Innehåll

1 Promemorians huvudsakliga innehåll

Promemorian innehåller förslag som syftar till att genomföra ett EG-direktiv om ett gemenskapsramverk för elektroniska signaturer.

En elektronisk signatur kan användas för att säkerställa att elektroniskt överförd information inte har förändrats, vem informationens avsändare är samt för att förhindra avsändaren att förneka att han sänt informationen.

För att kunna använda en elektronisk signatur i ett öppet system, såsom Internet, där parterna inte känner varandra i förväg, finns det ett behov av att parterna kan inhämta information om kopplingen mellan en elektronisk signatur och en bestämd person. Därför har det utvecklats ett system för elektroniska signaturer som kan benämnas det öppna nyckelsystemet (Public Key Infrastructure, PKI). I detta system utfärdas ett elektroniskt intyg (certifikat) ofta av en betrodd tredje part. Ett certifikat innehåller uppgifter om vem som är innehavare av en elektronisk signatur.

Direktivets reglering bygger på elektroniska signaturer enligt det öppna nyckelsystemet. Det innehåller främst näringsrättsliga regler om dem som utfärdar certifikat, men även regler om skadeståndsansvar och om rättsverkan av elektroniska signaturer.

Direktivet föreslås genomföras genom en ny lag, lagen om vissa elektroniska signaturer m.m.

Lagen skall innehålla regler om krav på, tillsyn över och skadeståndsansvar för den som utfärdar certifikat för elektroniska signaturer, om certifikaten anges ha en viss säkerhetsnivå. Lagen skall vidare ge en särställning åt elektroniska signaturer med en viss säkerhetsnivå. Lagen skall inte innehålla regler om tillsyn och skadeståndsansvar vad gäller certifikat som utfärdas inom slutna

system och inte heller reglera frågor om ingående eller giltighet av avtal.

Enligt direktivet kan medlemsstaterna införa frivilliga ackrediteringssystem som syftar till att höja nivån på tillhandahållandet av certifikattjänster. I promemorian görs bedömningen att lagen (1992:1119) om teknisk kontroll redan nu ger en möjlighet till frivillig ackreditering av certifieringsorgan med det syfte som anges i direktivet.

En tillsynsmyndighet, Post- och telestyrelsen, föreslås utöva tillsyn över efterlevnaden av bestämmelserna i lagen och de föreskrifter som meddelas med stöd av lagen. En möjlighet för regeringen att införa ett avgiftssystem för att bekosta myndighetens verksamhet föreslås.

Den nya lagen föreslås träda i kraft den 1 januari 2001.

2 Lagtext

Lag om vissa elektroniska signaturer m.m.

Inledande bestämmelse

1 § Denna lag innehåller bestämmelser om vissa elektroniska signaturer, om certifikat för elektroniska signaturer och om certifikatutfärdare som är etablerade i Sverige.

Definitioner

2 § I lagen avses med

elektronisk handling: en bestämd mängd data i digital form som kan läsas, avlyssnas eller på annat sätt uppfattas med tekniskt hjälpmedel,

elektronisk signatur: data i elektronisk form som är fogade till eller logiskt knutna till en elektronisk handling och som används för att kontrollera om innehållet härrör från den som framstår som undertecknare,

avancerad elektronisk signatur: en elektronisk signatur som

a) är knuten uteslutande till undertecknaren,

b) undertecknaren kan identifieras genom,

c) är skapad med medel som endast undertecknaren kontrollerar, och

d) är knuten till en elektronisk handling på ett sådant sätt att alla efterföljande ändringar av den elektroniska handlingen kan upptäckas,

kvalificerad elektronisk signatur: en avancerad elektronisk signatur som är baserad på ett kvalificerat certifikat och som är skapad av en säker anordning för signaturframställning,

undertecknare: den som har kontroll över en anordning för signaturframställning,

signaturframställningsdata: unika data, såsom koder eller privata krypteringsnycklar, som undertecknaren använder för att skapa en elektronisk signatur,

anordning för signaturframställning: en konfigurerad maskin- eller programvara för att använda signaturframställningsdata,

signaturverifieringsdata: data, såsom koder eller öppna krypteringsnycklar, som används för att verifiera en elektronisk signatur,

certifikat: ett intyg i elektronisk form som kopplar ihop signaturverifieringsdata med en undertecknare och bekräftar dennes identitet,

certifikatutfärdare: den som utfärdar certifikat.

Kvalificerade certifikat

3 § Ett kvalificerat certifikat skall vara utfärdat för viss tid av en certifikatutfärdare som uppfyller kraven i 8–12 §§ och innehålla

1. uppgift om att det utfärdats som ett kvalificerat certifikat,
2. certifikatutfärdarens identitet och hemvist,
3. undertecknarens namn eller pseudonym med uppgift om att det är en pseudonym,
4. särskilda uppgifter om undertecknaren, om de är relevanta för ändamålet med certifikatet,
5. signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren vid tidpunkten för utfärdandet har kontroll över,
6. start- och sluttidpunkt för certifikatets giltighet,
7. certifikatets identifieringskod,
8. certifikatutfärdarens avancerade elektroniska signatur, och
9. uppgift om eventuella begränsningar av certifikatets användningsområde eller av värdet på de transaktioner för vilka certifikatet kan användas (transaktionsbelopp).

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten, får meddela närmare föreskrifter om krav enligt första stycket.

Säkra anordningar för signaturframställning

4 § En säker anordning för signaturframställning skall säkerställa att signaturen är tillfredsställande skyddad mot förfalskning samt att signaturframställningsdata

1. praktiskt taget kan förekomma endast en gång och att sekretessen beträffande dessa data är tillfredsställande,
2. med rimlig säkerhet inte kan härledas, och
3. kan skyddas på ett tillfredsställande sätt av undertecknaren så att obehöriga inte kan använda dem.

Anordningen får inte förändra den elektroniska handling som skall signeras eller hindra att handlingen presenteras för undertecknaren före signeringen.

5 § Kraven på en säker anordning för signaturframställning i 4 § skall anses uppfyllda beträffande sådan maskin- eller programvara som överensstämmer med standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

6 § En anordning som anges vara en säker anordning för signaturframställning får släppas ut på marknaden eller användas för att skapa en kvalificerad signatur endast om ett för ändamålet anmält organ avgjort att anordningen uppfyller kraven i 4 §.

Organ som avses i första stycket utses enligt bestämmelserna i lagen (1992:1119) om teknisk kontroll.

Med ett avgörande enligt första stycket likställs ett avgörande av ett organ, som utsetts för detta ändamål i en annan stat inom Europeiska ekonomiska samarbetsområdet.

Utfärdande av kvalificerade certifikat

7 § En certifikatutfärdare får utfärda kvalificerade certifikat till allmänheten först efter anmälan hos den myndighet som regeringen bestämmer (tillsynsmyndigheten).

8 § En certifikatutfärdare som utfärdar kvalificerade certifikat skall bedriva verksamheten med den pålitlighet som krävs för att utfärda certifikat. Certifikatutfärdaren skall därvid

1. ha personal med erforderlig kompetens för de tjänster som erbjuds, särskilt vad avser ledning, teknik och säkerhetsrutiner,
2. använda adekvata administrativa rutiner och ledningsrutiner som uppfyller erkända standarder,
3. använda pålitliga system och produkter som är skyddade mot ändringar och garanterar teknisk och kryptografisk säkerhet i de förfaranden som stöds av dem,
4. förfoga över tillräckliga medel för att kunna bedriva verksamheten enligt denna lag och bära risken för skadeståndsskyldighet,
5. genom säkra rutiner kontrollera identiteten hos den undertecknare till vilken ett kvalificerat certifikat utfärdas,
6. förfoga över ett snabbt och säkert system för registrering och omedelbar spärrning av certifikat, och
7. vidta åtgärder mot förfalskning av certifikat och i förekommande fall garantera att tillhandahållandet av signaturframställningsdata sker konfidentiellt.

Certifikatutfärdaren får inte lagra eller kopiera signaturframställningsdata.

Kraven i första stycket 3 skall anses uppfyllda beträffande sådan maskin- eller programvara som överensstämmer med standarder för produkter för elektroniska signaturer som Europeiska gemenskapernas kommission fastställt och offentliggjort referensnummer till i Europeiska gemenskapernas officiella tidning.

9 § En certifikatutfärdaren som utfärdar kvalificerade certifikat skall

1. omedelbart spärra ett certifikat när undertecknaren begär det eller när det annars finns anledning till det
2. säkerställa att exakt tidpunkt kan anges för utfärdande och spärrning av certifikat, och
3. i förekommande fall endast framställa signaturframställningsdata och signaturverifieringsdata som kan användas som komplement till varandra.

10 § En certifikatutfärdaren som utfärdar kvalificerade certifikat skall registrera all relevant information om ett kvalificerat certifikat under rimlig tid samt använda tillförlitliga system för lagring av kvalificerade certifikat i verifierbar form så att
1. endast behöriga personer kan göra tillägg och ändringar,
2. uppgifternas äkthet kan kontrolleras,
3. ett certifikat är offentligt tillgängligt endast när innehavaren av certifikatet har lämnat sitt samtycke, och
4. tekniska förändringar som äventyrar säkerhetskraven är uppenbara för den som handhar systemet.

11 § Innan en certifikatutfärdare ingår avtal om att utfärda ett kvalificerat certifikat skall certifikatutfärdaren skriftligen informera motparten om
1. villkoren och begränsningarna för användning av certifikatet,
2. förekomsten av ett frivilligt ackrediterings- eller certifieringssystem, och
3. förfaranden för klagomål och avgörande av tvister.

Informationen enligt första stycket får överföras elektroniskt, om det sker i en för motparten omedelbart läsbar form. Informationen skall på begäran också göras tillgänglig för annan.

12 § Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får utfärda närmare bestämmelser om krav enligt 8–11 §§.

Skadestånd

13 § När en certifikatutfärdare till allmänheten utfärdar certifikat som anges vara kvalificerade eller när en certifikatutfärdare till allmänheten garanterar en annan certifikatufärdares certifikat som kvalificerade är utfärdaren skadeståndsskyldig i enlighet med 14 §.

14 § Om en certifikatutfärdare inte har uppfyllt kraven i 9 § eller om ett certifikat vid utfärdandet innehåller felaktiga uppgifter eller inte uppfyller kraven i 3 § första stycket, skall certifikatutfärdaren ersätta den skada som därigenom åsamkas den som har rimlig anledning att förlita sig på certifikatet. Certifikatutfärdaren är dock inte skyldig att utge ersättning om utfärdaren kan visa att skadan inte har orsakats av vårdslöshet hos denne.

Trots vad som föreskrivs i första stycket är certifikatutfärdaren inte ersättningsskyldig för skada som härrör från att ett certifikat använts i strid med tydliga begränsningar avseende användningsområde eller transaktionsbelopp som angetts i certifikatet.

Behandling av personuppgifter

15 § En certifikatutfärdare som utfärdar certifikat till allmänheten får endast inhämta personuppgifter direkt från den som uppgifterna avser eller med dennes uttryckliga samtycke och endast i den utsträckning som är nödvändig för att utfärda eller upprätthålla ett certifikat. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan uttryckligt samtycke från den som uppgifterna avser.

Rättslig verkan för elektroniska signaturer

16 § Om det av lag eller annan författning följer vissa formkrav för att en rättshandling skall anses giltig eller en förpliktelse fullgjord och om dessa krav kan uppfyllas genom elektronisk kommunikation med användning av någon form av elektronisk signatur, skall en kvalificerad elektronisk signatur godtas.

Tillsyn

17 § Tillsynsmyndigheten skall ha tillsyn över certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade och över anordningar som anges vara säkra anordningar för signaturframställning.

18 § 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 verkställighet hos kronofogdemyndigheten av de beslut som avser åtgärder för tillsynen enligt första och andra styckena. Därvid gäller bestämmelserna om sådan verkställighet som avses i 16 kap. 10 § utsökningsbalken.

19 § Tillsynsmyndigheten får meddela de förelägganden och förbud som behövs för efterlevnaden av denna lag eller av föreskrifter som meddelats med stöd av lagen.

20 § Tillsynsmyndigheten får förelägga certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade att helt eller delvis upphöra med verksamheten. Myndigheten får därvid besluta hur verksamheten skall avvecklas.

21 § Förelägganden och förbud enligt denna lag får förenas med vite.

Avgifter

22 § Regeringen eller, om regeringen bestämmer det, tillsynsmyndigheten får föreskriva om skyldighet för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten att betala avgift för tillsynsmyndighetens verksamhet enligt denna lag.

Överklagande

23 § Tillståndsmyndighetens beslut enligt denna lag eller enligt föreskrifter som meddelats med stöd av lagen får överklagas hos allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Tillståndsmyndigheten får bestämma att beslut enligt denna lag skall gälla omedelbart.

---

1. Denna lag träder i kraft den 1 januari 2001.

2. Beträffande certifikatutfärdare som redan före ikraftträdandet utfärdar kvalificerade certifikat till allmänheten skall föreskriften i 7 § om anmälan tillämpas först den 1 februari 2001.

3 Ärendet

Den 30 november 1999 antogs Europaparlamentets och rådets direktiv om ett gemenskapsramverk för elektroniska signaturer.

Direktivet har ännu inte (december 1999) publicerats i Europeiska gemenskapernas officiella tidning.

Direktivet, som det förelåg den 30 november 1999, bifogas som *bilaga*.

Direktivet innehåller bestämmelser om elektroniska signaturers rättsliga verkan och en reglering av de organ som avser att erbjuda elektroniska intyg om signaturers äkthet. Medlemsstaterna skall ha genomfört direktivet ett och ett halvt år efter det att det trätt i kraft.

Under förhandlingarna om direktivet har samråd skett med en av Näringsdepartementet tillkallad referensgrupp bestående av företrädare för Kommerskollegium, Statskontoret, Riksarkivet, SWEDAC, Post- och telestyrelsen, Konsumentverket, Riksskatteverket, Göteborgs universitet, IT-kommissionen, Svenska kommunförbundet, Stockholms Handelskammare, SEIS, Sveriges advokatsamfund, Svenska Bankföreningen, Sveriges Industriförbund, Svenska IT-företagen, Advokatfirman Lagerlöf & Leman, Telia Promotor AB, Tele2 AB, Posten AB, Ericsson AB, iD2 Technologies AB och IBM Svenska AB.

Denna promemoria har föregåtts av samråd med Danmark, Island, Norge och Finland. Därvid har man försökt enas om tolkningen av direktivet och diskuterat genomförandet av det. Avsikten är att fortsätta de nordiska överläggningarna efter remissbehandlingen av denna promemoria.

4 Bakgrund och utgångspunkter

4.1 Varför behövs elektroniska signaturer?

En elektronisk signatur kan användas för att säkerställa att elektroniskt överförd information inte har förändrats, vem informationens avsändare är samt för att förhindra avsändaren att förneka att han sänt informationen.

Långt innan informationsteknologin (IT) började förändra vårt sätt att hantera och kommunicera information har den personliga namnteckningen varit en väsentlig del av den ekonomiska och juridiska verkligheten. Namnteckningar eller signaturer tillgodoser flera olika behov vid skriftlig informationshantering.

En signatur kan ge uttryck för en *vilja* att handla på ett visst sätt. Närmast avser undertecknaren att acceptera innehållet i den text som är placerad före namnteckningen. Nära knuten till denna viljefunktion är den *varningsfunktion* som är förbunden med namnteckningen. Ett krav på underskrift klargör på ett tydligt sätt att en bindande förpliktelse kan vara för handen.

Namnteckningen kan vidare användas för att *identifiera* en person.

Genom att skriva en namnteckning på en handling som innehåller en text, knyts texten på visst sätt till namnteckningen och därmed till den person som utpekas av namnteckningen. Namnteckningen kan sålunda användas för att identifiera den person som skall knytas till texten. Det faktum att både texten och namnteckningen fästs på papperet medför ett visst skydd mot manipulation (”*äkthet*”).

Identifieringsfunktionen och äkthetsfunktionen kan användas i situationer där behov av *bevisning* uppkommer, t.ex. för att i efterhand styrka rättshandlingar. Att förse en pappershandling med en namnteckning kan sägas vara ett sätt att säkra eventuellt framtida behov av att kunna bevisa såväl identiteten på som avsikten hos den som undertecknat en handling. Uttryckt på ett annat sätt kan namnteckningen sägas ha en funktion som hinder för undertecknaren att med framgång hävda att han inte står bakom en handling (”*oavvislighet*”).

I IT-system finns det ofta behov av att kunna verifiera en uppgiven identitet. ”Närvarande” i ett IT-system betyder oftast inte att finnas i samma fysiska rum men att via någon form av förbindelse vara i direkt kontakt med det tekniska systemet, som har behov av att verifiera användarens identitet. Det behövs för att man skall kunna styra behörighet att ta del av information som inte skall vara allmän. I vissa fall behövs det för att styra någon mer materiell funktion, som t.ex. att få tillgång till sedlar i en uttagsautomat. Identitetsverifieringen används också för att man i efterhand skall kunna spåra vad någon gjort i ett elektroniskt system. Den metod som helt dominerat för att kontrollera identiteten av användare i datorsystem är att använda ett lösenord, ibland reducerat till en fyrsiffrig PIN-kod. En elektronisk signatur kan utgöra en säkrare metod som kan användas över Internet och andra osäkra förbindelser. Den mest intressanta frågan är emellertid om elektroniska signaturer också kan ges de funktioner vid elektronisk kommunikation som traditionella underskrifter har vid pappersbaserad kommunikation.

4.2 Rätts- och bevisverkan av signaturer

Allmänt

En nyckelfråga är om en elektronisk signatur kan ges samma rättsverkan som en egenhändig namnunderskrift. Det är dock inte alltid klart vad som avses med denna frågeställning. Frågan har vidare olika innebörd beroende på vilken rättsordning man syftar på. Det

finns rättsordningar där den traditionella namnteckningen har en rättslig betydelse i större utsträckning och på ett annat sätt än i svensk rätt. I Sverige finns det i varje fall inom civilrätten förhållandevis få regler som innebär att underskriften är en förutsättning för att vissa rättsverkningar skall inträda. Däremot kan underskriften ofta ha betydelse som bevis för ett visst påstått förhållande, dvs. bevisverkan.

Rättsverkan

När det gäller affärssituationer som avtal om köp av varor och tjänster samt hyra m.m. finns endast ett mycket begränsat antal situationer där svensk lagstiftning kräver avtal i skriftlig form med underskrifter av parterna. Som exempel kan nämnas fastighetsköp och krediter till konsumenter. Ett avtal om köp av fast egendom skall enligt 4 kap. 1 § jordabalken alltid upprättas skriftligen och undertecknas av köparen och säljaren. Ett avtal som gäller kredit till konsument skall enligt 9 § konsumentkreditlagen (1992:830) ingås skriftligen och undertecknas av konsumenten. Frånvaron av underskrifter kan ha olika konsekvenser i olika fall. I fallet med fastighetsförvärv är avtalet ogiltigt om underskrift saknas. I fallet med konsumentkrediter är avtalet ändå giltigt utom i fråga om villkor som är till nackdel för konsumenten. På familjerättens område finns det också ett antal situationer där det krävs underskrifter. Det gäller exempelvis testamente och äktenskapsförord, som inte är giltiga utan underskrifter. På förvaltningsrättens område finns det ett tämligen stort antal regler om att ansökningar m.m. till myndigheter skall göras skriftligen och undertecknas av exempelvis den sökande.

I det vardagliga privat- och affärslivet finns det dock väldigt få lagregler om att underskrifter måste användas. Användningen av underskrifter eller namnteckningar har i stället under lång tid utvecklats som en slags vardagens praxis. Undertecknandet har blivit en etablerad metod för bekräftelse, kontroll och bevisning kring våra göranden och låtanden i allmänhet. Detta är alltså något som i

princip utvecklats utan lagstiftning. Av någon betydelse i sammanhanget kan kanske vara existensen av brottet *förnekande av underskrift*. Enligt 15 kap. 13 § brottsbalken kan nämligen den som förnekar sin underskrift på en urkund dömas till böter eller fängelse i högst sex månader, förutsatt åtgärden innebär fara i bevishänseende. Är brottet grovt är straffet fängelse i högst två år.

Oavsett hur de lagregler som finns rörande underskrifter skall uppfattas i samband med elektronisk kommunikation, är det knappast främst lagstiftning som står i vägen för att elektroniska signaturer skall få samma betydelse som egenhändiga namnunderskrifter. Det viktigaste torde i stället vara att det utvecklas säkra och lättanvända tekniska lösningar för elektroniska signaturer så att människor känner tillit till dem och tycker att de är praktiska att använda.

När det gäller de formkrav som ändå finns på underskrift i olika författningar är den avgörande frågan om syftena bakom dessa krav lika väl kan uppfyllas med elektroniska signaturer. I detta sammanhang kan det vara intressant att erinra om det betraktelsesätt som kan uttolkas ur UNCITRALs[1] modellag om elektronisk handel[2], kallat *funktionell ekvivalens*. Detta betraktelsesätt innebär att man, när man ställs inför frågan om ett nytt kommunikationssätt bör omfattas av det gamla regelverket, skall ta fasta på de bakomliggande syftena med regeln. Sedan får man analysera om dessa syften kan tillgodoses också i den elektroniska miljön. Det elektroniska kommunikationssättet skall inte förnekas rättslig betydelse enbart på den grunden att det sker i elektronisk form.

De formkrav på underskrifter som finns i svenska författningar kan ha många syften. Ett syfte kan vara att *säkra bevisning* om att en åtgärd vidtagits, om vem som vidtagit den och om dess innehåll. Därvid kan ett viktigt syfte vara att det smidigt går att *arkivera och bevara* informationen under mycket lång tid. Ett annat syfte kan vara att statsmakterna kan *underlätta vissa förfaranden*, exempelvis beskattning. Ett betydelsefullt syfte är vidare ofta att formkrav kan ha en *varningsfunktion*, dvs. mana till och ge tid för

[1] United Nations Commission on International Trade Law.
[2] ”Model Law on Electronic Commerce”, antagen 1996.

eftertanke innan man vidtar en betydelsefull rättshandling eller annan åtgärd. Dessa formkrav har införts innan det var aktuellt med elektroniska rutiner och signaturer eller kan antas ha tillkommit utan att informationstekniken har beaktats.

Frågan är då hur krav på underskrift eller liknande uttrycksätt bör förstås vid elektronisk hantering. Denna fråga har behandlats bl.a. i betänkandet Elektronisk dokumenthantering (SOU 1996:40). I betänkandet anförs att ordet *skriftlig*, i anknytning till förfaranderegler, huvudsakligen synes användas för att utesluta muntliga rutiner och utesluter därmed inte användning av elektroniska rutiner. I betänkandet konstateras emellertid att när det krävs att en handling skall vara ”undertecknad” innefattas inte elektroniska rutiner. Här hänvisar utredaren bl.a. till att telefaxmeddelanden i praxis inte ansetts uppfylla rättegångsbalkens krav på att handlingen skall vara egenhändigt undertecknad genom att det i kravet på egenhändigt undertecknande också har ansetts ligga ett krav på att det just är det undertecknade exemplaret som skall ges in till domstolen.

