tillfälligt har upphävts ska certifikatet vara ogiltigt under perioden för det tillfälliga upphävandet.

b) Perioden för det tillfälliga upphävandet ska tydligt anges i certifikatdatabasen och certifikatets status som tillfälligt upphävt ska under perioden för det tillfälliga upphävandet vara synlig genom den tjänst som tillhandahåller information om certifikatets status.

6. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska stämplar. Överensstämmelse med kraven i bilaga III ska förutsättas när ett kvalificerat certifikat för elektroniska stämplar uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 39

Kvalificerade anordningar för skapande av elektroniska stämplar

1. Artikel 29 ska på motsvarande sätt gälla för kraven på kvalificerade anordningar för skapande av elektroniska stämplar.

2. Artikel 30 ska på motsvarande sätt gälla för certifieringen av kvalificerade anordningar för skapande av elektroniska stämplar.

3. Artikel 31 ska på motsvarande sätt gälla för offentliggörandet av en förteckning över certifierade kvalificerade anordningar för skapande av elektroniska stämplar.

Artikel 40

Validering och bevarande av kvalificerade elektroniska stämplar

Artiklarna 32, 33 och 34 ska på motsvarande sätt gälla för validering och bevarande av kvalificerade elektroniska stämplar.

AVSNITT 6

Elektroniska tidsstämplingar

Artikel 41

Rättslig verkan av elektroniska tidsstämplingar

1. En elektronisk tidsstämpling ska inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att den har elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk tidsstämpling.

2. En kvalificerad elektronisk tidsstämpling ska omfattas av en presumtion om korrekthet hos det datum och den tid som den anger och integritet hos de uppgifter som datumet och tiden är kopplade till.

3. En kvalificerad elektronisk tidsstämpling som utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk tidsstämpling i alla medlemsstater.

Artikel 42

Krav på kvalificerade elektroniska tidsstämplingar

1. En kvalificerad elektronisk tidsstämpling ska uppfylla följande krav:

a) Den ska binda datumet och tiden till uppgifter så att möjligheten att uppgifterna ändras utan att det går att upptäcka rimligtvis kan uteslutas.

b) Den ska vara grundad på en korrekt tidskälla som är kopplad till samordnad universaltid.

c) Den ska vara undertecknad med hjälp av en avancerad elektronisk underskrift eller förseglad med en avancerad elektronisk stämpel från den kvalificerade tillhandahållaren av betrodda tjänster eller genom en likvärdig metod.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för bindning av datum och tidpunkt till uppgifter och för korrekta tidskällor. Överensstämmelse med kraven i punkt 1 ska förutsättas när bindningen av datum och tidpunkt till uppgifter och den korrekta tidskällan uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 7

Elektroniska tjänster för rekommenderade leveranser

Artikel 43

Rättslig verkan av elektroniska tjänster för rekommenderade leveranser

1. Uppgifter som sänds och tas emot genom en elektronisk tjänst för rekommenderade leveranser får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller inte uppfyller kraven på den kvalificerade elektroniska tjänsten för rekommenderade leveranser.

2. Uppgifter som sänds och tas emot genom en kvalificerad elektronisk tjänst för rekommenderade leveranser ska omfattas av en presumtion om uppgifternas integritet, om uppgifternas avsändande av den identifierade avsändaren, uppgifternas mottagande av den identifierade adressaten samt om riktigheten i det datum och den tidpunkt för avsändande och mottagande som anges i den kvalificerade elektroniska tjänsten för rekommenderade leveranser.