Ett åtminstone delvis annorlunda synsätt förefaller finnas i exempelvis Elektronisk handel och avtal, 1998, s. 65 ff. Med utgångspunkt från en analys av syftena bakom olika formkravsregler menar författaren att ett krav på underskrift i en författning i allmänhet inte behöver betyda att det krävs en egenhändigt skriven namnunderskrift, utan att det skulle gå lika bra med en elektronisk signatur. Resonemanget bygger på principen om funktionell ekvivalens som kan härledas från UNCITRALS modellag om elektronisk handel

Även om man anlägger ett sådant betraktelsesätt som kan uttolkas ur UNCITRALs modellag är det i dag inte realistiskt att tänka sig att svenska domstolar och myndigheter skulle tolka alla formkrav på underskrift eller liknande i författningar så att de även skulle kunna uppfyllas genom elektroniska signaturer. I sammanhanget är det dock intressant att påpeka att när det gäller formkrav som kräver skriftlighet har myndigheter och domstolar på vissa

områden godtagit att dessa krav kan uppfyllas med elektroniska rutiner, exempelvis telefax.

Elektroniska signaturers likställighet med traditionella egenhändiga namnunderskrifter är en komplicerad fråga. Det är viktigt att komma ihåg att de är olika till sin natur och utförs på olika sätt. Den elektroniska signaturen bygger ofta på ett komplicerat tekniskt krypteringsförfarande och en och samma signatur kan oftast användas av alla personer som har tillgång till de nödvändiga koderna och signeringsutrustningen. Det är f.n. möjligt för innehavaren av en elektronisk signatur att överlämna den till andra personer. I gengäld präglas tekniken med elektroniska signaturer av en hög grad av säkerhet. Förfalskningar avseende härkomst och innehåll är betydligt svårare att åstadkomma än när det gäller pappershandlingar med namnunderskrifter. Namnunderskriften däremot är knuten till en viss persons sätt att skriva och kan inte överlämnas till andra. Vissa personer kan dock vara mycket skickliga på att efterbilda andras underskrifter. En egenhändig namnunderskrift är vidare lätt att påföra en handling och kan vara lätt att läsa. De båda metoderna har således delvis olika fördelar och nackdelar.

Bevisverkan

Även i de fall en underskrift inte utgör ett formellt krav tillmäts den ibland mycket stor betydelse i bevishänseende. En namnunderskrift på en handling kan användas som bevis för att en viss person skrivit under den och att denna person godtagit de villkor som står i exempelvis ett skriftligt kontrakt.

Svensk rättsskipning bygger på principen om fri bevisprövning. Det betyder egentligen två saker. Det ena är att det inte finns någon begränsning när det gäller vilka kunskapskällor man får använda som bevis i en rättegång. Principen innebär dessutom att när en domare skall bedöma och värdera bevisningen är denne obunden av lagregler. Det finns alltså ingen begränsning i svensk rätt om att åberopa eller beakta elektroniska signaturer eller andra IT-tillämpningar som bevisning.

Vad som däremot ibland finns i både lagstiftning och praxis är bevisbörderegler. I det här sammanhanget är det särskilt intressant att se om det finns några bevisbörderegler när någon förnekar en namnunderskrift och påstår att den är förfalskad. Det har inte ansetts nödvändigt att lagstifta om detta, men det finns avgöranden där Högsta domstolen har uttalat sig i frågan. Rättsfallet NJA 1976 s. 667 gällde ett fall där en person förnekade att det var han som undertecknat en skuldförbindelse. Högsta domstolen uttalade att om någon gör en sådan invändning får den påstådde fordringsägaren visa att handlingen är äkta. Om en gäldenär däremot gör gällande att handlingen visserligen är äkta men att texten ändrats, s.k. innehållsförfalskning, anses dock allmänt att gäldenären i princip har bevisbördan. Högsta domstolen har även prövat frågan vad som skall gälla när det gäller påstådda förfalskningar av inköpsnotor i samband med användande av kontokort (NJA 1992 s. 263). I detta rättsfall ansåg Högsta domstolen det ligga på kontohavaren att åtminstone göra antagligt att det förelåg en förfalskning. Om detta krav uppfylls krävs enligt Högsta domstolen att kontokortsföretaget visar att inköpsnotan är äkta.

Frågan om bevisverkan av elektroniska signaturer behandlades i departementspromemorian Digitala signaturer – en teknisk och juridisk översikt (Ds 1998:14). Där gjordes bedömningen att det aldrig kan komma i fråga att rubba den fria bevisprövningen. Man ansåg vidare att det inte heller skulle vara ändamålsenligt att uppställa vissa generella bevisbörderegler för elektroniska signaturer. Så gott som samtliga remissinstanser delade denna bedömning.

Det vore onekligen en farlig väg att ge generella bevisbörderegler när det gäller elektroniska signaturer. Bevisbördan bör inte placeras uteslutande med ledning av vilket medium som kommit till användning. Det avgörande måste naturligtvis bl.a. vara vad det är för typ av uppgifter som bekräftats genom den elektroniska signaturen och vad det rör för typ rättshandling och vad det är för förhållande som skall bevisas. Parternas inbördes förhållande kan också ha betydelse.

4.3 Tekniska grunder

Teknik och juridiska överväganden kring elektronisk dokumenthantering och signering har inte funnits i särskilt många år. Det är därför inte förvånande att terminologin fortfarande utvecklas och kan framstå som något förvirrande. Det beror också på att samma eller snarare liknande begrepp används på flera olika sätt. Tekniker har andra utgångspunkter än jurister. Marknadsförare har ett annat språkbruk med slagkraftiga uttryck som kanske är lättanvända men inte alltid så lämpliga av andra skäl. Till detta kommer att utvecklingen i hög grad är internationell och det är svårt att hitta bra svenska termer på begrepp som länge endast haft engelska namn och förkortningar.

Termen ”digital signatur” har bl.a. i EG-direktivet fått ge vika för ”elektronisk signatur”. Vad gäller relevansen av ordet ”elektronisk” kan följande sägas. En signatur är som regel inte intressant isolerad, utan när den används för att säkra andra uppgifter av något slag. Det blir i hög grad karaktären av dessa som också avgör vilka egenskaper en signatur har. Idag lagras och behandlas uppgifter eller data i hög grad i elektroniska system. Man kallar därför ofta sådana data för *elektroniska* och motsvarigheten till den handskrivna underskriften kan kallas en *elektronisk signatur*, också för att markera att ett elektroniskt system har använts för att skapa en sådan elektronisk signatur.

Det är dock viktigt att i ett rättsligt begreppssystem kunna skilja på metoder som används i framställningen av uppgifter inklusive signaturer och de uppgifter man faktiskt har att ta ställning till. Det faktum att en elektronisk ordbehandling idag nästan alltid föregått framställningen av en traditionell pappershandling saknar betydelse för bedömningen av handlingen i fråga. Det kan däremot vara väsentligt att man måste använda sig av ett tekniskt elektroniskt hjälpmedel för att uppfatta och bedöma uppgifterna eller signaturerna.

De ”elektroniska” signaturer som finns i dag är uteslutande ”digitala” signaturer. Dagens informationsteknik är inriktad på *digital* representation av information där det centrala skyddsob-

jektet är ett informationsinnehåll som representeras av ettor och nollor. Under hanteringens gång och när information kommuniceras byter denna representation många gånger fysisk form. Den digitala datamängden kan finnas som högst tillfälliga elektriska strömmar, mer permanenta magnetfält på en hårddisk, eller bestå av små fördjupningar på en CD.

En väsentlig egenskap som skiljer den digitala handlingen från andra data är att den är helt entydig med sin digitala informationsrepresentation. Endast vissa bestämda värden tillåts, representerade av siffror, i praktiken ettor och nollor. Det finns inga gråskalor. Det är denna egenskap som gör att man i digitala system exakt kan kopiera en datamängd så att kopian är identisk med ursprungsmängden. Analog kopiering blir aldrig på samma sätt identisk. Det går inte att på traditionellt sätt skilja ett originalexemplar från en kopia när data förs över från en databärare till en annan; informationen förekommer endast som ett originalinnehåll. Denna egenskap gäller givetvis signaturer lika väl som andra data.

Vid den följande kortfattade genomgången av de tekniska grunderna redogörs för signering av information i digital form. (I promemorian används emellertid genomgående termen ”elektronisk signatur” som numera får anses vara den vedertagna beteckningen.) För en mer utförlig beskrivning hänvisas till departementspromemorian Digitala signaturer – en teknisk och juridisk översikt (Ds 1998:14).

4.3.1 Kryptografisk teknik med privata och öppna nycklar

Den teknik som idag allmänt används för att skapa elektroniska signaturer utnyttjar kryptografiska principer för att med en matematisk funktion generera en signatur från de data i digital form som ingår i den elektroniska handling som skall signeras och någon form av unik nyckel som hör ihop med den som signerar (undertecknaren).

Elektroniska signaturer säkerställer att förändring av ett meddelande inte gjorts samt verifierar vem som signerat det. Kryptografiska metoder kan även användas för att dölja ett meddelandes informationsinnehåll. Detta användningsområde behandlas emellertid inte i denna promemoria.

Signering

Signering av datamängden, som kan representera text, bild, ljud eller information i någon annan form, börjar med att datamängden förbehandlas med en s.k. hashfunktion. Av datamängden skapas därigenom ett *hashvärde* som kan liknas vid ett kondensat eller ”fingeravtryck” av datamängden. Hashvärdet är
– unikt, dvs. alla datamängder som inte är identiska ger olika hashvärden, och
– icke omvändbart, så att datamängden inte kan beräknas utifrån hashvärdet.

Nästa steg i signeringen sker genom *kryptering*. Kryptering innebär att en datamängd omvandlas genom en bestämd metod, en algoritm. Vid krypteringen används förutom datamängden vissa andra ingångsvärden som fungerar som nycklar vid krypteringen.

Vid signering används i allmänhet *asymmetrisk kryptering* med användande av ett *nyckelpar*. En nyckel är ett mycket stort tal, idag oftast 1 024 bitar motsvarande cirka 300 siffror. Den ena delen av nyckelparet kallas *privat nyckel* och används av undertecknaren för att skapa signaturer. Den måste skyddas mot obehörig åtkomst, vilket diskuteras närmare nedan (se avsnitt 4.3.5). Den andra delen av nyckelparet kallas *öppen nyckel* och kan användas för att verifiera signaturer men inte för att skapa dem. Denna nyckel kan spridas öppet till alla som har anledning att verifiera en persons elektroniska signatur, eftersom den inte kan missbrukas för att skapa signaturen och därmed inte behöver distribueras med sekretesskydd. Krypteringen sker genom att hashvärdet (kondensatet av datamängden) bearbetas med hjälp av en algoritm som tar den privata nyckeln som ett ingångsvärde. Resultatet av denna beräkning är den elektroniska signaturen.

Signeringen avslutas med att signaturen, bestående av det krypterade hashvärdet, tillförs den signerade handlingen. Handlingen med signatur kan nu sändas öppet till mottagaren.

Viktiga funktioner hos asymmetrisk kryptering är dels att ett krypterat meddelande inte kan dekrypteras med samma nyckel i nyckelparet, dels att det trots kunskap om den ena nyckeln i nyckelparet är omöjligt att beräkna den andra nyckeln. De två nycklarna är därmed beroende av varandra och bildar ett unikt par. Den asymmetriska krypteringen binder innehavaren av den privata nyckeln till hashvärdet.

Verifiering

En elektronisk signatur verifieras på följande sätt. Mottagaren separerar meddelandet och den medföljande signaturen. Samma hashfunktion som avsändaren använde vid sin signering används för att bearbeta det mottagna meddelandet, varvid man får ett hashvärde. Signaturen, i form av ett krypterat hashvärde, dekrypteras av mottagaren med upphovsmannens öppna nyckel och ett okrypterat hashvärde erhålls. Mottagaren jämför dessa två hashvärden. Om de är identiska vet mottagaren att meddelandet inte är förändrat samt att det verkligen härrör från innehavaren av det unika nyckelpar som innehåller den använda öppna nyckeln. Han kan vara säker på detta eftersom det bara är avsändarens privata nyckel som kan ha krypterat hashvärdet och det endast är ett identiskt meddelande som kan skapa ett identiskt hashvärde.

En central fråga med dessa tekniker är hur den som skall verifiera en signatur skall kunna vara säker på att en bestämd öppen nyckel verkligen hör ihop med den person som framstår som utställare av en elektronisk handling. Man kan tänka sig olika metoder av säker teknik och administrativa funktioner men de som helt kommit att dominera bygger på en användning av s.k. *certifikat* (se vidare nedan under avsnitt 4.3.3).

4.3.2 Utrustning för att signera elektroniskt

När en elektronisk handling skall signeras behöver undertecknaren någon form av elektronisk utrustning som kan:

- Presentera den information som skall signeras på ett begripligt sätt så att man vet vad man signerar.
- Lagra och använda den privata signeringsnyckel som skall användas.
- Skapa en medveten beslutspunkt för undertecknaren att faktiskt signera.
- Utföra den beräkning som krävs, först av hashfunktionen på de digitala data som skall signeras och sedan den kryptoberäkning som behövs för att skapa den elektroniska signaturen.

4.3.3 Certifikat

Ett certifikat för en öppen nyckel är i sig en elektroniskt signerad handling där en betrodd part intygar att en viss öppen nyckel hör ihop med en viss person. Mottagaren kan vända sig till den som utfärdat certifikatet för att få veta, inte bara vem som innehar den öppna nyckeln, utan också om certifikatet, och därmed signaturen, är giltigt eller om giltighetstiden löpt ut eller certifikatet är spärrat. Mottagaren kan också få reda på om det finns begränsningar för vad signaturen kan användas till.

Certifikaten kan spridas på olika sätt, finnas i elektroniska katalogtjänster m.m. Det är också vanligt att den som signerar en elektronisk handling inkluderar ett certifikat med sin öppna nyckel, som skall kunna kontrolleras av mottagaren. Sådana certifikat, eller nyckelcertifikat, brukar följa en internationell standard kallad X.509, som anger vilka uppgifter som måste eller kan förekomma och hur dessa skall vara anordnade. Själva certifikatet är en signerad mängd data där den som utfärdat certifikatet tar ansvar för innehållet.

4.3.4 Infrastruktur för öppna nycklar

För att man på ett säkert och ekonomiskt rimligt sätt skall kunna använda elektroniska signaturer (och andra tjänster som utnyttjar öppna nycklar) i samhället mellan större grupper, enskilda, företag och myndigheter erfordras en infrastruktur som på engelska ofta kallas public key infrastructure, PKI (”det öppna nyckelsystemet”). Även i svenska texter är förkortningen PKI vanlig. Vad som ingår i begreppet är relativt oklart men följande kan nämnas.

- Utfärdande av certifikat är centralt.
- Distribution av certifikat kan i och för sig ske med hjälp av en öppen katalogtjänst. Vid kryptering för konfidentialitet och för identifiering av användare kan det ofta vara en nödvändig lösning men för elektroniska signaturtjänster behövs inte katalogen. I samband med utfärdandet kan nämligen nyckelinnehavaren/undertecknaren erhålla sitt certifikat i någon form (t.ex. på ett elektroniskt ID-kort eller via e-post) och den som signerar kan själv bifoga certifikatet till den signerade handlingen.
- Innehavaren av certifikatet och eventuellt andra parter skall kunna begära hos den som utfärdat certifikatet att det skall spärras, t.ex. beroende på att den privata nyckeln som korresponderar med certifikatets öppna nyckel befaras ha kommit på avvägar. Det kan t.ex. vara fråga om ett borttappat eller stulet elektroniskt ID-kort.
- Tillhandahållande av information om certifikatens aktuella status via spärrlistor eller statuskontroll ”on-line” av certifikat är en nödvändig funktion för att man skall kunna ha tilltro till en elektronisk signatur.
- En definition av ett certifikatformat som kan förstås av de samverkande parterna måste finnas. Detta kan synas trivialt men möjliggör att man faktiskt kan kommunicera och t.ex. verifiera signaturer.

4.3.5 Vissa säkerhetsfrågor för system med elektroniska signaturer

Förmedlingen av information från dataform till en för avsändaren/mottagaren uppfattbar form

Det är viktigt att klargöra gränserna mellan de digitala data som finns i ett elektroniskt informationssystem som t.ex. en vanlig persondator och den information som en människa slutligen tolkar utifrån dessa data. Vare sig dessa data skapar en text, en figur på en bildskärm, skrivs ut på papper eller kommunicerar talat språk via en högtalare, så tolkas primära data till en annan form, vilken mer eller mindre exakt uppfattas av en person som utgör mottagare. I allmänhet har man nöjt sig med att försöka skydda den digitala handlingen med hjälp av signaturtekniker utan att ta hänsyn till den process som så småningom skall göra dessa data begripliga för en människa.

Denna skillnad gäller inte bara för den tänkte mottagaren av den elektroniska handlingen utan kan även gälla för den som är upphovsman till informationen. I de moderna informationssystemen är det oftast svårt att vara helt övertygad om att den information som skrivs in och som kan iakttas före elektronisk signering också är korrekt representerad av den datamängd som blir signerad i en komplicerad matematisk process vars närmare detaljer inte kan iakttas eller kontrolleras direkt.

Skyddet för den privata nyckeln

Den mest centrala frågan att ta ställning till när det gäller utrustning för elektroniska signaturer, gäller skyddet av den privata nyckeln. Man brukar här tala om hårda respektive mjuka lösningar. Med hårda menar man då en speciell utrustning som tillverkats enligt mycket strikta metoder och som innehåller ett skyddande fysiskt skal mot olika former av attacker. Aktiva (smarta) kort är den mest

använda formen. För en närmare diskussion om fördelar med att använda aktiva kort för elektroniska signaturer hänvisas till departementspromemorian Digitala signaturer – en teknisk och juridisk översikt (Ds 1998:14) kapitel 3 och 5 samt bilaga 2.

Lösningar där man i stället med vanlig datorutrustning och speciell programvara försöker skydda en privat nyckel (med t.ex. kryptering) kallas på motsvarande sätt mjuka och är ofta billigare och enklare att införa, men säkerheten är mer svårbedömbar.

I många elektroniska signatursystem har man någon form av metod för att försöka verifiera att den behöriga innehavaren av signeringsnyckeln verkligen är närvarande. Den idag helt dominerande metoden är att ett lösenord erfordras. Med aktiva kort eller mobiltelefoner eller andra smärre handburna enheter har detta lösenord reducerats till i allmänhet fyra siffror (PIN-kod).

Denna typ av verifiering, som inte ensam duger till att unikt identifiera en person, kan dock i många fall tillsammans med övriga skyddsåtgärder anses vara tillräcklig för detta syfte. Man bör betona att i system med sådana handburna signeringsverktyg som aktiva kort, så är det det fysiska innehavet som är den väsentligaste skyddsfaktorn. En annan metod som diskuterats en hel del som ersättning för en PIN-kod, men ytterst sällan prövats i samband med signeringssystem, är att använda någon form av biometrisk mätutrustning (som exempelvis känner av den behöriga innehavarens tumavtryck) för att öka säkerheten.

Den pragmatiska lösning som i allmänhet tillämpas av myndigheter, företag och privatpersoner är att använda olika skyddsåtgärder, inte minst vanliga fysiska lås som skall säkerställa att den persondator och den programvara som används är rimligt säkra.

Det är också viktigt att uppmärksamma skyddet av övrig signeringsutrustning. Med utrustning måste man här inkludera all den programvara som används för den aktuella tillämpningen.

4.4 Standardisering, ackreditering, certifiering

Standarder och standardiseringsarbetet har ökat i betydelse för stora delar av samhället. En stor mängd varor och tjänster är utformade enligt internationell eller nationell standard. Glödlampan passar i sockeln, film passar i kameran, skruvar i muttrar, papper i pärmar etc, tack vare standarder.

Ett system med i princip frivilliga överenskommelser mellan olika intressenter, standarder, har vuxit fram. Ursprungligen togs standarder fram av näringslivet, huvudsakligen för att sänka tillverkningskostnaderna. Så småningom stod det dock klart att standardisering och tillverkarens egenkontroll inte var tillräckligt för att garantera säkerheten och den tekniska kvaliteten hos olika tillverkares produkter. Därför skapades olika, frivilliga, certifieringssystem. Med *certifiering* (av överensstämmelse) menas en handling, ofta utförd av en tredje part, som visar att tillräcklig tilltro uppnåtts att en vederbörligen identifierad produkt, process eller tjänst är i överensstämmelse med en bestämd standard eller med ett annat regelgivande dokument.

Standarder utnyttjas för att harmonisera tekniska regler som har betydelse för skydd av liv, hälsa och miljö och är således en angelägenhet även för myndigheter och andra offentliga organ. Standardisering har numera en mycket stor betydelse för den fria rörligheten för varor och tjänster över nationella gränser.

Internationella standardiseringsorganisationen, ISO, är en världsomfattande sammanslutning av nationella standardiseringsorgan. Tillsammans med IEC (International Electrotechnical Commission), som täcker standardisering inom det elektrotekniska området, utgör ISO världens största icke-statliga system för frivilligt industriellt och tekniskt samarbete på internationell nivå. Resultatet av ISO:s arbete utgörs av ISO-standarder eller riktlinjer.

Centralorgan för standardisering i Sverige är SIS (Standardiseringen i Sverige), som har till uppgift bl.a. att främja och fastställa svensk standard. SIS är en fristående ideell förening, vars stadgar är fastställda av staten. All fastställd svensk standard

har prefixet SS. Om det rör sig om en svensk standard som överför global standard utan ändringar blir prefixet t.ex. SS-ISO. Överförd europeisk standard betecknas SS-EN.

SIS och dess auktoriserade standardiseringsorgan inom olika fackområden deltar aktivt i utarbetandet av internationella standarder, dels inom ISO och IEC, men även i de europeiska standardiseringsorganen CEN (Comité Européen de Normalisation), CENELEC (Comité Européen de Normalisation Electrotechnique) och ETSI (European Telecommunications Standards Institute).

Det bör dock poängteras att inom IT-området, där utvecklingen är mycket snabb, sätts standarder i praktiken ofta av de dominerande leverantörerna och av andra organisationer än de ovan beskrivna standardiseringsorganen.

EG presenterade 1985 i den s.k. vitboken ett program för förverkligande av den inre marknaden, innefattande bl.a. fri rörlighet för varor (det som senare resulterade i den reformering av Romfördraget som skedde genom den Europeiska enhetsakten). En ny metod (”the New Approach) för harmonisering av medlemsstaternas lagstiftning rörande produkter anvisades. Enligt denna skall direktiven endast fastställa de väsentliga säkerhetskrav som produkterna skall uppfylla med hänsyn till skydd för liv, hälsa eller miljö m.m. Det överlåts till de europeiska standardiseringsorganen att utarbeta harmoniserade frivilliga standarder med närmare tekniska specifikationer för produkten. En produkt som tillverkas i enlighet med dessa standarder skall förutsättas uppfylla de väsentliga kraven i direktivet. Tillverkarens egenkontroll i kombination med en försäkran från tillverkaren om att tillämpliga standarder har följts skall normalt vara tillräcklig kontrollåtgärd.

Produkter som kan medföra stor risk för hälsa och säkerhet skall dock i normalfallet kontrolleras av ett tredjepartsorgan. Detsamma gäller när en tillverkare inte har tillämpat harmoniserade standarder eller då sådana saknas. Det skall räcka med att en sådan kontroll sker i ett land för att få tillträde till hela den inre marknaden.

Efter förslag i vitboken antog EG också en resolution om en helhetssyn för provning och certifiering[3]. I denna anges riktlinjer för hur EG:s system för bestyrkande av överensstämmelse skall utformas. Som ett komplement till den nya metoden föreskrivs hur ömsesidiga erkännanden av provningar och certifieringar mellan medlemsstaterna skall komma till stånd samt gemensamma villkor och regler för laboratorier och certifierings- och kontrollorgan.

De tredjepartsorgan som får utföra en sådan bedömning som omtalats ovan skall anmälas till Europeiska gemenskapernas kommission. Organen kallas *anmälda organ*. Dessa kan vara både offentliga och privaträttsliga organ som av medlemsstaten bedömts ha tillräcklig kompetens för uppgiften. Det anmälda organet utför bedömningen på uppdragsbasis och får normalt själv bestämma avgiften för detta.