Artikel 44

Krav på kvalificerade elektroniska tjänster för rekommenderade leveranser

1. Kvalificerade elektroniska tjänster för rekommenderade leveranser ska uppfylla följande krav:

a) De ska tillhandahållas av en eller flera kvalificerade tillhandahållare av betrodda tjänster.

b) De ska med hög grad av tillförlitlighet säkerställa avsändarens identitet.

c) De ska säkerställa adressatens identitet innan uppgifterna levereras.

d) Avsändandet och mottagandet av uppgifter ska säkerställas genom en avancerad elektronisk underskrift eller en avancerad elektronisk stämpel från en kvalificerad tillhandahållare av betrodda tjänster på ett sätt som utesluter möjligheten att uppgifterna ändras utan att det går att upptäcka.

e) Eventuella ändringar av de uppgifter som behövs för att sända eller ta emot uppgifterna ska tydligt anges för uppgifternas avsändare och adressat.

f) Datumet och tidpunkten för avsändande, mottagande och eventuella ändringar av uppgifter måste anges genom en kvalificerad elektronisk tidsstämpling.

Om uppgifterna överförs mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster ska kraven i leden a–f gälla för alla kvalificerade tillhandahållare av betrodda tjänster.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för processer för att sända och ta emot uppgifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när en process för att sända och ta emot uppgifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 8

Autentisering av webbplatser

Artikel 45

Krav på kvalificerade certifikat för autentisering av webbplatser

1. Kvalificerade certifikat för autentisering av webbplatser ska uppfylla kraven i bilaga IV.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för autentisering av webbplatser. Överensstämmelse med kraven i bilaga IV ska förutsättas när ett kvalificerat certifikat för autentisering av webbplatser uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

KAPITEL IV

ELEKTRONISKA DOKUMENT

Artikel 46

Rättslig verkan av elektroniska dokument

Ett elektroniskt dokument får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form.

KAPITEL V

DELEGERING AV BEFOGENHETER OCH GENOMFÖRANDEBESTÄMMELSER

Artikel 47

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 30.4 ska ges till kommissionen tills vidare från och med den 17 september 2014.

3. Den delegering av befogenhet som avses i artikel 30.4 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

5. En delegerad akt som antas enligt artikel 30.4 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 48

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL VI

SLUTBESTÄMMELSER

Artikel 49

Översyn

Kommissionen ska göra en översyn över denna förordnings tillämpning och rapportera resultaten till Europaparlamentet och rådet senast den 1 juli 2020. Kommissionen ska särskilt utvärdera huruvida det är lämpligt att ändra denna förordnings tillämpningsområde eller dess särskilda bestämmelser, som artiklarna 6, 7 f, 34, 43, 44 eller 45, med beaktande av den erfarenhet som erhållits vid tillämpningen av denna förordning samt den tekniska och rättsliga utvecklingen och marknadsutvecklingen.

Den rapport som avses i första stycket ska vid behov åtföljas av lagstiftningsförslag.

Dessutom ska kommissionen vart fjärde år efter den rapport som avses i första stycket lämna en rapport till Europaparlamentet och rådet om framstegen med att uppfylla målen för denna förordning.

Artikel 50

Upphävande

1. Direktiv 1999/93/EG ska upphöra att gälla med verkan från och med den 1 juli 2016.

2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till den här förordningen.

Artikel 51

Övergångsbestämmelser

1. Säkra anordningar för skapande av underskrifter vilkas överensstämmelse har fastställts i enlighet med artikel 3.4 i direktiv 1999/93/EG ska anses som kvalificerade anordningar för skapande av elektroniska underskrifter enligt denna förordning.

2. Kvalificerade certifikat som utfärdats till fysiska personer enligt direktiv 1999/93/EG ska anses som kvalificerade certifikat för elektroniska underskrifter enligt denna förordning till dess att de löper ut.

3. Tillhandahållare av en certifieringstjänst som utfärdar certifikat enligt direktiv 1999/93/EG ska lämna in en rapport om bedömning av överensstämmelse till tillsynsorganet så snart som möjligt och senast den 1 juli 2017. Fram till dess att denna rapport har inlämnats och tillsynsorganet har slutfört sin bedömning av den ska tillhandahållaren av certifieringstjänsten anses vara en kvalificerad tillhandahållare av betrodda tjänster enligt denna förordning.

4. Om en tillhandahållare av certifieringstjänster som utfärdar kvalificerade certifikat enligt direktiv 1999/93/EG inte lämnar in någon rapport om bedömning av överensstämmelse till tillsynsorganet inom den tidsfrist som avses i punkt 3 ska denna tillhandahållare av certifieringstjänster inte anses vara en kvalificerad tillhandahållare av betrodda tjänster enligt denna förordning från och med den 2 juli 2017.

Artikel 52

Ikraftträdande

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Den ska tillämpas från och med den 1 juli 2016, med undantag för följande:

a) Artiklarna 8.3, 9.5, 12.2–12.9, 17.8, 19.4, 20.4, 21.4, 22.5, 23.3, 24.5, 27.4, 27.5, 28.6, 29.2, 30.3, 30.4, 31.3, 32.3, 33.2, 34.2, 37.4, 37.5, 38.6, 42.2, 44.2, 45.2, 47 och 48 ska tillämpas från och med den 17 september 2014.

b) Artiklarna 7, 8.1, 8.2, 9, 10, 11 och 12.1 ska tillämpas från och med tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8.

c) Artikel 6 ska tillämpas från och med tre år efter tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8.

3. Om det anmälda systemet för elektronisk identifiering före det datum som avses i punkt 2 c i denna artikel finns upptaget i den förteckning som kommissionen offentliggjort enligt artikel 9, ska medlet för elektronisk identifiering inom ramen för detta system enligt artikel 6 erkännas senast 12 månader efter systemets offentliggörande, dock inte före det datum som avses i punkt 2 c i denna artikel.

4. Trots vad som sägs i punkt 2 c i denna artikel får en medlemsstat besluta att ett medel för elektronisk identifiering inom ramen för ett system för elektronisk identifiering som har anmälts i enlighet med artikel 9.1 av en annan medlemsstat ska erkännas i den första medlemsstaten från och med tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8. De berörda medlemsstaterna ska underrätta kommissionen. Kommissionen ska offentliggöra denna information.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel 23 juli 2014.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	S. GOZI
Ordförande	*Ordförande*

BILAGA I

KRAV PÅ KVALIFICERADE CERTIFIKAT FÖR ELEKTRONISKA UNDERSKRIFTER

Kvalificerade certifikat för elektroniska underskrifter ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska underskrifter.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar,

— för fysiska personer: personens namn.

c) Åtminstone undertecknarens namn eller en pseudonym. Om en pseudonym används ska detta tydligt anges.

d) Valideringsuppgifter för elektroniska underskrifter som stämmer överens med uppgifterna för skapande av elektroniska underskrifter.

e) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

f) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

g) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

h) Uppgift om var det certifikat som stöder den avancerade elektroniska underskrift eller den avancerade elektroniska stämpeln som avses i led g finns tillgängligt kostnadsfritt.

i) Uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.

j) Om de uppgifter för skapande av elektroniska underskrifter som avser valideringsuppgifterna för elektroniska underskrifter är placerade i en kvalificerad anordning för skapande av elektroniska underskrifter, en lämplig uppgift som anger detta, åtminstone i en form som lämpar sig för automatiserad behandling.

BILAGA II

KRAV PÅ KVALIFICERADE ANORDNINGAR FÖR SKAPANDE AV ELEKTRONISKA UNDERSKRIFTER

1. Kvalificerade anordningar för skapande av elektroniska underskrifter ska genom lämpliga tekniker och förfaranden säkerställa att åtminstone

   a) konfidentialiteten för de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter är säkerställd på rimligt sätt,

   b) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter i praktiken endast kan förekomma en gång,

   c) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter med rimlig säkerhet inte kan härledas och att den elektroniska underskriften på ett tillförlitligt sätt är skyddad mot förfalskning med den teknik som för närvarande finns tillgänglig,

   d) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter kan skyddas på ett tillförlitligt sätt av den legitime undertecknaren så att andra inte kan använda dem.