För att skapa förtroende för provningar och bevis om överensstämmelse, oavsett i vilket land de utförts, har de europeiska standardiseringsorganen, på EG:s vägnar, utarbetat enhetliga standarder för kompetensen hos provnings,- certifierings- och kontrollorgan. Dessa återges i den europeiska standardserien EN 45 000.

Att kraven är uppfyllda kan visas genom ackreditering[4]. EG:s helhetssyn förutsätter också att det inrättas nationella ackrediteringsorgan med uppgift att svara för bedömning av kompetensen hos laboratorier, certifieringsorgan och kontrollorgan. I Sverige har Styrelsen för ackreditering och teknisk kontroll, SWEDAC, denna uppgift.

Liksom SIS deltar i det internationella standardiseringsarbetet är SWEDAC engagerat i uppbyggnaden av de europeiska systemen för ömsesidigt godtagande av provning och kontroll samt i ut-

---

[3] Resolutionen den 21 december 1989 om en helhetssyn på bedömning av överensstämmelse (EGT C 10, 16.1.90, s.1). Se även beslutet den 13 december 1990 om moduler för olika stadier i förfaranden vid bedömning av överensstämmelse, avsedda att användas i tekniska harmoniseringsdirektiv (EGT L 380, 31.12.1990, s. 13).

[4] Med *ackreditering* menas ett formellt erkännande att ett organ (laboratorium, certifieringsorgan, besiktningsorgan etc.) är kompetent att utföra specificerade provningar, kalibreringar, mätningar, certifieringar etc.

formandet av enhetliga regler för bedömning av kompetens hos de organ som utför teknisk kontroll. Detta sker främst inom ramen för organisationen European Accreditation, EA. Inom EA finns multilaterala avtal om ömsesidigt erkännande av ackrediteringssystem och om erkännande av kompetens och därigenom av certifikat och system.

I Sverige har det beskrivna öppna systemet med anmälda organ genomförts genom lagen (1992:1119) och förordningen (1993:1065) om teknisk kontroll. Enligt dessa får både offentliga och enskilda organ som uppfyller kraven på kompetens utföra certifierings-, provnings- och besiktningsuppgifter och konkurrera om uppdragen. SWEDAC har till uppgift att i samråd med berörda sektorsmyndigheter bedöma om de organ som önskar bli anmälda uppfyller kraven. Som huvudregel gäller att organen skall kunna visa att de uppfyller kraven i EN 45 000-serien. Enligt lagen och förordningen om teknisk kontroll gäller dessutom som huvudprincip att kraven även för ackreditering av organ som utför annan kontroll, besiktning och certifiering än de som föreskrivs i EG-direktiven skall baseras på EN 45 000-serien.

Av särskilt intresse för denna promemoria är den provning och certifiering av produkter som sker frivilligt, utan att det krävs i EG-direktiv eller i nationella föreskrifter – det s.k. *frivilliga området*. Detta är vanligt och krav på produkter finns ofta formulerade i standarder mot vilka frivillig certifiering kan ske. Det är viktigt att påpeka att certifiering inte bara sker av produkter, utan också av kvalitetssystem, verksamheten i allmänhet, ledningssystem, personal etc.

Det är utan tvivel en fördel om det även inom det frivilliga området tillämpas likartade former för provning och certifiering. I EG:s system för bedömning av överensstämmelse har man också tagit fasta på att tekniken för att bedöma om en produkt överensstämmer med vissa uppställda krav är densamma oavsett om bedömningen sker utifrån tvingande regler eller frivilliga former. I sitt meddelande den 24 juni 1989 En helhetssyn på certifiering och provning markerade kommissionen att ömsesidiga erkännanden inte

bara är av intresse för den reglerade sektorn utan i lika hög grad har betydelse inom det frivilliga området. Även frivillig provning och certifiering kan, om den skiljer sig åt i olika länder, medföra betydande handelshinder. Problemen med att skapa ömsesidiga godtaganden är desamma inom de reglerade och frivilliga områdena, nämligen att skapa förtroende för att de berörda organen är kompetenta och oberoende.

4.5 Marknadsutvecklingen i Sverige

4.5.1 Svensk standard

Samarbetet mellan Riksförsäkringsverket, Riksskatteverket, Rikspolisstyrelsen och Försvarsmakten (beställare) samt Datainspektionen (kravställare) och Statskontoret (upphandlare för offentlig sektor) kring ”Allterminalen” kan sägas vara det första steget i utvecklingen av säkerhet för persondatorer. I det arbetet togs tekniska specifikationer fram för en s.k. moduluppbyggd säkerhetsmiljö för skydd av persondatorer. Till lösningen hör aktiva säkerhetskort, s.k. Allterminalkort (AT-kort) och särskilda kortläsare. De aktiva korten konfigureras med nycklar för de tre funktionerna identifiering, signering och kryptering för konfidentialitet. Kortet är således bärare av nycklar för unik elektronisk identitet, nycklar för elektronisk signering respektive stöd för kryptering.

Samarbetet i bank- och finanssektorn kring aktivt kort/elektroniskt identitetskort för kunder pågick i projektet ”Strategisk samverkan”. Syftet med projektet var att finna en gemensam teknisk lösning för ett elektroniskt identitetskort med vars hjälp det skulle bli möjligt att höja säkerhetsnivån i olika elektroniska tjänster. Specifikationerna för lösningen gjordes allmänt tillgängliga.

Våren 1995 bildades den ideella föreningen Säkrad Elektronisk Information i Samhället (SEIS). I SEIS togs erfarenheter från projekten Allterminalen och Strategisk samverkan tillvara samtidigt som ett fortsatt arbete initierades med syfte att främja utvecklingen av ett ramverk för allmänt accepterade, enkla, praktiska och ekonomiska säkerhetslösningar. Samtliga sektorer i samhället är

representerade i föreningen. I arbetet inom SEIS har bl.a. tekniska specifikationer för elektronisk identifiering, elektronisk signatur och stöd för kryptering på aktiva kort utvecklats.

Vissa specifikationer har överlämnats till Standardiseringen i Sverige (SIS). Sedan 1998 finns svensk standard för elektroniskt ID-kort med de tre grundfunktionerna identifiering, signering och stöd för kryptering för konfidentialitet.

SEIS har också tagit fram ett regelverk (S 10) för utfärdande av elektroniska identitetskort, aktiva kort, som till sitt utförande också överensstämmer med den relativt nyligen fastställda svenska standarden för vanliga visuella ID-kort.

”Spridnings- och hämtningssystemet” (SHS) är ett myndighetsgemensamt kommunikationssystem med målsättning att effektivisera informationsflödet inom och mellan myndigheter. Det definierar ett standardiserat sätt att transportera skilda typer av information. Dessutom ger systemet möjligheter att förenkla informationsutbytet för enskilda och företag med offentlig sektor. Det ger också tekniska möjligheter till en flexibel åtkomst av information över myndighetsgränserna.

SHS gör det möjligt att förse delar av informationen som transporteras i systemet med elektronisk signatur som skyddar informationen under överföringen. Detta är dock inte sådana signaturer som är avsedda att lagras i det mottagande systemet.

Gemenskapen för elektroniska affärer, GEA, bildades i januari 1999 av nio branschövergripande organisationer för att åstadkomma en kraftsamling i syfte att utveckla och befästa Sverige som elektronisk affärsnation. GEA:s huvuduppgifter är att:

- påverka utformningen av regelsystem och infrastruktur, nationellt och internationellt,
- stimulera elektroniska affärer och
- medverka i standardiseringsarbetet.

4.5.2 Befintliga system

Tullverket

Tullverket har lång erfarenhet av ”sigillering” av elektroniska dokument. Redan år 1991 började Tullverket ge företagen möjlighet att skicka in elektroniska (sigillerade) handlingar för import- och exportklarering. Sigillet är baserat på en symmetrisk algoritm och garanterar att dokumentets innehåll är intakt och att korrekt utställare identifieras. Systemet är utformat så att korten (innehållande användarens hemliga nyckel) utfärdas och administreras via ett centralt register inom Tullverket. Drygt 80 procent av klareringshandlingarna lämnas för närvarande elektroniskt, vilket innebär att det i dagsläget finns cirka 5 000 kort utfärdade, spridda på 500 företag.

För Tullverkets egna tjänstemän används en allterminal-lösning med tillhörande AT-kort. Tullverket utfärdar självt de certifikat som används. Huvudsakligen används systemet för identifiering vid inloggning, men i vissa fall används även krypteringsnycklar inlagda på korten för att skydda känslig information.

Riksförsäkringsverket

På socialförsäkringsområdet har Riksförsäkringsverket (RFV) sedan 1995 ansvarat för införande av Allterminalkonceptet. Totalt omfattas cirka 15 000 anställda hos RFV och försäkringskassorna. RFV är idag utgivare av AT-kort för det egna behovet. Under 1999 har en utveckling av konceptet mot en komplett PKI-lösning inletts, omfattande funktioner för identifiering av användare, elektronisk signering och kryptering för konfidentialitet. Tillämpningar med elektronisk signering är under utveckling och kommer att införas successivt med start under år 2000. Visionen för framtida socialförsäkringsadministration är att allmänheten kan erbjudas tjänster över Internet.

Riksskatteverket

Inom områdena folkbokföring, beskattning och utsökning använder samtliga cirka 14 000 tjänstemän inom Riksskatteverket (RSV) s.k. AT-kort. RSV är sin egen certifikatutfärdare och utfärdare av kort. Elektronisk signering av beslut används i förvaltningens nya skatte- och avgiftssystem ”Magi”. Detta innefattar också en egenutvecklad tidstämplingsfunktion. RSV planerar att byta ut AT-korten med anledning av att de inte har tillräcklig kapacitet för den PKI-struktur som är under införande i RSV.

RSV har tillsammans med Patent- och registreringsverket ett projekt som berör start av företag. Systemet kommer att använda Spridnings- och hämtningssystem (SHS). RSV har även önskemål om att förbättra rutinerna för att företagen skall kunna lämna skattedeklarationer elektroniskt. Uppgifter om firmatecknare och årsredovisningar, signerade av styrelsen är andra intressanta områden.

RSV är vidare certifikatutfärdare för ett antal ”kunder”, t.ex. informationsmottagare av folkbokföringsaviseringar. Detta föregås av att;

– RSV skriver ett avtal med kunden (normalt en annan myndighet, en kommun eller motsvarande),
– kunden genererar ett nyckelpar på sin web-läsare,
– kunden kopplar upp sig mot en av RSV:s öppna web-sidor, vilket sker genom att följa vissa säkerhetsåtgärder, t.ex. ett unikt lösenord som kunden får då avtalet ingås, och begär att RSV skapar ett certifikat innefattande kundens publika nyckel,
– RSV:s mottagarfunktion kontrollerar kundens uppgifter och skapar certifikatet som stämplas med RSV:s utfärdarnyckel och
– certifikatet återsänds till kunden.

Den fortsatta informationslämningen/hämtningen sker under skydd av kryptering och RSV:s certifikat.

Angående verksamheter hos *Rikspolisstyrelsen* och *Centrala studiestödsnämnden*, se Ds 1998:14.

Posten AB

Posten uppträder genom sitt affärsområde PostNet som publik certifikatutfärdare. PostNet har byggt vidare på Postens tradition som utgivare av traditionella visuella ID-kort. Identifiering, signering och kryptering för konfidentialitet är tre grundbehov vid elektroniska affärer eller andra kontakter över publika nät, t.ex. Internet. PostNet har skapat en säkerhetsplattform för dessa behov.

I dag är PostNet certifikatutfärdare för isolerade grupper. Avsikten är att när elektroniska ID-kort har nått en större spridning kunna agera som en publik certifikatutfärdare och ge service till allmänheten.

Telia AB

Telia har i sitt utbud tjänsten ”Telia Elektronisk Identifiering”, ett koncept för säker elektronisk identifiering och säker elektronisk kommunikation. Telia står därvid för utgivning, produktion, administration och kontroll av elektroniska identiteter.

Telias elektroniska ID-handlingar används idag i tillämpningar som avser att skapa säkra och trygga elektroniska relationer och transaktioner vad gäller identifiering, signering och kryptering.

Telia driver även IT-projekt inom den offentliga och den privata sektorn.

Försvarsmakten

Inom delar av Totalförsvaret används ”Totalförsvarets Aktiva Kort” (TAK). Kortet togs i drift under 1996 och används framför allt för identifiering i ett antal datorsystem med höga säkerhetskrav och som bärare av kryptonycklar till hårdvarukrypto för skydd av hemliga uppgifter. Användningen av elektroniska signaturer är i dagsläget mycket begränsad, men förväntas öka i framtiden. Kortet får användas endast med godkänd programvara i godkänd kortläsare. Totalförsvarets Signalskyddssamordning (TSA)

fungerar som ansvarig kortutgivare och certifikatutfärdare för Totalförsvaret. Ett projekt för att ta fram nästa generation av kort med längre nycklar och större minneskapacitet har nyligen påbörjats. Där studeras även möjligheten att följa svensk standard för elektroniska ID-kort, i första hand avseende certifikathantering.

Kommuner

Elektroniska signaturer används idag endast i mindre omfattning i kommunerna. Ett ramavtal som Statskontoret träffat med Posten AB och Telia AB våren 1999 har dock visat sig ha positiv effekt. Ett 30-tal kommuner har visat intresse för försöksverksamhet med elektroniska signaturer.

Som exempel på större pilotprojekt kan nämnas STEHLA-projektet som för närvarande bedrivs i Stockholms stad. Det är ett projekt för att stimulera elektronisk handel där man bl.a. använder elektronisk signatur vid beställning av varor och för attest av fakturor. Signaturen används inte gentemot leverantörer utan i den interna administrationen i Stockholms stad. Den elektroniska signaturen ger internrevisionen möjlighet att kontrollera att behörig tjänsteman beställt varor, attesterat fakturor m.m. Telia AB är certifikatutfärdare.

Stadsbyggnadskontoret i Stockholms stad (SBK) har ett pilotprojekt som går ut på att regelbundna och obligatoriska ventilationsprotokoll från Stockholmshem kan överföras elektroniskt och signerade till SBK. I verksamheten används elektroniska ID-kort enligt svensk standard. Korten levereras av Posten AB, som också står för säkerhetsplattformen.

SBK har förhoppningar om att i närtid utveckla denna service även till andra ärendetyper såsom ansökningar om bygglov m.m., varvid elektronisk signatur kommer att användas både av sökande och beslutsfattare i SBK.

Stockholms stad har också beslutat att starta ett antal pilotprojekt med elektroniskt ID-kort, varav några innefattar elektronisk

signatur. Projektområdena är bl.a. socialtjänstsystemet och ansökningar om utskänkningstillstånd.

Även i mindre kommuner har försöksverksamhet påbörjats med elektroniska signaturer. Det gäller såväl användning av elektroniska signaturer i samband med expediering av fattade beslut som vid elektronisk handel.

Från Svenska Kommunförbundets sida har ett fortlöpande arbete skett i syfte att påskynda användningen av elektroniska signaturer bl.a. med anknytning till elektronisk handel.

Landsting, hälso- och sjukvård

Arbete i och samarbete mellan landsting angående användning av elektroniska signaturer inom sjukvården och för elektronisk handel har diskuterats i Ds 1998:14. Här kan tilläggas att en modell har utarbetats för hur en infrastruktur med öppna nycklar (Publik Key Infrastructure, PKI) kan byggas i hälso- och sjukvården.

Vidare pågår inom ramen för EU-projektet Trust Health 2 tester av olika modeller för hur integritetskänslig vårdinformation skyddas med systemlösningar byggda på PKI-teknik och aktiva kort. Både lokala installationer inom sjukvårdsorganisationer i de sex deltagarländerna och elektronisk överföring mellan länderna testas. I Sverige testas bl.a. metoder för elektronisk signering med hjälp av aktiva kort konfigurerade enligt svensk standard och levererade av Posten AB och Telia AB.

Region Skåne har tagit beslut om en modell för säker meddelandehantering som inkluderar elektronisk signatur beträffande signering av journaler. Värmlands läns landsting driver ett försök med 20 användare med aktiva kort, stark kryptering och elektroniska signaturer. Även inom ”FYRNET” och ”SJUNET” – ett samarbete mellan ett antal landsting i Nord- och Mellansverige – planeras respektive pågår olika försök med elektroniska ID-kort för säker elektronisk informationsöverföring.

Bank- och finanssektorn

I samarbete med fyra stora banker har Bankgirocentralen utvecklat en lösning för säkra elektroniska betalningar med elektroniska ID-kort att användas mellan företagens ekonomisystem och bankgirosystemet. Säkerhetsfunktionerna består av säker elektronisk identifiering, elektronisk signatur och stöd för kryptering för konfidentialitet enligt svensk standard. Vid slutet av 1999 kommer ca 1 000 licenser att vara utfärdade, vilket innebär att ca 1 000 företagskunder anslutit sig och att ett par tusen anställda i företagen har försetts med elektroniska ID-kort. Bankgirot utvecklar även informationstjänster med elektroniskt ID-kort som säkerhetsattribut.

Flera banker erbjuder sina tjänster över Internet där elektroniska signaturer används. Bankerna utfärdar än så länge själva certifikat och aktiva kort i slutna system. Svenska Handelsbanken har dock valt en annan lösning än användning av elektroniska ID-kort (se Ds 1998:14). Det pågår vidare ett arbete med att skapa en för bankerna gemensam lösning, baserad på elektroniska ID-kort enligt SEIS S10.

SET (Secure Electronic Transaction) är en teknisk specifikation utarbetad i syfte att skapa förutsättningar för betalning med kredit/betalkort över Internet med utnyttjande av befintlig konto-kortsinfrastruktur. SET beskrivs närmare i Ds 1998:14.

5 Direktivet om ett gemenskapsramverk för elektroniska signaturer

5.1 Allmänt

Anledningen till att EG-kommissionen lade fram ett förslag till direktiv var bl.a. att den befarade att skilda juridiska och tekniska strategier i medlemsstaterna beträffande elektroniska signaturer skulle utgöra ett allvarligt hinder för den inre marknaden och hindra utvecklingen av nya ekonomiska verksamheter som är kopplade till elektronisk handel. Olika bestämmelser i medlemsstaterna om rättsligt erkännande av elektroniska signaturer och om auktorisering av dem som tillhandahåller certifikat för elektroniska signaturer skulle skapa betydande sådana hinder.

Syftet med direktivet är att underlätta användningen av elektroniska signaturer och bidra till deras rättsliga erkännande. Avsikten är att fastställa ett rättsligt ramverk för elektroniska signaturer och vissa certifikattjänster för att säkerställa en väl fungerande inre marknad. Direktivet omfattar inte frågor om ingående eller giltighet av avtal om formkrav föreskrivs och påverkar inte heller bestämmelser som reglerar användningen av dokument (*artikel 1*). Regelverket för elektroniska signaturer är avsett att stärka förtroendet för och ge ett allmänt godtagande av den nya tekniken.

I direktivet definieras signaturer som uppfyller vissa specificerade krav som *avancerade elektroniska signaturer*. Ett intyg i elektronisk form som kopplar ihop en person med uppgifter, såsom koder eller öppna kryptografiska nycklar, som verifierar en signatur

samt bekräftar personens identitet kallas *certifikat*. Den tredje part som utfärdar certifikatet och som således går i god för att den uppgivne undertecknaren verkligen är den som påstås kallas *tillhandahållare av certifikattjänster*. Ett certifikat som innehåller i en bilaga uppräknade uppgifter och som utfärdats av en tillhandahållare av certifikattjänster som uppfyller kraven i en annan bilaga benämns *kvalificerat certifikat*. Dessa och flera andra definitioner ges i *artikel 2*.

Den metod som används i direktivet är att ge avancerade elektroniska signaturer, som baseras på ett kvalificerat certifikat och som dessutom skapas av en ”säker anordning för skapande av signaturer” (se nedan), en viss rättsverkan. Dessa signaturer skall anses uppfylla kraven på en signatur i förhållande till uppgifter i elektronisk form på samma sätt som en handskriven signatur uppfyller samma krav i förhållande till uppgifter på papper och skall godtas som bevis vid rättsliga förfaranden. Vidare stadgas att andra elektroniska signaturer inte får förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden (*artikel 5*).

Villkoren för marknadstillträde för tillhandahållare av certifikattjänster och den tillsyn som skall ske regleras i *artikel 3*. Fri rörlighet för certifikattjänster behandlas i *artikel 4* och skadestånd i *artikel 6*. I *artikel 7* regleras behandlingen av certifikat utfärdade i länder utanför gemenskapen, medan *artikel 8* behandlar frågor om dataskydd. I övrigt ges regler om den kommitté för elektroniska signaturer som skall biträda kommissionen (*artikel 9 och 10*), om uppgifter som skall anmälas till kommissionen (*artikel 11*), om en översyn av direktivet tre och ett halvt år efter dess ikraftträdande (*artikel 12*) samt om genomförande och ikraftträdande (*artikel 13–15*).

Målsättningar vid direktivets utformande kan i stort sägas vara att inte låsa sig vid en viss teknik, att det inte får förekomma något krav på förhandstillstånd för att uppträda som tillhandahållare av certifikattjänster samt att säkerställa att elektroniska signaturer får rättslig verkan.

5.2 Tillämpningsområde

Av ingressen till direktivet och av definitionen av tillhandahållare av certifikattjänster framgår att dessa inte bör vara begränsade till att endast utfärda och hantera certifikat. Även andra tjänster som har anknytning till elektroniska signaturer bör kunna erbjudas, såsom registrerings-, tidsstämplings-, katalog-, databehandlings- eller konsulttjänster. För tillhandahållare av certifikattjänster och för produkter med anknytning till elektroniska signaturer föreskriver direktivet en fri inre marknad, och detta gäller för alla sorters elektroniska signaturer, certifikattjänster och ”signaturprodukter”. Beträffande rättsverkan för elektroniska signaturer har dock direktivet ett smalare tillämpningsområde. Det omfattar inte frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser om den nationella lagstiftningen eller gemenskapslagstiftningen föreskriver vissa formkrav. Det påverkar heller inte bestämmelser och begränsningar i nationell lagstiftning eller gemenskapslagstiftning som reglerar användningen av dokument. Vidare ges endast elektroniska signaturer som uppfyller vissa krav (avancerade elektroniska signaturer) samma status som handskrivna signaturer. Slutligen framgår i ingressen att elektroniska signaturer som endast används inom system, vilka grundar sig på frivilliga civilrättsliga avtal mellan ett bestämt antal deltagare, inte faller under direktivet, även om också sådana signaturer kan dra nytta av reglerna om rättsverkan. Parternas frihet att sinsemellan komma överens om på vilka villkor de godkänner elektroniskt signerade uppgifter kvarstår (i den omfattning det är förenligt med nationell lag).

5.3 Definitioner

En *elektronisk signatur* definieras som uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska uppgifter och som används som metod för autenticering.

För att en signatur skall få kallas *avancerad elektronisk signatur* krävs att den är knuten uteslutande till undertecknaren, vilken kan identifieras genom signaturen, att den är skapad med medel som undertecknaren kan behålla uteslutande under sin egen kontroll samt att den är kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Genom direktivet införs vidare en rad tekniska termer, t.ex. *uppgifter för skapande av signaturer* som avser unika uppgifter såsom koder eller kryperingsnycklar som används för att skapa en signatur och *uppgifter för signaturverifiering*, som avser uppgifter för att verifiera en elektronisk signatur. Program- eller hårdvara för att använda uppgifterna för att skapa en signatur respektive uppgifterna för signaturverifiering benämns *anordning för skapande av signaturer* respektive *anordning för signaturverifiering*.