2. Kvalificerade anordningar för skapande av elektroniska underskrifter får inte förändra de uppgifter som ska undertecknas eller hindra att dessa uppgifter läggs fram för undertecknaren före undertecknandet.

3. Generering eller hantering av uppgifter för skapande av elektroniska underskrifter för undertecknarens räkning får endast utföras av en kvalificerad tillhandahållare av betrodda tjänster.

4. Kvalificerade tillhandahållare av betrodda tjänster som för undertecknarens räkning hanterar uppgifter för skapande av elektroniska underskrifter får, utan att det påverkar tillämpningen av punkt 1 d, endast kopiera dessa uppgifter för framställning av säkerhetskopior om följande krav är uppfyllda:

   a) Tillitsnivån för de kopierade uppsättningarna av uppgifter måste vara densamma som för de ursprungliga uppsättningarna av uppgifter.

   b) Antalet kopierade uppsättningar av uppgifter får inte överskrida det minsta antal som krävs för att säkerställa tjänstens kontinuitet.

28.8.2014 SV Europeiska unionens officiella tidning L 257/113

BILAGA III

KRAV PÅ KVALIFICERADE CERTIFIKAT FÖR ELEKTRONISKA STÄMPLAR

Kvalificerade certifikat för elektroniska stämplar ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska stämplar.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna,

— för fysiska personer: personens namn.

c) Åtminstone namnet på skaparen av stämpeln och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar.

d) Valideringsuppgifter för elektroniska stämplar som stämmer överens med uppgifterna för skapande av elektroniska stämplar.

e) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

f) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

g) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

h) Uppgift om var det certifikat som stöder den avancerade elektroniska underskrift eller den avancerade elektroniska stämpeln som avses i led g är tillgängligt kostnadsfritt.

i) Uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.

j) Om de uppgifter för skapande av elektroniska stämplar som har koppling till uppgifterna för validering av elektroniska stämplar är placerade i en kvalificerad anordning för skapande av elektroniska stämplar, en lämplig uppgift om detta, åtminstone i en form som lämpar sig för automatiserad behandling.

BILAGA IV

KRAV PÅ KVALIFICERADE CERTIFIKAT FÖR AUTENTISERING AV WEBBPLATSER

Kvalificerade certifikat för autentisering av webbplatser ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för autentisering av webbplatser.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar,

— för fysiska personer: personens namn.

c) För fysiska personer: åtminstone namnet på den person som certifikatet utfärdats för eller en pseudonym. Om en pseudonym används ska detta tydligt anges.

För juridiska personer: åtminstone namnet på den juridiska person som certifikatet utfärdats för och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar.

d) Adressuppgifter, inbegripet åtminstone stad och stat, för den fysiska eller juridiska person som certifikatet utfärdats för och, i förekommande fall, i enlighet med vad som uppgetts i officiella handlingar.

e) Det eller de domännamn som drivs av den fysiska eller juridiska person som certifikatet utfärdats för.

f) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

g) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

h) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

i) Uppgift om var det certifikat som stöder den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln som avses i led h finns tillgängligt kostnadsfritt.

j) Uppgift om var de tjänster är lokaliserade som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet.

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare. Fi.
4. För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. M.
9. Det handlar om oss. – unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed och hantera oredlighet i forskning. U.
11. Vägskatt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt. Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med privat kapital? Fi.
14. Migrationsärenden vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt handläggning. S.
26. Delningsekonomi. På användarnas villkor. Fi.
27. Vissa frågor inom fastighets- och stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. A.
29. Brottsdatalag. Ju.
30. En omreglerad spelmarknad. Del 1 och 2. Fi.
31. Stärkt konsumentskydd på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi för kunskap och likvärdighet. U.
36. Informationssäkerhet för samhällsviktiga och digitala tjänster. Ju.
37. Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra. Ju.

38. Kvalitet i välfärden – bättre upphandling och uppföljning. Fi.
39. Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. Ju.
40. För dig och för alla. S.
41. Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. Ju.
42. Vem har ansvaret? M.
43. På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. S.
44. Entreprenad, fjärrundervisning och distansundervisning. U.
45. Ny lag om företagshemligheter. Ju.
46. Stärkt ordning och säkerhet i domstol. Ju.
47. Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. S.
48. Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. S.
49. EU:s dataskyddsförordning och utbildningsområdet. U.
50. Personuppgiftsbehandling för forskningsändamål. U.
51. Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. U.
52. Så stärker vi den personliga integriteten. Ju.
53. God och nära vård. En gemensam färdplan och målbild. S.
54. Fler nyanlända elever ska uppnå behörighet till gymnasiet. U.
55. En ny kamerabevakningslag. Ju.
56. Jakten på den perfekta ersättningsmodellen. Vad händer med medarbetarnas handlingsutrymme? Fi.
57. Lag om flygpassageraruppgifter i brottsbekämpningen. Ju.
58. Amerikansk inresekontroll vid utresa från Sverige – så kan avtalen genomföras. Ju.
59. Reglering av alkoglass m.fl. produkter. S.
60. Nästa steg? Förslag för en stärkt minoritetspolitik. Ku.
61. Villkorlig frigivning – förstärkta åtgärder mot återfall i brott. Ju.
62. Kärnavfallsrådets yttrande över SKB:s Fud-program 2016. M.
63. Miljötillsyn och sanktioner – en tillsyn präglad av ansvar, respekt och enkelhet. M.
64. Detaljplanekravet. N.
65. Hyran vid nyproduktion – en utvärdering och utveckling av modellen med presumtionshyra. Ju.
66. Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning. S.
67. Våldsbejakande extremism. En forskarantologi. Ku.
68. Barnets rättigheter i ett straffrättsligt förfarande m.m. Genomförande av EU:s barnrättsdirektiv och två andra straffprocessuella frågor. Ju.
69. Marknadskontrollmyndigheter – befogenheter och sanktionsmöjligheter. UD.
70. Förstärkt skydd för uppgifter av betydelse för ett internationellt samarbete för fred och säkerhet som Sverige deltar i. Ju.
71. Bostäder på statens mark – en möjlighet? N.
72. Genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism. Ju.
73. En gemensam bild av bostadsbyggnadsbehovet. N.
74. Brottsdatalag – kompletterande lagstiftning. Ju.
75. Datalagring – brottsbekämpning och integritet. Ju.
76. Enhetliga priser på receptbelagda läkemedel. S.
77. En generell rätt till kommunal avtalssamverkan. Fi.
78. En sammanhållen budgetprocess. Fi.
79. Finansiering av public service – för ökad stabilitet, legitimitet och stärkt oberoende. Ku.