För att få kallas *säker anordning för skapande av signaturer* skall anordningen uppfylla de krav som anges i bilaga III till direktivet. Anordningarna skall enligt denna säkerställa att uppgifterna för att skapa signaturen praktiskt taget enbart kan förekomma en gång och att sekretessen för uppgifterna är säkerställd inom rimliga gränser. Vidare skall uppgifterna för att skapa signaturen ”med rimlig garanti” inte kunna härledas och signaturen vara skyddad mot förfalskning ”med den teknik som för närvarande finns tillgänglig”. Ett ytterligare krav är att uppgifterna för att skapa signaturen kan skyddas på ett tillförlitligt sätt så att andra inte kan komma åt dem. Slutligen stadgas att anordningen inte får förändra de uppgifter som skall signeras eller hindra att dessa uppgifter presenteras för undertecknaren före undertecknandet.

Beträffande signaturverifiering finns en bilaga IV till direktivet, som innehåller rekommendationer för säker signaturverifiering.

Tillhandahållare av certifikattjänster definieras som nämnts inte endast som den som utfärdar certifikat, utan även den som tillhandahåller andra tjänster som har anknytning till elektroniska signaturer.

Kvalificerade certifikat

Kvalificerade certifikat är sådana certifikat som uppfyller kraven i direktivets bilaga I och som utfärdas av en tillhandahållare av certifikattjänster som uppfyller kraven i direktivets bilaga II. Certifikatet skall bl.a. innehålla uppgift om att det har utfärdats som ett kvalificerat certifikat, uppgifterna för signaturverifiering som motsvarar de uppgifter för skapande av signaturer som undertecknaren har kontroll över samt angivande av giltighetstidens början och slut för certifikatet (se vidare i bilagan).

Bilaga II innehåller krav på pålitlighet, ett säkert och snabbt system för omedelbart återkallande, identitetskontroll av den till vilken ett certifikat utfärdas, kompetent personal, användandet av pålitliga system och produkter som garanterar teknisk säkerhet, konfidentialitet beträffande uppgifter för skapande av signaturer m.m. (se vidare i bilagan).

Certifikatutfärdaren skall dessutom förfoga över tillräckliga ekonomiska medel för att bedriva verksamheten i enlighet med kraven enligt direktivet, i synnerhet för att kunna bära risken för skadeståndsskyldighet. De certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten har nämligen det skadeståndsansvar som stadgas i artikel 6.

Nämnas kan också att utfärdaren enligt bilagan måste informera den som ansöker om ett certifikat om villkoren, inklusive eventuella begränsningar för certifikatet, förekomsten av ett frivilligt ackrediteringssystem samt förfarande för klagomål och avgörande av tvister. Vidare är utfärdaren förbjuden att lagra eller kopiera uppgifter för skapande av signaturer.

5.4 Marknadstillträde

Medlemsstaterna får inte göra tillhandahållandet av certifikattjänster beroende av förhandstillstånd. Med förhandstillstånd menas enligt ingressen till direktivet inte endast alla tillstånd som kräver ett beslut från de nationella myndigheterna innan tillhanda-

hållaren av certifikattjänster får tillhandahålla dessa tjänster, utan också alla andra åtgärder med samma verkan.

Det står dock medlemsstaterna fritt att införa eller behålla frivilliga ackrediteringssystem som syftar till att höja nivån på tillhandahållandet av certifikattjänster. *Frivillig ackreditering* definieras i direktivet som sådana tillstånd i vilka de rättigheter och skyldigheter fastställs som är specifika för tillhandahållandet av certifikattjänster och som på begäran av den berörda tillhandahållaren av certifikattjänster skall utfärdas av de offentliga eller privata institutioner som ansvarar för utarbetandet och övervakningen av dessa rättigheter och skyldigheter, då tillhandahållaren av certifikattjänster inte får utöva rättigheterna enligt tillståndet förrän denne har erhållit beslutet från institutionen.

Medlemsstaterna är skyldiga att införa ett system som gör det möjligt att övervaka de tillhandahållare av certifikattjänster som är etablerade på deras territorium och som utfärdar kvalificerade certifikat till allmänheten. I direktivet ges inga närmare regler för hur denna övervakning skall vara organiserad eller hur sträng den skall vara. I ingressen påpekas att övervakningssystem baserade inom den privata sektorn inte utesluts.

Vad gäller säkra anordningar för skapande av signaturer föreskriver direktivet att medlemsstaterna skall utse särskilda organ som skall avgöra om anordningarna översensstämmer med bilaga III.

I direktivet ges en möjlighet för medlemsstaterna att förena användningen av elektroniska signaturer inom den offentliga sektorn med högre krav än vad som följer av direktivet.

5.5 Fri rörlighet

Medlemsstaterna får inte begränsa tillhandahållandet av certifikattjänster med ursprung i andra medlemsstater. De skall också säkerställa att produkter för elektroniska signaturer som överensstämmer med direktivet har fri rörlighet på den inre marknaden

Ett beslut av ett organ i en medlemsstat att en anordning för skapande av signaturer överensstämmer med kraven i bilaga III skall erkännas av samtliga medlemsstater. Kommissionen får fastställa och offentliggöra referensnummer till allmänt erkända standarder för produkter för elektroniska signaturer. Medlemsstaterna skall då utgå från att dessa produkter överensstämmer med kraven i direktivet.

5.6 Rättslig verkan

Den rättsliga verkan man vill ge avancerade elektroniska signaturer som baseras på ett kvalificerat certifikat och som skapas av en säker anordning för skapande av signaturer har beskrivits ovan.

För övriga elektroniska signaturer gäller att dessa inte får förvägras rättslig verkan eller giltighet som bevis enbart på grund av att signaturen är i elektronisk form, inte är baserad på ett kvalificerat certifikat eller ett certifikat som utfärdats av en ackrediterad tillhandahållare av certifikattjänster, eller inte är skapad av en säker anordning.

I ingressen anges att direktivet inte påverkar nationella domstolars behörighet att fastslå om det föreligger överensstämmelse med kraven i direktivet. Vidare sägs att direktivet inte inverkar på nationella bestämmelser om fri bevisprövning.

Det finns således två nivåer av rättsligt erkännande av signaturer, beroende på den tekniska säkerhet som signaturen anses ha. Dels elektroniska signaturer i allmänhet, som inte får förvägras rättslig verkan, dels kvalificerade elektroniska signaturer, som ges samma erkännande som en handskriven underskrift på papper.

5.7 Skadestånd

Direktivet fastställer en undre gräns för skadeståndsskyldighet för tillhandahållare av certifikattjänster. Regleringen avser dock bara

dem som utfärdar eller garanterar (se nedan under ”Internationella förhållanden”) certifikat som kvalificerade certifikat till allmänheten. Medlemsstaterna skall se till att tillhandahållaren är ansvarig för skada som orsakas den som har rimlig anledning att förlita sig på ett certifikat. Tillhandahållaren skall, om han inte kan visa att han inte handlat försumligt, ansvara för felaktigheter och brister i den information som ges i ett kvalificerat certifikat, att den undertecknare som anges i certifikatet inte är i besittning av de uppgifter för att skapa en signatur som påstås, att uppgifter för signaturskapande respektive verifiering inte stämmer överens samt underlåtenhet att registrera återkallandet av ett certifikat.

Tillhandahållare av certifikattjänster skall dock kunna ange begränsningar i ett certifikats tillämpningsområde eller för värdet av transaktioner som certifikatet får användas för. Tillhandahållaren är då inte ansvarig för skador som härrör från att ett certifikat använts i strid med dessa begränsningar, under förutsättning att begränsningarna varit identifierbara för tredje man.

5.8 Internationella aspekter

Kvalificerade certifikat som utfärdats av en tillhandahållare av certifikattjänster som är etablerad utanför Europeiska unionen skall enligt direktivet i tre situationer betraktas som rättsligt likvärdiga med kvalificerade certifikat utfärdade inom unionen: Då tillhandahållaren i tredje land uppfyller kraven i direktivet och är ackrediterad i en medlemsstat; då en tillhandahållare inom gemenskapen som utfärdar kvalificerade certifikat och uppfyller kraven i direktivet garanterar certifikatet; eller då certifikatet eller tillhandahållaren är erkänd genom ett bilateralt eller multilateralt avtal mellan gemenskapen och tredje land eller internationella organisationer.

Direktivet föreskriver också som uppgift för kommissionen att lägga förslag till genomförande av standarder och internationella avtal som underlättar gränsöverskridande certifikattjänster och rättsligt erkännande av signaturer med ursprung i tredje land.

5.9 Dataskydd

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 är tillämpliga på tillhandahållare av certifikattjänster och på nationella organ med ansvar för ackreditering och övervakning.

Tillhandahållare av certifikattjänster som utfärdar certifikat till allmänheten får endast samla in uppgifter direkt från den berörda personen eller med dennes uttryckliga medgivande och endast för att utfärda och bibehålla certifikatet. Uppgifterna får inte samlas in eller behandlas för andra ändamål utan ett uttryckligt medgivande från den berörde personen. Vidare får medlemsstaterna inte hindra tillhandahållare av certifikattjänster att ange en pseudonym i stället för undertecknarens namn.

5.10 Kommitté

En rådgivande kommitté, bestående av företrädare för medlemsstaterna och under ordförandeskap av en representant för kommissionen, skall konsulteras för att klargöra kraven i direktivets bilagor, kriterierna för utseende av de organ som skall avgöra om säkra anordningar för skapande av signaturer överensstämmer med kraven i bilaga III samt beträffande de allmänt erkända standarder för produkter för elektroniska signaturer som kommissionen skall fastställa och offentliggöra.

Kommissionens beslut i dessa frågor skall, sedan kommittén rådfrågats, ha omedelbar verkan. Om kommissionens beslut inte är förenligt med kommitténs yttrande skall rådet underrättas och kommissionen skjuta upp verkställandet av sitt beslut i tre månader. Under den tiden kan rådet med kvalificerad majoritet fatta ett annat beslut än kommissionens.

5.11 Anmälan, genomförande och översyn

Medlemsstaterna skall informera varandra och kommissionen om ackrediteringssystem som tillämpas, namn på de organ som svarar för ackreditering, övervakning och som avgör om anordningar för signaturskapande överensstämmer med direktivets krav samt namn på samtliga ackrediterade tillhandahållare av certifikattjänster.

De nationella bestämmelser som behövs för att följa direktivet skall vara i kraft senast ett och ett halvt år efter det att direktivet trätt i kraft, vilket sker samma dag som det offentliggörs i Europeiska gemenskapernas officiella tidning.

Kommissionen skall göra en översyn av direktivet och överlämna en rapport om denna senast tre och ett halvt år efter det att direktivet trätt i kraft.

6 Genomförande av direktivet

Det kan med fog ifrågasättas om det är lämpligt att redan nu reglera en marknad som ännu inte vuxit fram i nämnvärd omfattning. Ett bättre alternativ vore kanske att avvakta att elektroniska signaturer börjar användas i större utsträckning (se dock diskussionen i avsnitt 9). Antingen kan då konstateras att marknaden klarar sig utan lagreglering eller identifieras problem vars lösning kräver lagstiftning. Förutsättningarna för att utforma lagstiftningen på ett ändamålsenligt sätt är då betydligt större.

Den stora fördelen med direktivet är dock att det innebär en gemensam reglering för medlemsstaterna i den Europeiska unionen och övriga länder inom det Europeiska ekonomiska samarbetsområdet. Den utveckling som hade påbörjats, att regleringen av elektronisk kommunikation blir olika i varje land, har avstyrts.

Vid det svenska genomförandet av direktivet finns det dock anledning att vara försiktig med att reglera ett bredare område än vad direktivet kräver. Det kan finnas skäl, t.ex. vad gäller skadestånd, att även reglera sådant som inte krävs enligt direktivet. I denna promemoria föreslås dock inte någon sådan reglering, utan påpekas endast att utvecklingen kan göra det nödvändigt att i framtiden komplettera lagstiftningen.

6.1 En ny lag

Förslag: Direktivet skall genomföras genom en särskild lag, lagen om vissa elektroniska signaturer m.m.

Enligt artikel 251 i EG-fördraget är ett direktiv bindande för medlemsstaterna vad avser det resultat som skall uppnås. Det överlåts dock åt de nationella myndigheterna att bestämma form och tillvägagångssätt för genomförandet.

Ett genomförande av direktivet innebär införande av ett tämligen stort antal nya, främst näringsrättsliga, regler. Telelagen (1993:957) innehåller visserligen närliggande regler om förmedling av telemeddelanden via telenät. Det som direktivet reglerar, elektroniska signaturer och framför allt krav på dem som utfärdar certifikat för sådana signaturer, utgör dock en ny företeelse och söker reglera en helt ny marknad som inte rör televerksamhet i telelagens mening. På samma sätt finns kopplingar till regleringen av den finansiella sektorn, men direktivet rör ett mycket vidare område än den sektorn.

I andra sammanhang har det ansetts naturligt att föreslå ett införande i förvaltningslagen (1986:323) av definitioner och allmänna regler för elektroniska signaturer. Detta kan visserligen mycket väl vara lämpligt, men förvaltningslagen är av lätt insedda skäl inte rätt plats för att införa det främst näringsrättsliga regelverk det här är fråga om.

Den lämpligaste sättet att genomföra direktivets regler synes vara genom en ny särskild lag. Denna kommer visserligen att handla mer om certifikat för elektroniska signaturer och krav på dem som utfärdar sådana certifikat, än om elektroniska signaturer i sig. Trots detta föreslås lagen heta ”lag om vissa elektroniska signaturer m.m.”, eftersom detta är ett hanterligt kort namn på lagen, samtidigt som det ger en tillräckligt tydlig bild av lagens innehåll.

Med hänsyn till direktivets karaktär blir det ofrånkomligt att delar av direktivet mer eller mindre ordagrant måste tas in i lagen.

6.2 Lagens syfte och tillämpningsområde

Förslag: Lagen skall innehålla regler om krav på, tillsyn över och skadeståndsansvar för den som utfärdar certifikat för elektroniska signaturer, om certifikaten anges ha en viss säkerhetsnivå. Lagen skall vidare ge en särställning åt elektroniska signaturer med en viss säkerhetsnivå. Lagen skall inte innehålla regler om tillsyn och skadeståndsansvar vad gäller certifikat som inte utfärdas till allmänheten och inte heller reglera frågor om ingående eller giltighet av avtal.

Handel och annan kommunikation mellan enskilda, myndigheter och företag kan förväntas ske elektroniskt i ökad utsträckning om det finns ett allmänt förtroende för att den information som skickas via Internet och andra öppna nät är tillförlitlig. Avsikten är att lagen skall bidra till detta genom att den främjar användandet av elektroniska signaturer som har en sådan säkerhetsnivå att de får ett allmänt erkännande och därmed kan användas för säker kommunikation, även mellan parter som inte har ett tidigare avtal om hur deras inbördes kommunikation skall gå till.

I direktivet läggs stor vikt vid resonemanget om elektroniska signaturers rättsliga verkan. För Sveriges del, där principerna om den fria bevisprövningen och den fria bevisvärderingen är etablerade sedan länge, intar denna fråga inte en central roll vad gäller lagstiftningen. Vad som kommer i fokus är i stället vilka regler som skall gälla för dem som vill tillhandahålla certifikattjänster, såsom på vilka villkor sådan verksamhet får bedrivas, om, och i så fall hur, de ska övervakas, vilket ansvar de har, etc. Målsättningen bör vara att bygga upp ett system som inte i onödan lägger en hämsko på marknadens utveckling, t.ex. genom att låsa fast användning av en viss teknik, eller skapar etableringshinder. Samtidigt skall systemet vara uppbyggt på ett sådant sätt att det långsiktigt skapas en tilltro till det hos konsumenter, näringsidkare och andra användare. Detta underlättar att elektroniska signaturer används i

större omfattning, vilket sannolikt kommer att stimulera den elektroniska handeln liksom en rationalisering av förvaltningsväsendet baserad på elektroniska rutiner.

I lagen ges en säkerhetsnivå för vissa certifikat för elektroniska signaturer (”kvalificerade certifikat”) och ställs krav på dem som vill utfärda sådana certifikat. De som utfärdar sådana certifikat till allmänheten ställs under viss tillsyn och skadeståndsansvaret fastställs. Kraven och tillsynen gäller certifikatutfärdare som är etablerade i Sverige. Avsikten är däremot inte att i lagen reglera alla tjänster rörande elektroniska signaturer. Det kommer även efter lagens ikraftträdande vara möjligt att utfärda certifikat för elektroniska signaturer utan att underkasta sig tillsyn eller ackreditering eller vara tvungen att nyttja sig av viss bestämd teknik.

De som väljer att beteckna de certifikat de utfärdar som kvalificerade certifikat, väljer således också att omfattas av den ordning som föreskrivs i lagen (jfr. dock avsnitt 6.10). Lagen syftar till att möjliggöra att det på marknaden finns produkter och tjänster som uppfyller vissa minimikrav, som är gemensamma för länderna i det Europeiska ekonomiska samarbetsområdet.

Vad gäller uppfyllandet av formkrav på underskrift ges i lagen en särställning åt elektroniska signaturer som har en viss säkerhetsnivå (”kvalificerade elektroniska signaturer”).

Lagen reglerar inte frågor om ingående eller giltighet av avtal.

6.3 Definitioner

Förslag: Direktivets definitioner skall i allt väsentligt också anges i lagen.

Den tekniska utvecklingen och ersättandet av traditionella pappershandlingar med elektroniska data reser en mängd frågor om, och i så fall hur, denna företeelse kräver en annan rättslig reglering än den existerande. Dessa frågor har behandlats i flera utredningar och i vissa fall lett till lagstiftning. Användningen av s.k. elektroniska dokument regleras i ett trettiotal svenska författningar.

Som exempel kan nämnas tullagstiftningen, enligt vilken Tullverket kan ge tillstånd till att bl.a. tulldeklarationer får lämnas genom ett elektroniskt dokument[5]. Ett elektroniskt dokument definieras där som en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande. Sådana elektroniska dokument kan också, efter särskilt medgivande, i viss omfattning användas inom skatteområdet och exekutionsväsendet samt för vissa ansökningar gällande registrering av datapantbrev[6].

Riksdagen har ett flertal gånger efterlyst en mer generell reglering av elektroniska dokument i förvaltningsförfarandet. För att underlätta en sådan har i betänkandet Elektronisk dokumenthantering (SOU 1996:40) föreslagits att det i förvaltningslagen (1986:223) införs vissa grundläggande begrepp. ”Elektronisk handling” föreslås där definieras som en bestämd mängd data som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. Vidare föreslås (i kontrast mot det i befintlig lagstiftning använda ”elektroniskt dokument”) begreppet ”digitalt dokument”, som anges vara en elektronisk handling med digital signatur eller digital stämpel. Digital signatur definieras som resultatet av en omvandling av en elektronisk handling som gör det möjligt att kontrollera om innehållet härrör från den fysiska person som framstår som utställare. ”Digital stämpel” skulle på samma sätt härröra från en juridisk person eller myndighet. Betänkandet har inte lett till någon lagstiftning i denna del.

Sverige är visserligen inte bundet av den terminologi och systematik som angivits i direktivet, om det avsedda resultatet kan uppnås med annan terminologi och systematik. Direktivet är emellertid så utformat att möjligheten att avvika från terminologin är begränsad.

En strävan är givetvis att lagtexten skall vara så enkel och lättförstådd som möjligt. Den tämligen komplicerade verklighet som

---

[5] 12 § tullagen (1994:1550).

[6] Se t.ex. 2 § lagen (1990:325) om självdeklaration och kontrolluppgifter, 2 a § indrivningsförordningen (1993:1229) och 17 § lagen (1994:448) om pantbrevsregister.

direktivet beskriver kräver dock en begreppsapparat som, för att kunna fungera, inte kan förenklas för mycket. Det mål som angetts, att direktivet skall vara teknikneutralt, gör inte uppgiften lättare.

En annan strävan är att i möjligaste mån anknyta till den begreppsbildning som redan existerar i Sverige. En tredje är att åtminstone de nordiska länderna får en så enhetlig reglering som möjligt.

Den definition som föreslagits i det ovan nämnda betänkandet av ”elektronisk handling” skulle kunna ge en god grund att utgå från. Begreppet torde inte stå i konflikt med de ”elektroniska dokument” som redan används i ett antal författningar. Om begreppet införs bör det, såsom utredaren angivit, inte definieras på ett sådant sätt att det täcker mer än begreppet ”upptagning” i 2 kap. 3 § tryckfrihetslagen. Till skillnad från utredarens förslag föreslås dock här en begränsning till data *i digital form*, för att utesluta mikrofilm, ljudband, videoband etc. Detta kan å andra sidan innebära en viss teknikbundenhet och det kan hävdas att ett införande av begreppet skapar fler problem än det löser. Det är därför inte självklart att ”elektronisk handling” skall användas i lagen. Det skulle visserligen skapa ett begrepp som kan vara praktiskt att använda i andra sammanhang, men i denna lagtext används det endast, men är inte nödvändigt, för att definiera ”elektronisk signatur”.

Till skillnad från direktivet används i promemorian och i den föreslagna lagtexten ordet ”data” i stället för ”uppgifter”, då det mindre är fråga om ”uppgifter” i betydelsen ”information” som skall förstås av så många som möjligt, än om konstellationer av ettor och nollor som ofta inte i sig ger ett mänskligt öga särskilt mycket omedelbar information. Det är dessutom ofta önskvärt att hemlighålla dessa data. (Jämför Datastraffrättsutredningens (SOU 1992:110) definition av ”data” som en representation av fakta och av ”information” som innebörden av data.)

Definitionerna i direktivet har som nämnts utformats i avsikt att vara teknikneutrala. Den teknik som f.n. är förhärskande, där man använder digitala signaturer med ett certifikat som intygar kopplingen mellan en öppen nyckel och en bestämd person (det öppna

nyckelsystemet), har dock legat till grund för den struktur som valts i direktivet.

En elektronisk signatur bör i lagen definieras på samma sätt som i direktivet, men med användning av det introducerade begreppet elektronisk handling. (Om man väljer att inte införa begreppet elektronisk handling kan elektronisk signatur definieras i enlighet med direktivet, dvs. som data i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska data etc.) Detta torde innebära att alla elektroniska ”identifieringar” som är logiskt knutna till ett elektroniskt meddelande omfattas; från biometriska identifieringsmetoder till enkla engångskoder.

Definitionerna av ”avancerad elektronisk signatur”, och ”certifikat” kan lämpligen tas direkt från direktivet.

”Uppgifter för skapande av signaturer” (”den privata nyckeln” i det öppna nyckelsystemet) och ”uppgifter för signaturverifiering” (den öppna nyckeln) föreslås ersättas med ”signaturframställningsdata”, respektive ”signaturverifieringsdata”. Dessa begrepp är visserligen varken korta eller särskilt lättbegripliga vid första anblicken. De är dock i överensstämmelse med vad som föreslås i andra nordiska länder och ger en god bild av vad som avses. Användandet av ordet ”data” i stället för ”uppgifter” torde bidra till en bättre beskrivning av företeelserna.

En ”undertecknare” är den som utpekas i certifikatet och som har kontroll över en anordning för signaturframställning och signaturframställningsdata. Det saknas behov av att införa begreppet ”digital stämpel” eller liknande, som diskuterats ovan. Direktivet förutsätter att en fysisk person är knuten till signaturen. Det hindrar visserligen inte ett system med elektroniska stämplar för juridiska personer eller certifikat som anger att signaturen innehas av en identifierad person som är behörig firmatecknare för en juridisk person (”rollcertifikat”). Något särskilt behov av att reglera detta synes emellertid inte finnas. I stället kan vanliga regler om rättshandlingsförmåga, fullmakt och behörighet att företräda juridiska personer gälla.