80. Stärkt integritet i Rättsmedicinalverkets verksamhet. Ju.
81. Rättslig översyn av skogsvårdslagstiftningen. N.
82. Vägledning för framtidens arbetsmarknad. A.
83. Brännheta skatter! Bör avfallsförbränning och utsläpp av kväveoxider från energiproduktion beskattas? Fi.
84. Uppehållstillstånd på grund av praktiska verkställighetshinder och preskription. Ju.
85. Rekrytering av framtidens domare. Ju.
86. Hyresmarknad utan svarthandel och otillåten andrahandsuthyrning. Ju.
87. Finansiering, subvention och prissättning av läkemedel – en balansakt. S.
88. Nästa steg? Del 2. Förslag för en stärkt minoritetspolitik. Ku
89. Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet. Ju.
90. Makars, registrerade partners och sambors förmögenhetsförhållanden i internationella situationer. Ju.
91. Nationella minoritetsspråk i skolan – förbättrade förutsättningar till undervisning och revitalisering. U.
92. Transpersoner i Sverige. Förslag för stärkt ställning och bättre levnadsvillkor. Ku.
93. Klarlagd identitet. Om utlänningars rätt att vistas i Sverige, inre utlänningskontroller och missbruk av identitetshandlingar. Ju.
94. Beräkning av skattetillägg – en översyn av reglerna. Fi.
95. Ett land att besöka. En samlad politik för hållbar turism och växande besöksnäring. N.
96. Utvidgat hinder mot erkännande av utländska barnäktenskap. Ju.
97. Totalförsvarsdatalag – Rekryteringsmyndighetens personuppgiftsbehandling. Fö.
98. Tidiga förhör – nya bevisregler i brottmål. Ju.
99. Effektivare energianvändning. N.
100. Beslag och husrannsakan – ett regelverk för dagens behov. Ju.
101. Jämställt föräldraskap och goda uppväxtvillkor för barn – en ny modell för föräldraförsäkringen. S.
102. Skatt på kadmium i vissa produkter och kemiska växtskyddsmedel. Fi.
103. Lagliga vägar för att söka asyl i EU. Ju.
104. Etikprövning – en översyn av reglerna om forskning och hälso- och sjukvård. U.
105. Kapacitetstilldelningen på höghastighetsjärnvägen. N.
106. Nystart för byggstandardiseringen genom stärkt samverkan. N.
107. Slutrapport från Sverigeförhandlingen. Infrastruktur och bostäder – ett gemensamt samhällsbygge. N.
108. Lån och garantier för fler bostäder. N.
109. Servicekontor i ny regim. Fi.
110. Värna demokratin mot våldsbejakande extremism. Hinder och möjligheter. Ku.
111. För barnets bästa? Utredningen om tvångsåtgärder mot barn i psykiatrisk tvångsvård. S.
112. Ett fönster av möjligheter. – stärkt barnrättsperspektiv för barn i skyddat boende. S.
113. Alkoholreklam i sociala medier m.m. S.
114. reboot – omstart för den digitala förvaltningen. Fi

Statens offentliga utredningar 2017

Systematisk förteckning

Villkorlig frigivning – förstärkta åtgärder mot återfall i brott. [61]

Hyran vid nyproduktion – en utvärdering och utveckling av modellen med presumtionshyra. [65]

Barnets rättigheter i ett straffrättsligt förfarande m.m. Genomförande av EU:s barnrättsdirektiv och två andra straffprocessuella frågor. [68]

Förstärkt skydd för uppgifter av betydelse för ett internationellt samarbete för fred och säkerhet som Sverige deltar i. [70]

Genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism. [72]

Brottsdatalag – kompletterande lagstiftning. [74]

Datalagring – brottsbekämpning och integritet. [75]

Stärkt integritet i Rättsmedicinalverkets verksamhet. [80]

Uppehållstillstånd på grund av praktiska verkställighetshinder och preskription. [84]

Rekrytering av framtidens domare. [85]

Hyresmarknad utan svarthandel och otillåten andrahandsuthyrning. [86]

Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet. [89]

Makars, registrerade partners och sambors förmögenhetsförhållanden i internationella situationer. [90]

Klarlagd identitet. Om utlänningars rätt att vistas i Sverige, inre utlänningskontroller och missbruk av identitetshandlingar. [93]

Utvidgat hinder mot erkännande av utländska barnäktenskap. [96]

Tidiga förhör – nya bevisregler i brottmål. [98]

Beslag och husrannsakan – ett regelverk för dagens behov. [100]

Lagliga vägar för att söka asyl i EU. [103]

Kulturdepartementet

Nästa steg? Förslag för en stärkt minoritetspolitik. [60]

Våldsbejakande extremism. En forskarantologi. [67]

Finansiering av public service – för ökad stabilitet, legitimitet och stärkt oberoende. [79]

Nästa steg? Del 2. Förslag för en stärkt minoritetspolitik. [88]

Transpersoner i Sverige. Förslag för stärkt ställning och bättre levnadsvillkor. [92]

Värna demokratin mot våldsbejakande extremism. Hinder och möjligheter. [110]

Miljö- och energidepartementet

Kraftsamling för framtidens energi. [2]

Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. [8]

Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. [22]

Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. [32]

Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. [34]

Vem har ansvaret? [42]

Kärnavfallsrådets yttrande över SKB:s Fud-program 2016. [62]

Miljötillsyn och sanktioner – en tillsyn präglad av ansvar, respekt och enkelhet. [63]

Näringsdepartementet

För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. [1]

Detaljplanekravet. [64]

Bostäder på statens mark – en möjlighet? [71]

En gemensam bild av bostadsbyggnadsbehovet. [73]

Rättslig översyn
av skogsvårdslagstiftningen. [81]

Ett land att besöka.
En samlad politik för hållbar turism
och växande besöksnäring. [95]

Effektivare energianvändning. [99]

Kapacitetstilldelningen
på höghastighetsjärnvägen. [105]

Nystart för byggstandardiseringen genom
stärkt samverkan. [106]

Slutrapport från Sverigeförhandlingen.
Infrastruktur och bostäder –
ett gemensamt samhällsbygge. [107]

Lån och garantier för fler bostäder. [108]

Socialdepartementet

För en god och jämlik hälsa.
En utveckling av det
folkhälsopolitiska ramverket. [4]

Svensk social trygghet i en globaliserad
värld. Del 1 och 2. [5]

Kvalitet och säkerhet
på apoteksmarknaden. [15]

Läs mig! Nationell kvalitetsplan
för vård och omsorg om äldre personer.
Del 1 och 2. [21]

Samlad kunskap – stärkt handläggning. [25]

För dig och för alla. [40]

På lika villkor! Delaktighet, jämlikhet och
effektivitet i hjälpmedelsförsörjningen.
[43]

Nästa steg på vägen mot en mer jämlik hälsa.
Förslag för ett långsiktigt arbete för en
god och jämlik hälsa. [47]

Kunskapsbaserad och jämlik vård.
Förutsättningar för en lärande hälso-
och sjukvård. [48]

God och nära vård. En gemensam färdplan
och målbild. [53]

Reglering av alkoglass m.fl. produkter. [59]

Dataskydd inom Socialdepartementets
verksamhetsområde – en anpassning
till EU:s dataskyddsförordning. [66]

Enhetliga priser på receptbelagda
läkemedel. [76]

Finansiering, subvention och prissättning
av läkemedel – en balansakt. [87]

Jämställt föräldraskap och
goda uppväxtvillkor för barn
– en ny modell för föräldraförsäk-
ringen. [101]

För barnets bästa? Utredningen
om tvångsåtgärder mot barn
i psykiatrisk tvångsvård. [111]

Ett fönster av möjligheter.
– stärkt barnrättsperspektiv
för barn i skyddat boende. [112]

Alkoholreklam i sociala medier m.m. [113]

Utbildningsdepartementet

Det handlar om oss.
– unga som varken arbetar eller studerar. [9]

Ny ordning för att främja god sed
och hantera oredlighet i forskning. [10]

En nationell strategi för validering [18]

Tillträde för nybörjare – ett öppnare och
enklare system för tillträde till hög-
skoleutbildning. [20]

Samling för skolan.
Nationell strategi för kunskap och
likvärdighet. [35]

Entreprenad, fjärrundervisning
och distansundervisning. [44]

EU:s dataskyddsförordning och
utbildningsområdet. [49]

Personuppgiftsbehandling
för forskningsändamål. [50]

Utbildning, undervisning och ledning
– reformvård till stöd för en bättre
skola. [51]

Fler nyanlända elever ska uppnå behörighet
till gymnasiet. [54]

Nationella minoritetsspråk i skolan
– förbättrade förutsättningar till
undervisning och revitalisering. [91]

Etikprövning – en översyn av reglerna om
forskning och hälso- och sjukvård.
[104]

Utrikesdepartementet

Sverige i Afghanistan 2002–2014. [16]

Marknadskontrollmyndigheter
– befogenheter och
sanktionsmöjligheter. [69]