”Anordning för skapande av signaturer” kan definieras såsom det angetts i direktivet, med de ändringar som följer av det föregående. ”Anordning för signaturverifiering” kommer inte att regleras i lagen varför det saknas skäl att införa begreppet.

Direktivet använder sig av begreppet ”tillhandahållare av certifikattjänster” och inbegriper där inte bara de som utfärdar certifikat utan också de som tillhandahåller andra tjänster som har anknytning till elektroniska signaturer. Det som direktivet syftar till att reglera är i praktiken dock huvudsakligen begränsat till utfärdande av certifikat. Exempelvis rör kraven i direktivets bilaga II endast tillhandahållare av certifikattjänster vilka utfärdar kvalificerade certifikat. Det finns därför inte behov av att i lagen skapa en definition som omfattar mer än de som utfärdar certifikat, lämpligast genom termen ”certifikatutfärdare”. I den mån man här eller i annat sammanhang önskar reglera annat än själva utfärdandet av certifikatet (registrering av återkallande, garanterande av annans certifikat, tidstämpling, kryptering för konfidentialitet, diverse konsulttjänster, etc.) låter sig detta väl göras utan att tynga lagtexten med en onödigt vid och diffus definition, som kan skapa osäkerhet kring vilken verksamhet som omfattas av lagen. Detta kan kanske också bidra till att minska den redan olyckliga förväxlingsrisken mellan de certifikat och den certifiering som här avses och det styrkande av certifikatutfärdarens kompetens som i sin tur kan ges av (eventuellt ackrediterade) certifieringsorgan.

Ett ”kvalificerat certifikat” och en ”säker anordning för signaturframställning” behandlas i avsnitt 6.4 och 6.8.

Direktivet vill ge en särskild ställning för de elektroniska signaturer som inte bara är avancerade utan också baserade på ett kvalificerat certifikat och skapade av en säker anordning för signaturframställning. Det förefaller därför lämpligt att ge dessa signaturer en särskild benämning. Här har valts ”kvalificerade elektroniska signaturer”.

Det saknas anledning att i svensk lag införa den definition av ”frivillig ackreditering” som ges i direktivet. Dess innebörd är oklar och ett införande skulle inte tjäna till annat än att tynga lagtexten och försvåra förståelsen av densamma (se avsnitt 6.7). Likaså fyller

”produkt för elektroniska signaturer” ingen funktion i den svenska lagtexten.

6.4 Kvalificerade certifikat

Förslag: I lagen skall anges vad som krävs för att ett certifikat skall anses ha en särskild säkerhetsnivå. Dessa certifikat skall betecknas som ”kvalificerade certifikat”.

I direktivet anges en särskild nivå på certifikat – kvalificerade certifikat. De krav på vad certifikatet måste innehålla som anges i bilaga I till direktivet bör också anges i den svenska lagtexten. Likaså bör i enlighet med direktivet anges att endast certifikat som utfärdats av en certifikatutfärdare som uppfyller vissa i lagen angivna krav är kvalificerade certifikat.

I kravet på att kvalificerade certifikat måste ha visst innehåll ligger att detta innehåll skall vara tillgängligt för den mottagare som förlitar sig på certifikatet. När denne tar emot ett signerat meddelande måste han således kunna tillgodogöra sig denna information, antingen genom att han ser certifikatet, där all nödvändig information finns, eller genom att informationen på annat sätt presenteras i samband med att han mottar en elektronisk handling. Inte minst viktiga är uppgifter om begränsningar för certifikatet vad gäller användningsområde eller värdet på de transaktioner för vilka certifikatet kan användas.

6.5 Utfärdande av certifikat

Förslag: I lagen skall anges vad som krävs av en certifikatutfärdare för att utfärda kvalificerade certifikat.

En certifikatutfärdares uppgift är att som en betrodd part intyga att vissa signaturverifieringsdata hör till en viss undertecknare. Nyck-

elordet härvidlag är ”betrodd”. För att certifikatutfärdarna skall bli betrodda krävs att de bedriver verksamheten med erforderlig garanti för pålitlighet.

Direktivet ställer krav endast på de certifikatutfärdare som utfärdar kvalificerade certifikat. Det saknas anledning att i svensk lagstiftning ställa krav på en vidare krets av certifikatutfärdare än dessa. (Vad gäller skadeståndsskyldigheten kan det däremot finnas anledning att mer ingående diskutera om en reglering bör träffa en vidare krets, se avsnitt 6.11.2.)

Det skall stå var och en fritt att komma överens med andra om en säkerhetsnivå som man accepterar inbördes för att sluta avtal etc. Svårigheten ligger i att sätta en gräns mellan slutna system och öppna system. Frågan har ett nära samband med frågan om när en certifikatutfärdare skall anses utfärda certifikat ”till allmänheten”. I ingressen till direktivet anges att det inte behövs något rättsligt ramverk för elektroniska signaturer som endast används inom system, vilka grundar sig på frivilliga civilrättsliga avtal mellan ett bestämt antal deltagare. Parternas frihet, sägs det, att sinsemellan komma överens om på vilka villkor de godkänner elektroniskt signerade uppgifter bör respekteras i den utsträckning det är förenligt med den nationella lagstiftningen.

Vissa klara fall kan identifieras, såsom när certifikatutfärdaren också är den ende mottagare som skall förlita sig på certifikatet och signaturen (exempelvis det existerande ”bank på Internet”). Där är det utan tvekan frågan om ett slutet system. Ett lika tydligt exempel på ett öppet system är det fallet när den mottagare som skall förlita sig på certifikatet inte har något tidigare kontraktuellt förhållande med vare sig undertecknaren eller certifikatutfärdaren. Har certifikatutfärdaren emellertid på förhand slutit ett avtal med den mottagare som skall förlita sig på certifikatet, blir gränsen svårare att dra.

”Till allmänheten” kan i detta sammanhang inte tolkas i dess mer generella betydelse. I stället får man som huvudregel utgå från att det rör sig om utfärdande till allmänheten när en certifikatutfärdare erbjuder ett certifikat till en större grupp. Det gäller även om denna grupp skulle vara begränsad till t.ex. befintliga kunder, om

certifikatet kan användas vid kommunikation med andra än certifikatutfärdaren. När en certifikatutfärdare anger att certifikaten är kvalificerade utan att i certifikatet begränsa kretsen av möjliga mottagare på ett mer precist sätt, kan det finnas anledning att anse att certifikatutfärdaren omfattas av direktivets krav på tillsyn och ett särskilt skadeståndsansvar. Problemets betydelse skall dock inte överdrivas, då den certifikatutfärdare som endast avser att agera i ett slutet system kan låta bli att benämna certifikaten som kvalificerade, varvid han undgår tillsyn och det särskilda skadeståndsansvaret.

De krav som direktivet ställer på certifikatutfärdare som utfärdar kvalificerade certifikat (bilaga II), bör ställas också i den svenska lagen. Detta innebär krav på bl.a. pålitlighet, system för säker och snabb spärrning av certifikat, säker identitetskontroll av undertecknaren, kompetent personal samt användande av pålitliga system och produkter som garanterar teknisk säkerhet. Vad gäller kravet på användandet av pålitliga system och produkter bör vidare anges att det skall anses uppfyllt om de överensstämmer med standarder för produkter för elektroniska signaturer som kommissionen offentliggjort referenser till (artikel 3.5 i direktivet).

I praktiken kommer certifikatutfärdarna med största sannolikhet också att erbjuda andra tjänster, såsom tidstämpling av signaturer m.m. och framför allt kryptering för konfidentialitet. Därmed sammanhängande frågor om exportkontroll, brottsbekämpning m.m. behandlas inte i denna promemoria. Information om den svenska politiken i dessa avseenden kan hämtas i regeringens skrivelse 1998/99:116 Om kryptografi och Utrikesutskottets betänkande 1999/2000:UU3 Om kryptografi.

6.6 Standardisering

För att elektroniska signaturer ska få en bred användning är det väsentligt att ha en gemensam syn på vilka tekniska krav som skall gälla i olika avseenden och bygga upp system som kan samverka

med varandra. Tekniska standarder har här en viktig roll att fylla och kan underlätta för användare av systemen och göra det möjligt att bedöma signaturernas säkerhet.

Tekniska standarder kan ange precisa krav för produkter för elektroniska signaturer, såsom t.ex. anordningar för signaturframställning och signeringsalgoritmer, och för certifikatutfärdande och andra certifikattjänster. Standardisering underlättar också bedömningen av om ett specifikt system eller en viss produkt uppfyller de krav som man vill ställa för den aktuella tillämpningen.

Tekniska standarder möjliggör vidare interoperabilitet, dvs. att utrustningen hos avsändare och mottagare av elektronisk kommunikation är sådan att de faktiskt kan förstå varandras meddelanden. Det önskvärda är att det utvecklas ett informationssamhälle där man helst globalt eller åtminstone inom en definierad intressesfär kan utbyta och verifiera elektroniskt signerade handlingar. Myndigheternas elektroniska gränsyta mot omvärlden skulle bli ohanterlig om antalet metoder som används för elektroniska signaturer inte begränsas.

Kommissionen uppdrog hösten 1998 åt de europeiska standardiseringsorganen och andra organisationer att analysera de framtida behoven av standardisering enligt direktivet med avseende på produkter för elektroniska signaturer och tjänster som finns tillgängliga på marknaden. Det ingick i uppdraget att föreslå en plan för att utveckla de standarder som behövs. Detta resulterade i European Electronic Signature Standardization Initiative (EESSI) som presenterat en rapport under 1999.

Analysen i rapporten visar att området är mycket komplext. Ett hundratal existerande relevanta standarder identifierades. Trots detta var slutsatsen att många viktiga specifikationer behöver utvecklas med hög prioritet (se vidare under avsnitt 6.7).

Rapporten följdes under hösten 1999 av ett ”mandat” från kommissionen till de europeiska standardiseringsorganen (CEN, CENELEC och ETSI) att följa upp EESSI-rapporten, i syfte att förse marknaden med standarder till stöd för genomförandet av direktivet. I mandatet ingår också att bilda en särskild rådgivande grupp, kallad Electronic Signature Standardization Industry

Advisory Group, för att ge rekommendationer till den rådgivande kommitté som skall inrättas enligt direktivet (se avsnitt 5). Kommittén skall av kommissionen konsulteras när den sistnämnda skall klargöra kraven i direktivets bilagor och kriterierna för utseende av de organ som skall avgöra om säkra anordningar för skapande av signaturer överensstämmer med kraven i bilaga III. Kommittén skall också konsulteras beträffande de allmänt erkända standarder för produkter för elektroniska signaturer som kommissionen skall fastställa och offentliggöra referensnummer till.

6.7 Ackreditering och certifiering

Bedömning: Lagen (1992:1119) om teknisk kontroll ger redan nu en möjlighet till frivillig ackreditering av certifieringsorgan med det syfte som anges i direktivet.

Enligt direktivet kan medlemsstaterna införa frivilliga ackrediteringssystem som syftar till att höja nivån på tillhandahållandet av certifikattjänster. Inom direktivets svårgenomträngliga definition av ”frivillig ackreditering” torde rymmas det system för ackreditering och, inte minst, certifiering under ackreditering, som tillhandahålls genom lagen (1992:1119) om teknisk kontroll. Mot bakgrund av att direktivet uttryckligen förbjuder varje form av förhandstillstånd torde de ”rättigheter och skyldigheter” som nämns i definitionen vara rättigheten att kalla sig ackrediterad/certifierad och skyldigheten att leva upp till den nivå som krävs för ackreditering/certifiering.

Syftet med ackreditering (jfr. avsnitt 4.4) är att skapa tilltro till de tjänster som de ackrediterade organen presterar. Härigenom skapas också tilltro till provningsintyg, certifikat m.m., som bl.a. gör det möjligt att godta sådan dokumentation från ett annat land utan omkontroll. Därmed har ackreditering fått en viktig roll för att främja fri rörlighet av varor och tjänster på den inre marknaden. I detta arbete gäller som en viktig princip att statliga för-

handsgodkännanden skall undvikas. Det hindrar inte att krav ställs på provning och kontroll. Bedömning av överensstämmelse ses dock som en teknisk uppgift utanför den offentligrättsliga sfären.

En ackreditering är alltid frivillig. Aktörer på marknaden vill ofta ha bevis på att varor och tjänster uppfyller ställda krav. Provning eller kontroll utförda av organ med särskild påvisad kompetens kan vara ett sätt att åstadkomma detta. Att ackreditering är frivillig hindrar inte att ett ackrediteringssystem utnyttjas för att åstadkomma legalt tvingande regler om provning och kontroll. Så sker ibland i Sverige. Tekniken blir då att man ålägger dem som omfattas av tvånget att anskaffa ett provningsintyg eller certifikat från ett ackrediterat organ. Ett sådant intyg eller certifikat får därmed rättsverkningar utan att förhållandet mellan utfärdaren och beställaren får någon offentligrättslig prägel. Staten tar själv inget ansvar för dokumentet på annat sätt än att man ålägger beställaren att anskaffa dokumentet från ett organ som uppfyller av staten uppställda kvalitetskrav. I Sverige knyts dessa kvalitetskrav normalt till ett krav på ackreditering.

Så behöver dock inte alltid vara fallet. Inom EU har man hittills undvikit att ställa formella krav på ackreditering och i stället formulerat kvalitetskrav som ibland knyts till standarder. För certifieringsorgan kan således krävas att organet skall uppfylla kraven i t.ex. standarden EN 45 011. Detta behöver dock inte visas med ackreditering, även om ackreditering är det normala sättet att styrka att kravet är uppfyllt. Inom ramen för EG:s produktdirektiv skall medlemsländerna utse s.k. anmälda organ för uppgifter som innefattar provning och certifiering. Inte heller här uppställs krav på ackreditering, men anges att ett organ som är ackrediterat skall antas uppfylla kraven.

I Sverige finns det nationella ackrediteringssystemet reglerat i lagen om teknisk kontroll. Där finns också regler om utseende av anmälda organ enligt EG-regler. Grundläggande för både ackreditering och utseende av anmälda organ är att systemen är öppna för alla organ som begär det och kan visa sin kompetens enligt ställda krav. Anmälda organ skall granskas av SWEDAC på samma sätt som vid ackreditering.

Som har framgått av det tidigare har certifikaten en stor betydelse i den ordning som regleras i direktivet. Tilltron till certifikaten får därmed central betydelse och medlemsländerna förutsätts på olika sätt främja kvaliteten på erbjudna certifikat. I enlighet med vanliga EG-principer förbjuds krav på förhandstillstånd. Medlemsländerna får dock enligt en uttrycklig bestämmelse utnyttja frivilliga ackrediteringssystem, som då skall vara objektiva, öppna och ickediskriminerande.

En ordning med ackreditering av organ för certifiering av certifikatutfärdare ligger helt inom ramen för SWEDAC:s verksamhet enligt lagen om teknisk kontroll. Någon ordning för ackreditering av den här typen av certifieringsorgan finns ännu inte helt färdig men kan relativt lätt inrättas. Den befintliga standarden EN 45 012 kan med små justeringar användas för ackreditering av certifieringsorgan för att certifiera certifikatutfärdare. Dessutom är standarder för att ackreditera certifieringsorgan för produktcertifiering under utarbetande.

Det finns vidare redan i viss mån standarder som kan användas vid certifiering av certifikatutfärdare vad gäller lednings- och säkerhetssystem, såsom den brittiska BS 7799, del 1 (Code of practise for Information Security management) och ISO TR 13335 (Guidelines for the Management of Information Technology Security-GMITS). (Numera finns även en svensk standard, baserad på den brittiska; SS 62 77 99.) Det finns även standarder som i princip kan användas för certifiering av framställning av kvalificerade certifikat (t.ex. X.509).

Lagen om teknisk kontroll ger redan nu en möjlighet till frivillig ackreditering av certifieringsorgan med det syfte som anges i direktivet. Det finns därmed ingen anledning att i lagen om elektroniska signaturer införa regler om ackreditering eller certifiering. Skyldigheten enligt direktivet att informera kommissionen och andra medlemsstater om ackrediterade nationella tillhandahållare av certifikattjänster följer av grunderna för förordningen (1994:2035) om vissa skyldigheter för myndigheter vid ett medlemskap i Europeiska unionen.

Eftersom ackreditering är frivillig, finns det inte något hinder att utan ackreditering bedriva certifiering av certifikatutfärdare.

6.8 Anordningar för signaturframställning

Förslag: I lagen skall anges vad som krävs för att en anordning för signaturframställning skall vara säker samt föreskrivas att en anordning som anges vara en säker anordning får släppas ut på marknaden eller användas för att skapa en kvalificerad signatur endast om ett för ändamålet anmält organ inom Europeiska ekonomiska samarbetsområdet (EES) avgjort att den uppfyller kraven. Vidare skall det anges att anordningar som överensstämmer med vissa standarder skall presumeras uppfylla kraven.

På samma sätt som för de kvalificerade certifikaten bör de krav som anges i direktivets bilaga III anges i den svenska lagtexten beträffande de säkra anordningar för signaturframställning (”skapande av signaturer”), som krävs för att skapa en kvalificerad signatur.

Artikel 3.4 i direktivet anger att vissa organ *skall* avgöra om säkra anordningar överensstämmer med kraven i bilaga III. Det får förstås som ett krav på att endast anordningar som av ett sådant organ bedömts överensstämma med kraven får användas för att framställa kvalificerade signaturer och endast sådana anordningar får släppas ut på marknaden under beteckningen ”säkra anordningar för signaturframställning”. Samtidigt anges i artikel 3.5 att medlemsstaterna skall utgå från att produkter som uppfyller standarder som kommissionen refererat till i Europeiska gemenskapernas officiella tidning överensstämmer med kraven i bilaga III. Någon möjlighet att tolka direktivet som att det kan räcka med en tillverkardeklaration om att en produkt uppfyller de aktuella standarderna torde inte finnas. Den sistnämnda regeln måste anses vara riktad till de aktuella organen. Denna bedömning görs också i de

övriga nordiska länderna. En regel om obligatorisk kontroll av anordningarna kompletterad med presumtionen för produkter som uppfyller de nämnda standarderna bör alltså införas i den svenska lagen.

Den möjligen kostsamma och tidskrävande obligatoriska certifiering som det här är fråga om torde dock inte nödvändigtvis innebära alltför negativa konsekvenser, då det ju räcker med att produkten godkänns i ett av länderna inom EES. Tillverkaren eller marknadsföraren är dessutom inte hänvisad till ett organ i hemlandet. Detta följer också av artikel 3.5 i direktivet där det stadgas att ett beslut som fattats av ett organ skall erkännas av samtliga medlemsstater. Även detta bör anges i lagtexten.

Enligt direktivet skall medlemsstaterna, i enlighet med kriterier som kommissionen senare skall fastställa, utse sådana organ som skall avgöra om säkra anordningar för signaturframställning överensstämmer med kraven i direktivets bilaga III. Här kan i lagen om vissa elektroniska signaturer m.m. en hänvisning ske till lagen (1992:1119) om teknisk kontroll, där det i 3 § föreskrivs att regeringen eller den myndighet som regeringen bestämmer utser de organ som skall anmälas till Europeiska unionen för uppgifter i samband med bedömning av överensstämmelse enligt bestämmelser som gäller inom EES (se avsnitt 4.4). Regeringen eller myndigheten (SWEDAC) har därvid att ta hänsyn till de kriterier som kommissionen kommer att fastställa. Regeringen kan vid behov utfärda närmare bestämmelser om detta enligt ett bemyndigande i 5 § lagen om teknisk kontroll.

6.9 Tillsyn

Förslag: En tillsynsmyndighet skall utöva tillsyn över certifikatutfärdare som till allmänheten utfärdar certifikat som anges vara kvalificerade och över anordningar som anges vara säkra anordningar för signaturframställning.

Utgångspunkten i direktivet är att det inte får införas några krav på förhandstillstånd för att få verka som certifikatutfärdare. Frivilliga ackrediteringssystem får däremot förekomma. Samtidigt är medlemsstaterna skyldiga att införa ett system för övervakning av certifikatutfärdare. Kravet på övervakning begränsas till de certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten. Direktivet ger dock ingen möjlighet till att begränsa övervakningen endast till dem som är ackrediterade eller certifierade. Det är således inte möjligt att tillfredsställa kravet på övervakning genom att nöja sig med den övervakning som utförs av ackrediterings- och certifieringsorgan. Däremot kommer naturligtvis tillsynsuppgifterna att i hög grad underlättas om ett system med frivillig ackreditering av aktörerna på marknaden får genomslag.

I den svenska diskussionen har ibland möjligheten och behovet av en s.k. toppnod förts fram. En sådan utgörs, förenklat beskrivet, av en (ev. statlig) certifikatutfärdare som utfärdar certifikat för andra certifikatutfärdare och signerar deras öppna nycklar. I ett sådant system skulle toppnoden på ett effektivt sätt kunna utöva tillsyn över anslutna certifikatutfärdare.

Direktivets regel om förbud mot förhandstillstånd innebär dock att man inte kan kräva att alla certifikatutfärdare som utfärdar kvalificerade certifikat skall ansluta sig till en toppnod och få sina öppna nycklar signerade av denne. Detta krav innebär ju att en certifikatutfärdare inte kan verka på marknaden utan att ansluta sig till toppnoden, vilket är att jämställa med ett krav på förhandstillstånd. Ett sådant krav innebär vidare att certifikatutfärdaren måste anpassa sina tekniska lösningar till toppnoden för att kunna verka i dess underliggande struktur. Detta strider mot direktivets strävan mot teknikneutralitet, vilket innebär att direktivets krav skall kunna uppfyllas på flera olika sätt med hjälp av olika typer av teknik.

Omfattningen av tillsynen

Anledning saknas att gå längre än direktivet och låta en tillsyn omfatta även de certifikatutfärdare som inte utfärdar certifikat till allmänheten, se avsnitt 6.5. Ingenting hindrar emellertid att man i

den svenska lagstiftningen föreskriver att övervakningen inte skall begränsas till att gälla dem som utfärdar kvalificerade certifikat, utan omfatta alla som utfärdar certifikat till allmänheten. Detta skulle dock kunna leda till att marknaden påverkas negativt. Det ekonomiska värdet av elektroniska signaturer ligger inte främst i utfärdande av certifikat, utan i en ökad säkerhet för undertecknaren och mottagaren av det signerade meddelandet (parterna). Det är därför viktigt att det finns en hög grad av valfrihet på marknaden så att parterna kan välja den form av certifikat som passar för olika typer av transaktioner. En transaktion som rör högre värden och där man önskar hög säkerhet kan motivera användandet av ett kvalificerat certifikat (eller ett certifikat med ännu högre säkerhet), även om detta leder till en viss kostnad för parterna. För många fall kan emellertid förutses att signaturer används på en massmarknad för transaktioner med lågt värde. Obligatoriska krav och en obligatorisk tillsyn av alla certifikatutfärdare skulle kunna innebära en ökad kostnad för certifikaten som parterna anser vara för hög. Detta skulle i sin tur leda till att parterna väljer andra, mindre säkra lösningar, eller avstår från elektronisk kommunikation. Det finns därför inte anledning att gå längre vad gäller tillsyn än vad direktivet kräver.

Formen för tillsynen

För den som vill uppträda som certifikatutfärdare är det helt avgörande att han bygger upp en tillit till sina certifikat. Utan det förtroendet finns inget användningsområde för de elektroniska signaturer som är baserade på hans certifikat. Detta talar för att marknaden i hög grad kommer att reglera sig själv. Samtidigt kan det för tilliten till systemet i sin helhet vara värdefullt med en instans som kan ingripa mot missförhållanden. För att denna tillsyn skall ha något reellt innehåll bör instansen ha möjlighet till myndighetsutövning. Detta, i kombination med berättigade krav på insyn, rättssäkerhet, möjlighet till överprövning etc. talar för att övervakningen bör anförtros en statlig myndighet, även om direk-

tivet ger en möjlighet till att låta övervakningen skötas av en privat institution.

Den tillsyn som utövas bör vara så marknadsorienterad som möjligt. Med hänsyn till att verksamheten för en certifikatutfärdare är så beroende av att man hyser förtroende för hans certifikat, kan tillsynssystemet utformas så att det inte lägger några onödiga administrativa bördor på certifikatutfärdaren, utan inriktas på att vid klagomål kontrollera en utfärdare närmare.

I arbetet med denna promemoria har övervägts en mer ambitiös övervakningsmodell, som bl.a. skulle innefatta ett krav på certifikatutfärdaren att till tillsynsmyndigheten ge in ett ”certifikatsprogram”. Där skulle certifikatutfärdaren utförligt redogöra för hur han uppfyller kraven i lagstiftningen/direktivet. Detta program skulle ges in i samband med att verksamheten startade och därefter en gång per år. Detta system skulle möjligen, beroende på hur hårt tillsynsmyndigheten kan ingripa vid ett uteblivet program, kunna förenas med förbudet mot förhandstillstånd. Allvarligare är dock den tungrodda och kostsamma apparat detta skulle innebära, i viss mån för myndigheten men framförallt för certifikatutfärdaren. Det skulle stå i kontrast till de mer marknadsorienterade system som övervägs i andra länder.

Det får anses vara önskvärt att marknaden i så stor omfattning som möjligt begagnar sig av de kvalificerade certifikat som direktivet etablerar. Ett gemensamt europeiskt och i bästa fall globalt användande av dessa certifikat skulle leda till en allmän acceptans och förtroende för de signaturer som baseras på sådana certifikat, vilket skulle vara till fördel för elektronisk handel och andra användningsområden. För den certifikatutfärdare som önskar undgå den tillsyn som direktivet och lagen stipulerar kan det emellertid vara frestande att *inte* kalla sina certifikat för kvalificerade, trots att de uppfyller kraven i lagen. Kan han bygga upp ett förtroende för dem i alla fall, finns inget behov av detta (här bortses från eventuella rättsverkningar som i andra länder kan tänkas ges endast för kvalificerade signaturer). Stora administrativa krav på den som utfärdar kvalificerade certifikat till allmänheten skulle förstärka en

sådan utveckling. Det skulle också kunna förhindra framväxandet av öppna system.

Slutsatsen av detta resonemang är att det bör införas ett tillsynssystem i statlig regi, men där tillsynen är marknadsorienterad och inte innebär en tung administration för dem som uppträder på marknaden.

Tillsynsmyndighetens befogenheter m.m.

En grundläggande förutsättning för att kunna utöva tillsyn är att veta vem man skall kontrollera. Certifikatutfärdare som avser att utfärda kvalificerade certifikat till allmänheten bör därför i samband med att de startar verksamheten vara skyldiga att anmäla till tillsynsmyndigheten att så sker. Detta står inte i strid med förbudet mot förhandstillstånd.

Med utgångspunkt från den kravkatalog som i lagen ställs upp för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten blir myndighetens uppgift att ingripa mot dem som inte uppfyller kraven. Myndigheten bör därvid ha befogenhet att kräva in de handlingar och upplysningar som behövs för tillsynen. Om anmälningspliktig verksamhet bedrivs utan att anmälan skett eller brister i verksamheten upptäcks bör myndigheten kunna utfärda förelägganden om rättelser. Dessa förelägganden bör också kunna förenas med vite. Till slut bör tillsynsmyndigheten, om inte föreläggande räcker, kunna förbjuda den som begår upprepade eller allvarligare överträdelser att bedriva verksamheten, eller i varje fall att kalla sina certifikat för kvalificerade.

Myndighetens befogenheter får dock inte utövas på ett sådant sätt att de i praktiken utgör ett hinder för att ta sig in på marknaden (krav på förhandstillstånd). Ett gradvis upptrappat användande av förelägganden, så småningom förenade med vite torde inte anses utgöra sådana hinder. Vid någon tidpunkt måste det också anses rimligt att tvinga en certifikatutfärdare att upphöra med verksamheten, om denne t.ex. på ett flagrant sätt nonchalerar lagens krav, eller efter upprepade krav underlåter att följa lagstiftningen. I

slutänden handlar det om proportionalitet mellan överträdelser och åtgärder.

Tillsyn – certifiering

Tillsynen kan i praktiken utformas som stickprovskontroller och undersökningar sedan någon anmält misstänkta felaktigheter hos en certifikatutfärdare. I den mån en certifikatutfärdare valt att certifiera sin organisation eller sina produkter mot en vedertagen standard kan myndigheten i stor utsträckning nöja sig med den kontroll som certifieringen innebär. I det praktiska tillsynsarbetet kan myndigheten också använda sig av accepterade standarder för att jämföra om de tekniska lösningarna eller organisationen håller föreskriven standard. Det är dock väsentligt att myndigheten inte låser fast sig vid någon särskild teknik. Även system som inte ansluter sig till någon standard kan mycket väl uppfylla de krav på säkerhet m.m. som uppställs i lagstiftningen.

Marknadskontroll

Reglerna i lagen om att anordningar som anges vara säkra anordningar för signaturframställning får släppas ut på marknaden eller användas endast om vissa organ bedömt att de överensstämmer med lagens krav (se avsnitt 6.8) innebär att tillsynsmyndigheten också har att utöva viss marknadskontroll.

6.10 Behandling av personuppgifter

Förslag: I lagen skall anges begränsningar för hur den som utfärdar certifikat till allmänheten får behandla personuppgifter.

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda med avseende på behandling

av personuppgifter och om det fria flödet av sådana uppgifter har genomförts i svensk rätt genom personuppgiftslagen (1998:204). Lagen innehåller bestämmelser om när behandling av personuppgifter är tillåten.

Enligt lagen gäller bl.a. följande. Personuppgifter får behandlas (inkluderande insamlas) bara om den registrerade har lämnat sitt samtycke till behandlingen, eller om behandlingen är nödvändig av vissa närmare angivna skäl. Personuppgifter som samlats in för ett ändamål får inte behandlas för något annat oförenligt ändamål. Fler personuppgifter än som är nödvändigt med hänsyn till ändamålet får inte behandlas.

Personuppgiftslagen är tillämplig på certifikatutfärdare, SWEDAC och tillsynsmyndigheten, utan att detta särskilt behöver anges. Artikel 8.2 i direktivet innehåller dock regler som innebär strängare krav än de som uppställs i personuppgiftslagen. Det bör därför i lagen om vissa elektroniska signaturer m.m. införas en regel om att certifikatutfärdare som utfärdar certifikat till allmänheten endast under dessa strängare förutsättningar får behandla personuppgifter. Regeln skall inte vara begränsad till dem som utfärdar kvalificerade certifikat.

6.11 Skadestånd

6.11.1 Allmänt om skadestånd och användning av elektroniska signaturer

Det öppna nyckelsystemet

Direktivet bygger som nämnts på ett tekniskt och organisatoriskt system för elektroniska signaturer som brukar benämnas PKI (från engelskans Public Key Infrastructure). På svenska kan systemet benämnas det öppna nyckelsystemet (se avsnitt 4.3.4). Systemet är för dagen det helt förhärskande för elektroniska signaturer. I framtiden kan dock något annat komma att gälla.

Det öppna nyckelsystemet bygger på medverkan av tre aktörer, nämligen undertecknare, certifikatutfärdare och mottagare. Det kan dock förekomma – och det är inte ovanligt – att en och samma person är mer än en aktör i denna kedja. Det är t.ex. vanligt att en bank både är certifikatutfärdare och mottagare. Så är fallet när en bank utfärdar certifikat för att sedan förlita sig på elektroniska signaturer som används av bankens kunder.

Undertecknaren kan också benämnas ”nyckelinnehavaren”, dvs. den som innehar det unika nyckelpar som utgörs av en privat nyckel och en öppen nyckel (se avsnitt 4.3.1). Nyckelinnehavaren/undertecknaren är ”den behörige”, som kontrollerar signaturframställningsdata och anordningen för signaturframställning.

Det öppna nyckelsystemet reser i huvudsak tre olika särskilda skadeståndsrättsliga ansvarsförhållanden, nämligen

a. undertecknarens ansvar vid obehörig användning av den elektroniska signaturen,

b. certifikatutfärdarens ansvar gentemot undertecknaren och

c. certifikatutfärdarens ansvar gentemot mottagaren.

Undertecknarens ansvar vid obehörig användning

Det kan inträffa att någon annan än den egentlige undertecknaren obehörigen använder den privata nyckeln och med hjälp av denna vidtar rättshandlingar i undertecknarens namn. Det betyder alltså att någon falskeligen uppträder som undertecknare. Ett sådant missbruk kan t.ex. ha möjliggjorts genom att undertecknaren handskats vårdslöst med sin PIN-kod eller sitt smarta kort. Det kan också vara så att den elektroniska signaturen missbrukas utan undertecknarens förskyllan, t.ex. av en s.k. hacker eller av att certifikatutfärdaren lämnat ut den privata nyckeln till fel person.

De ansvarsfrågor som aktualiseras här regleras över huvud taget inte i direktivet. Det kan ändå finnas skäl att något behandla problemet.

Enligt svensk rätt torde som utgångspunkt gälla att undertecknaren inte blir bunden av rättshandlingar som inte har företagits av honom eller henne. I rättspraxis har man visserligen i vissa fall låtit

den som åberopar ogiltigheten bli skadeståndsskyldig om han eller hon genom vårdslöshet möjliggjort förfalskningen (jfr. t.ex. NJA 1935 s. 646). Huruvida en undertecknare skulle kunna bli skadeståndsskyldig enligt dessa principer om denne varit oaktsam och därigenom möjliggjort det obehöriga användandet måste dock betecknas som mycket osäkert.

Det är viktigt att komma ihåg att det alltid råder ett avtalsförhållande mellan undertecknaren och certifikatutfärdaren. Undertecknaren måste ju vända sig till certifikatutfärdaren för att få ett certifikat utfärdat. Det finns således alltid möjligheter att reglera ansvarsfrågor i avtalet mellan parterna.

De här aktuella problemen uppvisar vissa likheter med obehörig användning av kontokort. För dessa fall finns en särskild reglering i 34 § konsumentkreditlagen (1992:830). Bestämmelsen har införts för att komma till rätta med stränga avtalsvillkor rörande konsumenternas betalningsansvar vid obehöriga uttag med kontokort.

Det kan finnas skäl att överväga en särskild reglering på detta område i svensk rätt. Det kan nämnas att i den modellag för elektroniska signaturer som man för närvarande arbetar fram inom UNCITRAL (jfr. modellagen för elektronisk handel, avsnitt 4.2) diskuteras just principer för undertecknarens ansvar för obehörig användning. Frågan är dock komplicerad och bör lämpligen övervägas i något annat sammanhang än vid genomförandet av direktivet.

Certifikatutfärdarens ansvar gentemot undertecknaren

Som ovan nämnts är förhållandet mellan certifikatutfärdaren och undertecknaren kontraktsrättsligt. Frågan om certifikatutfärdarens ansvar gentemot undertecknaren kompliceras dock av att det kan vara svårt att ange vad som är avtalets objekt och vilken typ av avtal det är frågan om. Den privata nyckeln kan vara lagrad på ett smart kort, på en hårddisk, på en diskett osv. och man kan tänka sig att certifikatutfärdaren genererar ett nyckelpar till undertecknaren.

Certifikatutfärdaren och undertecknaren kan i dag efter gottfinnande reglera relevanta frågor i avtalet såsom ansvarsgrunder, ansvarets omfattning och ansvarsbegränsningar. Avtalsfriheten begränsas ytterst av 36 § lagen (1915:218) om avtal och andra rättshandlingar på förmögenhetens område (avtalslagen). Om certifikatutfärdaren inte uppfyller sina förpliktelser enligt avtalet med undertecknaren kan ett avtalsbrott föreligga.

Förhållandet mellan certifikatutfärdaren och undertecknaren regleras i viss mån genom artikel 6 i direktivet.

Certifikatutfärdarens ansvar gentemot mottagaren

Om uppgifterna i ett certifikat är felaktiga – t.ex. eftersom certifikatutfärdaren inte har kontrollerat identiteten hos undertecknaren på det sätt som påstås i certifikatet – kan mottagaren lida en skada om denne vid en ekonomisk transaktion förlitar sig på den elektroniska signaturen. Relationen mellan certifikatutfärdaren och mottagaren kan vara av olika slag. De kan ha en kontraktsrättslig relation, men vanligen torde det inte finnas något avtal mellan dem.

När det inte finns något avtal mellan certifikatutfärdaren och mottagaren gäller utomkontraktuella regler. I utomkontraktuella förhållanden är huvudregeln att skadeståndsskyldighet för ren förmögenhetsskada (dvs. ekonomisk skada som uppkommit utan att någon lidit person- eller sakskada) föreligger endast om skadan orsakats genom brott. Det framgår av 2 kap. 4 § skadeståndslagen (1972:207). För att ren förmögenhetsskada skall vara ersättningsgill i andra fall krävs i princip en specialbestämmelse i lag. Av förarbetena till 2 kap. 4 § skadeståndslagen framgår dock att avsikten inte varit att lägga hinder i vägen för en rättsutveckling i praxis i riktning mot ett vidgat ansvar för ren förmögenhetsskada (jfr. prop. 1972:5 s. 568). Sedan lång tid har också i rättspraxis skadeståndsansvar godtagits beträffande t.ex. felaktiga vederhäftighets- och vittnesintyg samt beträffande soliditetsupplysningar. Särskilt intressant i detta sammanhang är rättsfallet NJA 1987 s. 692 där en värderingsman som av oaktsamhet utfärdat ett oriktigt

värderingsintyg ansågs skadeståndsskyldig gentemot en långivare som förlitat sig på intyget.

Det kan diskuteras i vilken utsträckning en mottagare kan göra gällande att en certifikatutfärdare är skadeståndsskyldig i enlighet med principerna i 1987 års fall. När certifikatutfärdaren utfärdar ett certifikat sker det normalt i syfte att tredje man skall kunna förlita sig på uppgifterna i certifikatet. Certifikatet riktar sig ju ofta just till tredje man. I så måtto finns likheter med 1987 års fall. Av betydelse är dock att målgruppen för certifikatet i regel kan vara obegränsad. Det är omöjligt för en certifikatutfärdare att överblicka de transaktioner som signaturen kommer att användas till och vem som kan förväntas förlita sig på certifikatet. I normalfallet saknar certifikatutfärdaren vetskap om för vilka ändamål signaturen kommer att användas. Så behöver dock inte vara fallet om certifikatutfärdaren har begränsat t.ex. certifikatets användningsområde. Rättsläget måste hur som helst betecknas som osäkert.

I de fall det trots allt finns ett avtal mellan certifikatutfärdaren och mottagaren är det i dag fritt för dem att sinsemellan reglera förutsättningarna för ansvar. Avtalsfriheten begränsas också här ytterst av 36 § avtalslagen. Om certifikatutfärdaren inte uppfyller sina förpliktelser enligt avtalet med mottagaren kan ett avtalsbrott föreligga.

Ansvarsförhållandet mellan certifikatutfärdaren och mottagaren regleras i artikel 6 i direktivet.

6.11.2 Genomförandet av direktivets artikel om skadestånd

Förslag: I lagen skall föreskrivas ett skadeståndsrättsligt presumtionsansvar för den som utfärdar kvalificerade certifikat till allmänheten gentemot den som förlitar sig på certifikatet.

Ansvarets omfattning

Artikel 6 i direktivet föreskriver att som ett minimikrav skall medlemsstaterna säkerställa att certifikatutfärdaren har ett s.k. presumtionsansvar. Det innebär att om den som förlitar sig på certifikatet lider en skada till följd av t.ex. en felaktighet i certifikatet skall certifikatutfärdaren ersätta skadan såvida inte certifikatutfärdaren kan visa att felaktigheten beror på något annat än att denne varit vårdslös. Certifikatutfärdaren skall alltså antas – presumeras – ha orsakat skadan genom vårdslöshet, men lyckas utfärdaren bevisa att skadan inte beror på vårdslöshet på dennes sida skall utfärdaren kunna undgå skadeståndsansvar. Eftersom detta i direktivet formulerats som ett minimikrav är det möjligt för medlemsstaterna att i stället föreskriva ett strikt ansvar för certifikatutfärdaren, dvs. att denne skall vara skadeståndsskyldig oberoende av eget vållande.

Vid bestämmande av vilken omfattning certifikatutfärdarens ansvar skall ha finns flera hänsyn att ta. Det är viktigt att betona att certifikatets funktion är att skapa trygghet. Den som tar del av innehållet skall kunna förlita sig på att det är riktigt. Ett viktigt syfte med regleringen måste vidare vara att gynna förekomsten av elektroniska signaturer och certifikattjänster. Regleringen får inte riskera att onödigt hämma framväxten av certifikattjänster. Det är därvid väsentligt att komma ihåg att certifikat är något som certifikatutfärdarna normalt tar betalt för. Det vore naturligtvis olyckligt med en utveckling där certifikatutfärdarna tog så mycket betalt för certifikaten att elektroniska signaturer endast skulle komma att användas av företag och inte av privatpersoner.

En annan aspekt som inte är oväsentlig i sammanhanget är att man bör försöka uppnå nordisk rättslikhet på området. I övriga nordiska länder har man hittills planerat att genomföra direktivet så att certifikatutfärdarna åläggs ett presumtionsansvar.

Det som från angivna utgångspunkter framstår som mest lämpligt är att stanna för ett presumtionsansvar för certifikatutfärdaren. Sedan t.ex. en felaktighet i certifikatet och en därtill knuten skada för den som förlitar sig på certifikatet har konstaterats måste då certifikatutfärdaren bevisa att skadan inte uppkommit på grund av dennes vårdslöshet. Detta är rimligt eftersom certifikatutfärdaren

torde ha lättast att föra fram bevisning i detta avseende. Om däremot certifikatutfärdarna skulle sakna möjlighet att visa att man vidtagit alla rimliga åtgärder för att förhindra en felaktighet skulle utvecklingen av sådana tjänster hämmas på ett olyckligt sätt.

Certifikatutfärdare som skall omfattas av skadeståndsregeln

Det skadeståndsansvar som föreskrivs i direktivet omfattar endast de certifikatutfärdare som utfärdar, eller garanterar en annan certifikatutfärdares, certifikat till allmänheten och som uppger att certifikatet är kvalificerat. En certifikatutfärdare som inte utger sig för att utfärda kvalificerade certifikat träffas över huvud taget inte av direktivets skadeståndsregler. Frågan är om vi i Sverige nu bör införa en regel som går längre än direktivet och ålägger en skadeståndsskyldighet även för andra certifikatutfärdare. Direktivet torde inte hindra en sådan nationell lagstiftning.

Det finns bärkraftiga argument både för att utöka den krets som skall träffas av direktivets skadeståndsregler och för att inte göra det. Som nämnts ovan är det tämligen oklart vad som i dag gäller om certifikatutfärdares ansvar gentemot mottagaren enligt allmänna skadeståndsrättsliga regler, i varje fall när de inte har något avtalsförhållande med varandra, vilket torde vara det vanliga. Denna osäkerhet talar för att kretsen bör utökas i förhållande till direktivet. Det kan förutsättas att många av de certifikat som finns och kommer att finnas på marknaden i framtiden inte är kvalificerade i direktivets mening. Det kan i dessa fall finnas väl så starka skäl att ha en specialreglering för certifikatutfärdarens ansvar. Samtidigt finns det starka betänkligheter med en utvidgad krets. Regleringen tar såvitt avser förhållandet mellan certifikatutfärdaren och mottagaren huvudsakligen sikte på skadeståndsansvar för ren förmögenhetsskada i utomobligatoriska förhållanden. På detta område präglas svensk rätt av tämligen stor restriktivitet. Om kretsen skulle utvidgas är det viktigt att den är tydligt identifierbar och definierad. Det skulle kunna föra för långt om skadeståndsansvar för rena förmögenhetsskador i utomkontraktuella förhållanden

träffade alla certifikatutfärdare eller alla som i en elektronisk miljö identifierar avsändare av elektroniska meddelanden. Det är förenat med betydande svårigheter att finna tydliga avgränsningar på området. Vidare bygger direktivet till stor del på att det skapas en slags standard för elektroniska signaturer i Europa och de som baserar sig på kvalificerade certifikat ges en särställning i direktivet (jfr. avsnitt 6.12). Det kan därför ses som mest förenligt med tankarna bakom direktivet att begränsa skadeståndsregleringen till de fall certifikatutfärdaren anger att han utfärdar kvalificerade certifikat. De som förlitar sig på certifikaten får därmed också en tydlig signal om de kvalificerade certifikatens särskilda kvalitéer. Samtidigt undviker man att förena certifikat som avses användas på ett sätt som inte kräver så hög säkerhet med avskräckande höga kostnader (jfr. resonemanget i avsnitt 6.9 och 6.11.1).

För dagen talar därför övervägande skäl för att inte utvidga den krets som träffas av direktivets skadeståndsregler. I sammanhanget kan nämnas att man hittills planerar att lösa frågan på samma sätt i övriga nordiska länder. En jämförelse med övriga nordiska länder i detta avseende haltar dock eftersom vi har delvis olika regler om ansvar för ren förmögenhetsskada utanför kontraktsförhållanden.

Reglernas utformning

Artikel 6 i direktivet föreskriver att certifikatutfärdaren har ett skadeståndsrättsligt presumtionsansvar för att uppgifterna i ett kvalificerat certifikat är korrekta och fullständiga, att undertecknaren vid tidpunkten för utfärdandet var i besittning av de signaturframställningsdata som motsvarar de signaturverifieringsdata som anges i certifikatet samt att signaturframställningsdata och signaturverifieringsdata kan användas som komplement till varandra om certifikatutfärdaren framställer båda. Vidare har certifikatutfärdaren samma ansvar för skada som genom underlåtenhet att registrera ett återkallande av ett certifikat åsamkats den som har rimlig anledning att förlita sig på certifikatet.

De i lagen ställda kraven på kvalificerade certifikat och den som utfärdar sådana till allmänheten (se avsnitt 6.5) kan utformas bl.a.

som handlingsregler för certifikatutfärdaren, som motsvarar vad certifikatutfärdaren enligt direktivet skall ha ett skadeståndsrättsligt presumtionsansvar för. Skadeståndsreglerna i lagen kan då lämpligen utformas så att certifikatutfärdaren bär det särskilda skadeståndsansvaret om uppgifterna i ett certifikat som anges vara kvalificerat är felaktiga eller ofullständiga, eller certifikatutfärdaren inte har uppfyllt vissa handlingsregler.

Artikel 6 stadgar också att medlemsstaterna skall föreskriva att en certifikatutfärdare får ange begränsningar för områden eller transaktionsbelopp som certifikatet får användas för samt att certifikatutfärdaren inte skall vara ansvarig för skador som härrör från ett överskridande av dessa begränsningar. Även detta bör anges i lagtexten.

6.12 Rättslig verkan för elektroniska signaturer

Förslag: Lagen skall innehålla en regel som anger de kvalificerade elektroniska signaturernas särställning.

Tillämpningsområdet

I direktivets artikel 5 regleras frågan om elektroniska signaturers rättsverkan. Artikeln kan dock inte läsas och tolkas isolerat från övriga artiklar i direktivet. Av särskild betydelse för hur artikel 5 skall uppfattas är artikel 1 i direktivet som reglerar direktivets tillämpningsområde.

Av artikel 1 framgår att syftet med direktivet är att underlätta användningen av elektroniska signaturer och bidra till deras rättsliga erkännande. Av artikeln framgår vidare att direktivet inte omfattar frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser om den nationella lagstiftningen eller gemen-

skapslagstiftningen föreskriver vissa formkrav. Direktivet påverkar inte heller bestämmelser och begränsningar i nationell lagstiftning eller gemenskapslagstiftning som reglerar användningen av dokument.

Frågan hur man skall uppfatta direktivets omfattning enligt artikel 1 är av helt avgörande betydelse för hur rättsverkansregeln i artikel 5 skall förstås. Till att börja med är det sålunda klart att direktivet inte inom något rättsområde föreskriver att elektronisk kommunikation måste accepteras. Vidare torde artikel 1 innebära att direktivet inte förbjuder medlemsstaterna att på något rättsområde ha formkrav på egenhändiga namnunderskrifter som utesluter användning av elektroniska signaturer.

Direktivets rättsverkansregel

I svensk lag finns egentligen inga regler som anger hur ett krav på underskrift skall uppfyllas. Det sägs ingenstans att underskriften skall vara läslig på det sättet att personens namn kan utläsas av underskriften. Det sägs vidare inget om att personen skall använda sitt fulla namn eller sina initialer eller enbart ett bomärke eller kryss. Kravet på underskrift uttrycks också på olika sätt i skilda författningar. Exempelvis krävs det i vissa författningar ”underskrift” medan det i andra författningar krävs ”namnunderskrift”. Även om det saknas regler om vad som krävs för att uppfylla ett formkrav på underskrift måste det åtminstone i vissa situationer finnas en gräns för vad som kan godtas när det ställs ett sådant krav. Någon form av angivelse om vem som avses med underskriften torde krävas. Är det en skrivkunnig person torde det möjligen krävas att det är ett allvarligt försök att forma namnet i skrift. I vissa situationer torde därför inte vilket avtryck som helst från exempelvis en penna anses konstituera en underskrift eller namnunderskrift. Frågan har nog tämligen sällan ställts på sin spets och fått praktisk betydelse och därmed vållat några problem.

När det gäller elektroniska signaturer förhåller det sig lite annorlunda. Den som förlitar sig på en elektronisk signatur ser inte tekniken i systemet och hur kontrollen går till. I princip får de

mottagare som förlitar sig på en elektronisk signatur endast ett meddelande på sin dator om att identitet och innehåll stämmer eller inte stämmer. Som tidigare nämnts bygger direktivet på elektroniska signaturer enligt det s.k. öppna nyckelsystemet. Även om detta koncept har en viss given struktur kan tekniken ha olika hög säkerhetsnivå.

I artikel 5.1 beskrivs en typ av elektroniska signaturer med särskilt hög säkerhetsnivå, i promemorian benämnda kvalificerade elektroniska signaturer.

Enligt artikel 5.1.a skall medlemsländerna säkerställa att dessa kvalificerade elektroniska signaturer uppfyller de rättsliga kraven på en signatur i förhållande till uppgifter i elektronisk form, på samma sätt som en handskriven signatur uppfyller samma krav i förhållande till uppgifter på papper. Medlemsstaterna är vidare enligt artikel 5.1.b skyldiga att se till att de godtas som bevis vid rättsliga förfaranden. Frågan är om det krävs några åtgärder för att svensk rätt skall leva upp till direktivet i denna del.

Som tidigare påpekats kan innebörden av artikeln i denna del inte vara att medlemsstaterna skall godta kvalificerade signaturer i alla fall där det finns ett krav på underskrift i svensk rätt eller gemenskapsrätt. Direktivet hindrar inte att man enligt nationell rätt utesluter användning av elektroniska signaturer när det finns formkrav på underskrift. Denna fråga regleras över huvud taget inte i direktivet enligt artikel 1. Därför måste nog artikel 5.1.a uppfattas så att om man i nationell rätt – antingen på grund av lagstiftning eller på grund av tolkning av formkravsregler – anser att ett formkrav på traditionell underskrift i stället kan uppfyllas med en elektronisk signatur, måste de kvalificerade signaturerna alltid anses uppfylla kravet. En kvalificerad elektronisk signatur måste alltså då betraktas som en underskrift i förhållande till uppgifter i elektronisk form på samma sätt som egenhändiga namnunderskrifter godtas som underskrift i förhållande till uppgifter på papper. På detta vis skapas inom hela gemenskapen en standard för elektroniska signaturer, vilket kan vara gynnsamt för den inre marknaden.

Därför bör det i den svenska lagen införas en bestämmelse som klargör detta förhållande.

När det gäller artikel 5.1.b – dvs. att kvalificerade signaturer skall godtas som bevis vid rättsliga förfaranden – behövs knappast några lagstiftningsåtgärder. Enligt principen om den fria bevisprövningen som gäller i Sverige följer att det inte finns något hinder mot att använda vissa kunskapskällor eller medier som bevisning. Något hinder mot att använda elektroniska signaturer finns således inte.

I artikel 5.2 ges regler för alla typer av elektroniska signaturer, dvs. inte enbart de som är kvalificerade. Där sägs att medlemsstaterna skall se till att en elektronisk signatur inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på den grunden att signaturen

– är i elektronisk form,

– inte är baserad på ett kvalificerat certifikat,

– inte är baserad på ett kvalificerat certifikat utfärdat av en ackrediterad tillhandahållare av certifikattjänster eller

– inte är skapad av en säker anordning för skapande av signaturer.

När det gäller kravet att elektroniska signaturer inte får förvägras giltighet som bevis vid rättsliga förfaranden på grund av skäl som anges i artikel 5.2 innebär det med hänvisning till den fria bevisprövningens princip inga problem för svensk del. Några lagstiftningsåtgärder krävs inte för att genomföra direktivet i denna del. Men frågan är vad artikeln i övrigt kan innebära för svensk del.

Lika lite som artikel 5.1 kan denna bestämmelse anses innebära att medlemsstaterna måste se till att en elektronisk signatur över huvud taget skall kunna användas för att uppfylla formkrav som finns i nationell lagstiftning. Det följer som tidigare nämnts redan av artikel 1.

Till skillnad från artikel 5.1 har inte artikel 5.2 någon hänvisning till ”handskrivna signaturer på papper”. Det sägs bara att elektroniska signaturer inte får förvägras rättslig verkan på grund av omständigheter som där anges. I svensk rätt finns knappast några regler som kan sägas förvägra elektroniska signaturer rättslig

verkan över huvud taget. Visserligen kan det finnas formkrav för rättshandlingar som utesluter användning av elektroniska signaturer, men detta är tillåtet enligt artikel 1. Vidare är det enbart kvalificerade elektroniska signaturer som måste anses uppfylla kraven på en handskriven underskrift när man i nationell rätt gör en sådan jämställelse. Artikel 5.2 torde därför inte kräva några lagstiftningsåtgärder i Sverige.

Som framgått finns det ett antal formkravsregler i svensk rätt som kräver underskrift, egenhändig namnunderskrift eller liknande. Dessa regler finns främst inom förvaltningsrätten men det finns också ett begränsat antal sådana regler inom förmögenhets- och familjerätten. Reglerna kan antas i flera fall utesluta elektroniska rutiner eller i varje fall föranleda tvekan till följd av formuleringen av formkravet.

I denna situation bör utgångspunkten vara att det inte bör finnas otidsenliga formkrav som på ett onödigt sätt hindrar elektronisk kommunikation. Någon generell regel i svensk lagstiftning som likställer egenhändiga namnunderskrifter med vissa typer av elektroniska signaturer torde dock inte vara möjlig (se vidare avsnitt 9).

När artikel 5 genomförs i svensk rätt bör man därför inte generellt jämställa vissa elektroniska signaturer med egenhändiga namnunderskrifter i de författningar där det finns formkrav som kräver underskrifter. I stället bör det införas en regel som anger de kvalificerade elektroniska signaturerna särställning i de fall det i lag eller andra författningar finns formkrav som kan uppfyllas med hjälp av elektroniska signaturer.

Bestämmelsen bör utformas så att en kvalificerad signatur alltid måste anses uppfylla formkravet på elektronisk signatur. Bestämmelsen bör självfallet inte hindra att det är möjligt att ifrågasätta härkomsten, dvs. om det är rätt person som ligger bakom signaturen. Liksom vid användning av egenhändiga namnunderskrifter kan alltid härkomsten ifrågasättas om det finns anledning till det.

Användning av elektroniska signaturer i den offentliga sektorn

I direktivets artikel 3.7 anges att medlemsstaterna får förena användningen av elektroniska signaturer i den offentliga sektorn med eventuella ytterligare krav. Sådana krav skall vara objektiva, tydliga, proportionella och icke-diskriminerande och skall endast gälla de särskilda egenskaperna för den berörda tillämpningen. Dessa krav får inte utgöra ett hinder för gränsöverskridande tjänster för medborgaren.

Inom den offentliga sektorn är det tänkbart att problem kan uppstå om en myndighet inte har utrustning som kan tyda ett elektroniskt meddelande, eller om avsändaren eller innehållet efter en viss tid inte längre kan verifieras eller meddelandena inte är tidstämplade eller inte kan arkiveras på det sätt som önskas.

Det kan vara värdefullt att vid bedömningen av om detta föranleder särskilda krav inom den offentliga sektorn jämföra motsvarande behov när kommunikationen sker genom pappersbaserade meddelanden.

Den föreslagna bestämmelsen tar endast sikte på formkrav. Det fallet att en myndighet inte kan tyda ett inkommet meddelande torde i sig inte utgöra en brist i formkravet att handlingen skall vara underskriven. En pappershandling kan mycket väl vara underskriven men fullständigt oläsbar. Huruvida den som gett in handlingen har uppfyllt formkravet att handlingen skall vara underskriven är därmed inte avgörande för om denne uppfyllt de krav som ställs för att t.ex. fullgöra en förpliktelse.

Problemet med att en avsändaren av en handling eller innehållet i densamma efter en viss tid inte längre kan läsas måste inte heller det nödvändigtvis vara kopplat till ett formkrav. Myndigheten torde tämligen enkelt kunna upprätta en procedur för att senare kunna vara säker på vem som avsänt en handling och dess riktiga innehåll. På samma sätt kan myndigheten säkerställa att det i dess eget system anges när en handling inkommit till myndigheten.

Vad gäller pappershandlingar torde det mer sällan krävas att den som ger in en handling till en myndighet skall använda sig av arkivsäkert bläck eller arkivsäkert papper. Finns det undantagsvis fog för ett sådant krav är det kanske inte lämpligt att kommunika-

tionen sker elektroniskt. Även här kan man förutse system för myndigheternas vidimering av inkommande handlingar och kanske överförande till databärare som bättre uppfyller kraven för arkivering. En annan sak är att det inom myndigheten finns ett behov av att kunna framställa handlingar som kan arkiveras en längre tid. Detta kan dock ske utan att det i lagen anges att högre krav får ställas på elektroniska signaturer inom offentlig förvaltning. En mer ingående diskussion i dessa frågor återfinns i betänkandet Elektronisk dokumenthantering (SOU 1996:40).

Resonemanget ovan utesluter inte att det i framtiden kan bli uppenbart att de kvalificerade elektroniska signaturerna inte är tillräckliga för den offentliga sektorns behov. Om det sker kan lagstiftningen kompletteras med en regel om att användningen av elektroniska signaturer får förenas med ytterligare krav om det finns särskilda skäl. För närvarande finns dock inte tillräckliga skäl att införa en sådan reglering, med hänsyn till den fördel som vinns om kvalificerade elektroniska signaturer ges en sådan ställning att de accepteras i alla sammanhang.

7 Val av tillsynsmyndighet och finansieringen av dess verksamhet

Förslag: Post- och telestyrelsen skall utses till tillsynsmyndighet.

I lagen skall införas en bestämmelse som ger regeringen rätt att föreskriva om skyldighet för certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten att betala avgift för myndighetens verksamhet enligt lagen. Befogenheten skall kunna delegeras till myndigheten.

Som framgår av avsnitt 6.9 föreslås i promemorian att direktivets krav på ett lämpligt system för övervakning av certifikatutfärdare skall genomföras genom att en statlig myndighet ges i uppdrag att utöva tillsyn.

En möjlighet vore att inrätta en ny myndighet för den aktuella tillsynsuppgiften. Certifikatutfärdande för elektroniska signaturer är en ny verksamhet som för närvarande inte omfattas av den tillsyn som finns inom förvaltningen. En sådan myndighet skulle även kunna ta hand om andra uppgifter inom området för informationssäkerhet, som nu är spridda på flera myndigheter. Mot detta talar att kompetens på området redan har byggts upp inom dessa myndigheter. Det går vidare inte i dag att överblicka vilken omfattning tillsynsarbetet kommer att få. Det troliga är dock att det kommer att innebära en tämligen begränsad uppgift, som inte motiverar inrättandet av en ny myndighet. Det lämpliga är därför att lägga uppgiften på en befintlig myndighet.

Vid valet av myndighet bör bl.a. myndighetens vana vid hantering av tillsynsärenden och dess IT-kompetens beaktas. Vidare krävs en analys av myndighetens instruktion och karaktär. De myndigheter som nämnts i diskussionen är Finansinspektionen (FI), Post- och telestyrelsen (PTS), Patent- och registreringsverket (PRV), Riksskatteverket (RSV), Datainspektionen (DI) och Styrelsen för ackreditering och teknisk kontroll (SWEDAC).

Finansinspektionen

FI är tillsynsmyndighet för de finansiella marknaderna och arbetar inom tre huvudområden; försäkrings-, kredit- och värdepappersmarknaderna. De övergripande målen för verksamheten är att bidra till det finansiella systemets stabilitet och effektivitet samt att verka för ett gott konsumentskydd. Bank- och finanssektorn är ett område som kommit långt i användandet av elektroniska signaturer. Främst används elektroniska signaturer vid utförandet av banktjänster på Internet. FI är därigenom en myndighet som i sin dagliga tillsyn har kommit i kontakt med elektroniska signaturer. FI är en utpräglad tillsynsmyndighet med erfarenhet av tillsyn över omfattande IT-system.

Post- och telestyrelsen

PTS är central förvaltningsmyndighet med ett samlat ansvar, sektorsansvar, inom post- tele- och radioområdena. På radio- och teleområdet skall PTS främja ett effektivt telesystem och verka för att enskilda och myndigheter skall få tillgång till effektiva telekommunikationer till lägsta möjliga samhällsekonomiska kostnad.

Vidare skall PTS främja en sund konkurrens, övervaka pris- och tjänsteutvecklingen, följa den tekniska utvecklingen, pröva frågor om tillstånd och utöva tillsyn enligt bl.a. postlagen (1993:1684) och telelagen (1993:597). PTS skall följa den tekniska utvecklingen vad avser teletjänster samt tjänster på angränsande områden såsom data och media. PTS har från och med den 1 november 1999 till uppgift

att även följa utvecklingen av säkerheten vid elektronisk informationshantering.

PTS är en utpräglad tillstånds- och tillsynsmyndighet med vana att hantera tillståndsgivning av olika typer av IT-verksamheter.

Patent- och registreringsverket

PRV är central förvaltningsmyndighet för ärenden om patent, varumärken, mönster, efternamn och förnamn, samt för registerärenden angående aktiebolag, filialer och europeiska ekonomiska intressegrupperingar. Verket ansvarar också för registrering i handels- och föreningsregistret. PRV får även bedriva uppdragsverksamhet inom patent-, varumärkes-, och mönsterområdena. PRV har lång erfarenhet av att registrera aktiebolag och vana att föra omfattande register.

Riksskatteverket

RSV är central myndighet för beskattning, indrivning, folkbokföring och allmänna val. RSV skall bl.a. genom allmänna råd och uttalanden verka för lagenlighet vid rättstillämpningen inom verksamhetsområdet. RSV för bl.a. register över bolag och tilldelar organisationsnummer. RSV har hög IT-kompetens och är väl insatt i frågor kring förvaring och vidmakthållande av information under lång tid.

RSV ligger långt framme i utveckling och användning av elektroniska signaturer. Samtliga ca 14 000 tjänstemän inom RSV-koncernen använder s.k. AT-kort. RSV är sin egen certifikatutfärdare och utfärdare av kort.

Datainspektionen

DI är central förvaltningsmyndighet med uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter och för att god sed iakttas i kreditupplysnings- och inkassoverksamhet. DI skall följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik. DI är tillstånds- och tillsynsverksamhet enligt kreditupplysningslagen (1973:1173), inkassolagen (1974:182) och personuppgiftslagen (1998:204). DI har erfarenhet och teknisk kompetens på området för omfattande persondataregister.

Styrelsen för ackreditering och teknisk kontroll

SWEDAC är central förvaltningsmyndighet för teknisk kontroll och mätteknik. Det kommer att vara SWEDAC:s uppgift att i enlighet med lagen (1992:1119) om teknisk kontroll ackreditera certifieringsorgan som i sin tur kan certifiera certifikatutfärdare. SWEDAC kommer också att utse de organ som skall avgöra om säkra anordningar för signaturframställning uppfyller lagens krav. SWEDAC har lång erfarenhet av såväl egen bedömning av tekniska system som bedömning av andra organ. SWEDAC är vidare engagerat i uppbyggnaden av de europeiska systemen för ömsesidigt godtagande av provning och kontroll.

Val av myndighet

Tillsynsmyndigheten skall kontrollera att de certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten uppfyller lagens krav, innebärande bl.a. att de bedriver verksamheten med den pålitlighet som krävs och att de kvalificerade certifikaten innehåller de uppgifter som stadgas i lagen. Myndigheten skall också ingripa mot den som betecknar ett certifikat som utfärdas till allmänheten som kvalificerat, utan att de förutsättningar som ges i lagen är

uppfyllda samt utöva marknadskontroll beträffande säkra anordningar för signaturframställning.

Ingen av de ovan nämnda myndigheterna besitter idag helt den kompetens som krävs för att utföra de aktuella tillsynsuppgifterna. En förutsättning är att kompetens tillförs verksamheten och att kunskap byggs upp inom den myndighet som utses för ändamålet.

RSV hanterar person- och organisationsnummer för unik identifiering av fysiska och juridiska personer. De aktuella tillsynsuppgifterna ligger dock utanför RSV ordinarie verksamhet och ter sig tämligen artfrämmande från verkets centrala uppgifter.

DI är en utpräglad tillsynsmyndighet på data- och IT-området. Inspektionen har hög teknisk kompetens och erfarenhet av tillsyn över omfattande personregister. Certifikatutfärdarna kommer att föra register som kopplar ihop personers identitet med certifikat och står därmed under DI:s tillsyn. Den tillsyn DI bedriver är dock inriktad på hur integritetsfrågorna behandlas, och de tillsynsuppgifterna som nu är för handen ligger klart utanför myndighetens nuvarande inriktning.

PRV är främst en registreringsmyndighet och har idag inga sedvanliga tillsynsuppgifter. Att utöva tillsyn över certifikatutfärdare ligger långt i från verkets nuvarande myndighetsuppgifter.

FI är en utpräglad tillstånds- och tillsynsmyndighet som verkar på ett område som kännetecknas av en mycket hög IT-användning. Tillsynen som är i fråga gäller dock verksamhet på ett vidare område än den finansiella sektorn.

SWEDAC:s huvuduppgift att ackreditera bl.a. certifieringsorgan innebär kontroll och tillsyn av de ackrediterade organen. Praktiska skäl kan tala för att samma myndighet bör ansvara både för tillsyn över certifieringsorganen och över certifikatutfärdarna, såväl certifierade som icke certifierade. Kontrollen kan i praktiken komma att vila på internationella standarder som SWEDAC kan vara väl förtrogen med. Detta skulle dock innebära en dubbel roll för SWEDAC, som vore olämplig. SWEDAC skulle utöva tillsyn över certifikatutfärdare som är bedömda av organ som SWEDAC

ackrediterat, d.v.s. bedömt som kompetenta. En liknande dubbel roll skulle gälla beträffande marknadskontrollen.

PTS har erfarenhet av tillsynsuppgifter och övervakar redan idag den tekniska infrastrukturen som bärare av tele- och datakommunikation. Verket har sedan en tid tillbaka byggt upp såväl juridisk som teknisk kompetens på området för elektroniska signaturer. Vidare har PTS stor erfarenhet av standardiseringsarbete inom telesektorn och en god insyn i standardiseringsarbetet för elektroniska signaturer. Tillsyn över certifikatutfärdare skulle bredda PTS tillsynsuppgifter från att vara teknikinriktat till att också täcka en funktion där det förmedlade innehållet står i fokus.

En samlad bedömning leder till att PTS är mest lämpad för uppgiften att bedriva tillsyn över certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten. Myndigheten bedöms ha god teknisk och juridisk kompetens på området. Vidare är PTS den myndighet som har störst insyn i standardiseringsarbetet på området för elektroniska signaturer, vilket kommer bli viktigt i det fortsatta arbetet.

Finansiering av verksamheten

Det är naturligt att den tillsynsverksamhet som kommer att åligga tillsynsmyndigheten skall finansieras genom avgiftsuttag från dem som berörs av verksamheten och för vilka den i vissa avseenden får anses vara till nytta. Det bör därför i lagen öppnas en möjlighet för regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten, att införa ett avgiftssystem.

8 Ikraftträdande

Förslag: Lagen om vissa elektroniska signaturer m.m. skall träda i kraft den 1 januari 2001. För certifikatutfärdare som redan före ikraftträdandet utfärdar kvalificerade certifikat till allmänheten skall föreskriften om anmälningsskyldighet tillämpas först den 1 februari 2001.

Enligt artikel 13 i direktivet skall medlemsstaterna sätta i kraft de bestämmelser och lagar och andra författningar som är nödvändiga för att följa direktivet senast ett och ett halvt år efter det att direktivet har trätt i kraft. Enligt artikel 14 träder direktivet i kraft samma dag som det offentliggörs i Europeiska gemenskapernas officiella tidning, vilket kan förväntas ske runt årsskiftet 1999/2000. Det skall således vara genomfört runt halvårsskiftet år 2001. Den svenska lagen bör emellertid kunna träda i kraft redan den 1 januari 2001.

För att certifikatutfärdare som redan före ikraftträdandet utfärdar kvalificerade certifikat till allmänheten skall få rådrum att uppfylla kravet att anmäla verksamheten till tillsynsmyndigheten, bör det anges att skyldigheten inträder en månad efter det att lagen trätt i kraft.

9 Förändringar i förvaltnings- och straffrätten

Genomförandet av direktivet innebär som nämnts huvudsakligen en näringsrättslig reglering av certifikatutfärdarna. För att elektronisk kommunikation skall kunna ske i större skala inom den offentliga förvaltning torde dock dessutom krävas andra åtgärder. Avsikten är inte att i denna promemoria föreslå hur användandet av elektroniska signaturer skall främjas utöver genomförandet av direktivet. Här kan dock översiktligt nämnas det arbete som pågår (se också avsnitt 6.12).

Betänkandet Elektronisk dokumenthantering (SOU 1996:40) har nämnts vid ett flertal tillfällen. Betänkandet har lett till lagstiftning i form av lagen (1998:112) om ansvar för elektroniska anslagstavlor, men bereds i övrigt alltjämt i Justitiedepartementet. Vad gäller myndigheternas dokumenthantering innehåller förslaget, som redovisats tidigare (se avsnitt 6.3) definitioner av elektronisk handling, digital signatur etc. I den delen kan betänkandet sägas behandlas även i denna promemoria. Därutöver föreslås att det i förvaltningslagen (1986:323) införs en bestämmelse av följande lydelse.

> ”7 a § Om en bestämmelse om handläggning av förvaltningsärenden i en annan lag föreskriver att handlingar skall vara egenhändigt undertecknade eller om den föreskriver något annat som medför att elektroniska handlingar inte kan användas, får regeringen föreskriva att digitala dokument eller, när det kan anses tillräckligt, elektroniska handlingar utan digital signatur eller stämpel får användas.”

Den föreslagna bestämmelsen använder en något annan terminologi än den som används i denna promemoria och lämnar vissa

frågor olösta, exempelvis hur man skall hantera det förhållandet att 3 § förvaltningslagen stadgar att bestämmelser i annan lag eller förordning har företräde framför föreskrifter i förvaltningslagen, samtidigt som bemyndigandet i den föreslagna 7 a § syftar just till att regeringen skall få meddela föreskrifter som avviker från bestämmelser i andra lagar. Oavsett detta sätter förslaget fokus på en viktig fråga – hinder i lagstiftningen mot att elektroniska signaturer kan användas.

Såsom redogjorts för i avsnitt 4.2 och 6.12 förekommer inom förvaltningsrättens område i stor utsträckning krav på underskrift och liknande som utesluter användandet av elektroniska signaturer. I departementspromemorian Digitala signaturer – En teknisk och juridisk översikt (Ds 1998:14) diskuterades frågan om man generellt skulle föreskriva att om det i författning finns krav på underskrift eller liknande skall kravet kunna uppfyllas med vissa elektroniska signaturer. Slutsatsen i promemorian var att en sådan generellt verkande reglering inte torde vara möjlig mot bakgrund av bl.a. de olika skäl som finns bakom formkraven i olika författningar. I stället angavs att en prövning om en lagändring är motiverad bör göras i varje författning för sig bl.a. med beaktande av de syften som ligger bakom formkravet. Majoriteten av remissinstanserna delade denna bedömning. Vissa ansåg dock att frågan avfärdades alltför lättvindigt och vissa ansåg det nödvändigt med en generell likställighet genom lagstiftning.

Den föreslagna bestämmelsen, eller en bestämmelse med samma innebörd, löser visserligen inte i sig själv problemet, men kan kanske underlätta de förändringar som måste göras i de olika författningarna. Som framgått kan man knappast undgå det omfattande arbetet med att göra en inventering av befintliga författningar och överväga i varje enskilt fall om en ändring är motiverad. När behovet är klarlagt kan man dock på ett enkelt sätt genomföra nödvändiga förändringar, även om regeln ges i lag.

En naturlig utgångspunkt är att om det finns otidsenliga formkrav i författningar som omotiverat hindrar användningen av modern informationsteknik så bör dessa undanröjas. I vissa fall kan säkert domstolar och myndigheter tolka äldre formkravsregler på ett

sådant sätt att elektroniska rutiner kan användas. I andra fall saknas kanske utrymme för en sådan tolkning.

Här finns det återigen anledning att erinra om det betraktelsesätt som kan härledas ur UNCITRALs modellag om elektronisk handel (se avsnitt 4.2), dvs. funktionell ekvivalens. Det betyder således att man får analysera varje formkrav för sig och se om dess syfte lika väl kan upprätthållas med elektroniska rutiner och elektroniska signaturer.

Ett möjligt tillvägagångssätt är att låta myndigheterna själva inventera var användandet av elektronisk kommunikation skulle ge särskilt stor effekt och vad hindren i regelverket består i. Myndigheterna skulle då också kunna föreslå nödvändiga förändringar. I sammanhanget kan nämnas två uppdrag som regeringen i juni 1999 givit Statskontoret; dels att utreda behoven av åtgärder för att tillgodose kraven på säker elektronisk överföring av dokument och meddelanden till, från och inom statsförvaltningen, dels att utreda möjligheterna att upphandla elektroniskt under de s.k. tröskelvärdena, dvs. när en upphandlings låga värde medför att den inte regleras av EG-direktiven på området.

Betänkandet Elektronisk dokumenthantering innehåller vidare förslag till bestämmelser om inkommande elektroniska handlingar.

Här bör också nämnas Datastraffrättsutredningens betänkande Information och den nya informationsteknologin (SOU 1992:110). En huvudfråga för utredningen var en översyn av bestämmelserna om urkundsförfalskning. Betänkandet innehåller bl.a. en diskussion om begreppen ”urkund” och ”elektroniska dokument”.

Betänkandet bereds alltjämt i Justitiedepartementet. Här skall det bara tas upp vad gäller en för tilltron till elektroniska signaturer kanske särskilt intressant fråga, nämligen brottet ”förnekande av underskrift”.

> I 15 kap. 13 § brottsbalken stadgas att
> förnekar någon sin underskrift på urkund, dömes, om åtgärden innebär fara i bevishänseende, för *förnekande av underskrift* till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i två år.

Det kan ifrågasättas om detta straffbud har någon större praktisk betydelse. Icke desto mindre kan det vara värdefullt att markera att elektroniska signaturer kan ha samma betydelse som handskrivna underskrifter. Det ligger också i linje med direktivets krav på säkerställande av att kvalificerade signaturer ”uppfyller de rättsliga kraven på en signatur i förhållande till uppgifter i elektronisk form, på samma sätt som en handskriven signatur uppfyller samma krav i förhållande till uppgifter på papper”.

Datatraffrättsutredningen har föreslagit att det föreskrivs i brottsbalken att

> Förnekar någon sin underskrift eller sin digitala signatur på dokument, döms, om åtgärden innebär fara i bevishänseende, för *förnekande av signatur* till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år.

Även här finns olösta frågor, bl.a. om alla elektroniska signaturer enligt direktivets breda definition skall omfattas. Frågorna ger anledning till omfattande principiella överväganden och behovet av lagstiftning bör analyseras.

10 Författningskommentar

Inledande bestämmelse

1 §
I paragrafen fastställs lagens tillämpningsområde. Lagen är tillämplig på certifikatutfärdare som är etablerade i Sverige. Inga krav ställs på certifikattjänster med ursprung i andra länder. Därigenom genomförs artikel 4 i direktivet som stadgar att varje medlemsstat skall tillämpa de nationella bestämmelserna på tillhandahållare av certifikattjänster vilka är etablerade på dess territorium samt att medlemsstaterna inte får begränsa tillhandahållandet av certifikattjänster med ursprung i andra medlemsstater. Paragrafen, sammantagen med frånvaron av hindrande regler beträffande certifikat med ursprung i länder utanför den Europeiska unionen, är också i linje med artikel 7 i direktivet. Där sägs att medlemsstaterna skall säkerställa att kvalificerade certifikat med ursprung i sådana länder under vissa förutsättningar skall betraktas som rättsligt likvärdiga med certifikat som utfärdas av tillhandahållare av certifikattjänster som är etablerade inom unionen.

Definitioner

2 §
Paragrafen, som motsvaras av artikel 2 i direktivet, upptar definitioner av vissa begrepp som återkommer i lagen och har kommenterats utförligt i avsnitt 6.3.

Beträffande *elektronisk signatur* kan anmärkas att det lagtexten, liksom direktivet, inte begränsar sig till digitala data, vilket var fallet i EG-kommissionens ursprungliga förslag till direktiv. Den helt övervägande delen av den praktiska tillämpningen av elektroniska signaturer kommer emellertid under överskådlig tid att avse digitala data.

Signaturframställningsdata är vad som i det öppna nyckelsystemet (PKI) benämns den privata nyckeln.

En *anordning för signaturframställning* är den utrustning som används för att frambringa en elektronisk signatur. Anordningen använder signaturframställningsdata och kan i praktiken utgöras av t.ex. ett s.k. smart kort där signaturframställningsdata finns lagrade. När en elektronisk signatur skall framställas förs kortet in i en kortläsare som är kopplad till en datamaskin och en särskild kod skall anges. På det sättet skapas viss garanti för att den elektroniska signaturen inte kan användas utan att innehavaren av kortet är närvarande.

Signaturverifieringsdata motsvaras i det öppna nyckelsystemet av den öppna nyckeln.

För att kunna använda en elektronisk signatur i ett öppet system, såsom Internet, där parterna inte känner varandra i förväg, finns det ett behov av att parterna kan inhämta information om varandras signaturverifieringsdata (öppna nyckel). Ett *certifikat* innehåller uppgifter om vem som är innehavare av en elektronisk signatur. Certifikatet är ett elektroniskt intyg som anger sambandet mellan en undertecknares (nyckelinnehavares) identitet och dennes signaturverifieringsdata (öppna nyckel).

Kvalificerade certifikat

3 §

Bestämmelsen, varigenom artikel 2.10 i samt bilaga I till direktivet genomförs, behandlas i avsnitt 6.4.

I *andra punkten* i första stycket krävs det bl.a. att certifikatutfärdaren anger var han har hemvist. Detta har betydelse bl.a. för om certifikatutfärdaren omfattas av lagen. Dennes egna angivande av i

vilken medlemsstat han har hemvist är ett led i bedömningen av vilka nationella bestämmelser som är tillämpliga (jfr kommentaren till 1 §), vilket kan vara en viktig upplysning för den som skall förlita sig på certifikatet.

I *tredje punkten* ges möjligheten att ange undertecknaren med en pseudonym, om det framgår att det är fråga om en pseudonym. Värdet av en sådan signatur kan emellertid antas vara begränsat. Det avgörande för om en mottagare skall förlita sig på en signatur torde vara att det omedelbart framgår vem som innehar signaturen (jfr. kommentaren till 16 §).

Enligt *fjärde punkten* krävs att särskilda uppgifter om undertecknaren anges, om de är relevanta för ändamålet med certifikatet. Det kan t.ex. vara fråga om certifikat som endast skall användas för kommunikation med vissa organisationer och det är väsentlig att ange kundnummer, försäkringsnummer eller dylikt.

Kravet i *femte punkten* innebär att signaturverifieringsdata (den öppna nyckeln i PKI-lösningar) måste finnas i certifikatet. Det är alltså inte acceptabelt att den mottagare som skall förlita sig på certifikatet utöver den information han kan hämta i detta måste vända sig särskilt till certifikatutfärdaren eller någon annan för att få tillgång till signaturverifieringsdata.

I *sjätte punkten* stadgas att certifikatets giltighetstid måste anges. Av paragrafens inledning framgår också att certifikaten alltid skall vara utfärdade för en bestämd tid. Teknikutvecklingen på området kan förväntas vara fortsatt snabb och en elektronisk signatur som är säker i dag kan mycket väl inom några år inte vara skyddad mot förfalskningar på samma sätt. Det finns anledning att överväga om handlingar, där det finns behov av att säkert identifiera undertecknaren även efter det att certifikatets giltighetstid löpt ut, lämpar sig för att kommuniceras elektroniskt. Under alla förhållanden bör man i sådana fall på annat sätt dokumentera att identifiering skett (jfr. avsnitt 6.12).

Kravet i *åttonde punkten* innebär att certifikatutfärdaren skall signera certifikatet med sin avancerade elektroniska signatur. Därigenom kan den som förlitar sig på certifikatet identifiera certi-

fikatutfärdaren och avslöja om det skett några förändringar i certifikatet sedan certifikatutfärdaren signerat det (se också kommentaren till 17 §).

Enligt *andra stycket* kan regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten precisera kraven och ange hur de skall uppfyllas.

Kraven i 3 § har nära samband med skadeståndsbestämmelserna, se kommentaren till 14 §.

Säkra anordningar för signaturframställning

4–6 §§

4 § motsvarar artikel 2.6 i samt bilaga III till direktivet. 5 § motsvarar artikel 3.5 och 6 § motsvarar artikel 3.4 och delvis artikel 4.2. Genom hänvisningen bestämmelserna i lagen (1992:1119) om teknisk kontroll genomförs också artikel 11.1.b delvis. Bestämmelserna har behandlats i avsnitt 6.8.

Utfärdande av kvalificerade certifikat

7 §

I paragrafen föreskrivs en skyldighet för den som vill utfärda kvalificerade certifikat till allmänheten att anmäla detta hos den myndighet regeringen bestämmer – tillsynsmyndigheten. Detta står inte i strid med direktivets förbud mot förhandstillstånd för certifikatutfärdare. Det är inte fråga om att certifikatutfärdaren skall godkännas eller ges något tillstånd av tillsynsmyndigheten. Tillsynsmyndigheten ges endast förutsättningar att kontrollera efterlevnaden av lagen. Om anmälningsförfarandet inte fullgörs kan tillsynsmyndigheten förelägga certifikatutfärdaren att vidta rättelse, eventuellt förenat med vite. Det bör givetvis inte innebära att certifikatutfärdaren förbjuds att bedriva verksamheten.

Frågan om vilka certifikatutfärdare som omfattas av anmälningsskyldigheten behandlas i avsnitt 6.5 och 6.9.

8 §

Genom paragrafen genomförs delvis artiklarna 2.10 och 3.5 samt punkterna a, b, d, e, f, g, h och j i bilaga II till direktivet. Bestämmelsen, som innehåller krav på en sådan certifikatutfärdare som utfärdar kvalificerade certifikat, behandlas i avsnitt 6.5–6.7.

Första stycket innehåller en allmän regel om att certifikatutfärdarens verksamhet måste bedrivas med erforderlig pålitlighet.

Kraven i *första* och *andra punkten* första stycket motsvarar tillsammans med det inledande allmänna kravet i paragrafen i praktiken de krav som återfinns i befintliga standarder vad gäller ledning beträffande informationssäkerhet (se avsnitt 6.7).

Tredje punkten korresponderar med *tredje stycket* där det stadgas att sådana produkter som uppfyller vissa standarder som EG-kommissionen senare skall referera till skall presumeras uppfylla kraven i tredje punkten (jfr. avsnitt 6.5).

På vilket sätt certifikatutfärdaren skall uppfylla kravet i *fjärde punkten* varierar givetvis med vilken typ av certifikat utfärdaren tillhandahåller. Är det fråga om certifikat som kan komma att användas för transaktioner som kan innebära stora ekonomiska konsekvenser för parterna måste den ekonomiska beredskapen vara högre än om certifikaten endast kan användas för smärre transaktioner. Kravet kan exempelvis, som också anges i direktivet, uppfyllas genom att certifikatutfärdaren tecknar en lämplig försäkring.

I *femte punkten* föreskrivs en skyldighet för certifikatutfärdaren att säkert kontrollera identiteten hos den undertecknare till vilken ett kvalificerat certifikat utfärdas.

I *sjätte punkten* åläggs certifikatutfärdaren att ha ett snabbt och säkert system för registrering och spärrning av certifikat, jfr. 9 §.

Kraven i *sjunde punkten* kan delvis uppfyllas genom att certifikatutfärdaren påför certifikatet sin egen avancerade elektroniska signatur (jfr. 3 §). Andra ledet i punkten tar sikte på det fallet att certifikatutfärdaren också tillhandahåller signaturframställningsdata (den privata nyckeln). Genereringen av dessa data måste då ske på ett sådant sätt de inte röjs för obehöriga (se också andra stycket).

A*ndra stycket* tar också sikte på det fall att certifikatutfärdaren tillhandahåller signaturframställningsdata. Det är väsentligt för tilltron till elektroniska signaturer att det verkligen endast är undertecknaren som har tillgång till dessa data. Certifikatutfärdaren förbjuds därför att kopiera eller behålla dessa data.

Regeringen eller tillsynsmyndigheten kan enligt 12 § utfärda närmare bestämmelser om kraven i paragrafen.

9 §

Genom paragrafen genomförs bl.a. punkten c i bilaga II till direktivet.

Av *första punkten* framgår att certifikatutfärdaren är skyldig att omedelbart spärra ett certifikat när undertecknaren begär det eller det annars finns anledning till det, såsom när det står klart för certifikatutfärdaren att den privata nyckeln används av någon annan än den rättmätige innehavaren.

Andra punkten innebär att det skall vara möjligt att slå fast när ett certifikat är utfärdat eller spärrat. Detta kan vara av betydelse vid eventuella tvister mellan undertecknaren och mottagaren.

Det typiska fallet är att certifikatutfärdaren tillhandahåller både signaturframställningsdata och signaturverifieringsdata, exempelvis genom att utställa ett ”smart kort” där den elektroniska signaturen finns. Det är detta fall som kraven i *tredje punkten* tar sikte på. Det är då certifikatutfärdarens skyldighet att försäkra sig om att endast sådana signaturframställningsdata och signaturverifieringsdata framställs som kan användas som komplement till varandra.

Kraven i 9 § har nära samband med skadeståndsbestämmelserna, se kommentaren till 14 §.

Regeringen eller tillsynsmyndigheten kan enligt 12 § utfärda närmare bestämmelser om kraven i paragrafen.

10 §

Genom paragrafen, som behandlar certifikatutfärdarens skyldighet att registrera relevant information om ett kvalificerat certifikat samt använda tillförlitliga system för lagring av certifkat, genomförs punkterna j och l i bilaga II till direktivet.

Det inledande kravet på registrering av information syftar bl.a. till att vid rättsliga förfaranden kunna lägga fram bevis om utfärdande av certifikat. Vad som är ”rimlig tid” får avgöras med hänsyn till vilken typ av certifikat som utfärdas. Registreringen får ske elektroniskt.

Det är önskvärt att parter, som inte har något tidigare avtal om hur man skall kommunicera, kan kommunicera elektroniskt på ett säkert sätt. En metod för möjliggöra detta är att man kan hämta t.ex. en kommande avtalspartners certifikat i en öppen databas. Direktivet föreskriver emellertid att certifikatutfärdaren får göra certifikaten offentligt tillgängliga för hämtning av uppgifter endast i de fall för vilka certifikatinnehavarens samtycke har inhämtats.

Regeringen eller tillsynsmyndigheten kan enligt 12 § utfärda närmare bestämmelser om kraven i paragrafen.

11 §

Genom paragrafen genomförs punkten k i bilaga II till direktivet.

Paragrafen ålägger certifikatutfärdaren som utfärdar kvalificerade certifikat att till den som certifikatet utfärdas till ge de upplysningar som sätter denne i stånd att värdera tjänsten. Upplysningarna skall lämnas ”skriftligt”, dvs. i betydelsen ”inte muntligt”. Inget hindrar att de lämnas elektroniskt, under förutsättning att det sker på ett sådant sätt att mottagaren omedelbart kan förstå informationen och den också kan sparas av denne. Att hänvisa till en hemsida under certifikatutfärdarens kontroll, där denne från tid till annan kan ändra i villkoren, är givetvis inte tillräckligt.

Informationen skall också på begäran tillhandahållas andra, t.ex. mottagaren av en signatur baserad på certifikatet.

I paragrafen ställs inga krav utöver dem som uppställs i direktivet. Det kan emellertid inte uteslutas att det, när elektroniska signaturer börjat användas i större utsträckning, kan visa sig önskvärt att komplettera regleringen med andra föreskrifter till skydd för den som skaffar sig ett certifikat (jfr. också avsnitt 6.11.1).

Regeringen eller tillsynsmyndigheten kan enligt 12 § utfärda närmare bestämmelser om kraven i paragrafen.

12 §
Paragrafen ger regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten, möjlighet att närmare reglera kraven i 8–11 §§.

Skadestånd

Genom bestämmelserna i 13 och 14 §§ genomförs artikel 6 i direktivet. Bestämmelserna behandlas i avsnitt 6.11.

Förhållanden som inte omfattas av det särskilda skadeståndsansvaret i paragraferna, får bedömas i enlighet med den allmänna skadeståndsrätten.

13 §
I paragrafen anges vilka certifikatutfärdare som omfattas av den särskilda skadeståndsskyldighet som anges i direktivet, se närmare avsnitt 6.11.2. Det bör betonas att även certifikat som inte uppfyller kraven på ett kvalificerat certifikat, dvs. inte uppfyller kraven i 3 §, omfattas, om de utges för att vara kvalificerade certifikat.

Även certifikatutfärdare som garanterar någon annan certifikatutfärdares certifikat omfattas. Detta har samband med den särskilda möjlighet som beskrivs i artikel 7 i direktivet, nämligen att en certifikatutfärdare inom den Europeiska unionen garanterar ett certifikat som utfärdats av en certifikatufärdare som är etablerad utanför unionen.

Den skada som kan bli aktuell att ersätta enligt 13 och 14 §§ torde vara ren förmögenhetsskada. Huvudregeln vad gäller utomkontraktuella förhållanden enligt svensk skadeståndsrätt är enligt 2 kap. 4 § skadeståndslagen (1972:207) att ren förmögenhetsskada endast ersätts om skadan vållats genom brott. Enligt förarbetena till skadeståndslagen är dock inte avsikten att denna bestämmelse skall utgöra hinder för en utveckling i praxis i riktning mot ett vidgat ansvar för ren förmögenhetsskada. Som nämnts i avsnitt 6.11.1 har skadeståndsansvar för vissa felaktiga intyg godtagits i praxis sedan lång tid. De här aktuella skadeståndsreglerna är inte heller avsedda att läsas motsatsvis på sådant sätt att skade-

ståndsskyldighet för ren förmögenhetsskada enligt allmänna principer är utesluten utanför deras tillämpningsområde, t.ex. när det är en certifikatutfärdare som utfärdar ett certifikat som inte utges för att vara kvalificerat.

Se vidare avsnitt 6.11.2.

14 §

Artikel 6.1.a i direktivet stadgar att certifikatutfärdaren genom det särskilda skadeståndsansvaret svarar för att all information i certifikatet är korrekt vid tidpunkten för utfärdandet och att certifikatet innehåller alla de uppgifter som föreskrivs för ett kvalificerat certifikat. I 3 § första stycket föreskrivs vad ett kvalificerat certifikat skall innehålla. Genom att i denna paragrafs *första stycke* föreskriva att certifikatutfärdaren är skadeståndsskyldig om certifikatet innehåller felaktiga uppgifter vid utfärdandet eller inte uppfyller kraven i 3 § första stycket, täcks artikel 6.1.a i direktivet.

I artikel 6.1.b stadgas att certifikatutfärdaren svarar för att den undertecknare som anges i det kvalificerade certifikatet vid tidpunkten för utfärdandet var i besittning av de signaturframställningsdata som motsvarar de signaturverifieringsdata som anges i certifikatet. Genom 3 § första stycket 5 föreskrivs att det är certifikatutfärdarens skyldighet att se till att certifikatet innehåller signaturverifieringsdata som motsvarar de signaturframställningsdata som undertecknaren vid tidpunkten för utfärdandet har kontroll över. Motsvarar inte undertecknarens signaturframställningsdata de signaturverifieringsdata som anges i certifikatet innehåller certifikatet felaktiga uppgifter och certifikatutfärdaren är således enligt 14 § skadeståndsskyldig för den skada detta kan åsamka.

I artikel 6.1.c stadgas att certifikatutfärdaren svarar för att signaturframställningsdata och signaturverifieringsdata kan användas som komplement till varandra om certifikatutfärdaren framställer båda dessa. Genom att det genom 9 § 3 fastställs att det är certifikatutfärdarens skyldighet att, i förekommande fall, endast framställa signaturframställningsdata och signaturverifieringsdata som

kan användas som komplement till varandra, täcks även detta fall av 14 §.

I artikel 6.2 stadgas att certifikatutfärdaren också skall svara för skada som åsamkats genom underlåtenhet att registrera återkallande av certifikatet. Överträdelse av certifikatutfärdarens skyldighet enligt 9 § 1 att omedelbart spärra ett certifikat, eller 9 § 2, att säkerställa att exakt tidpunkt för när så har skett kan anges, innebär att certifikatutfärdaren kan vara skadeståndsskyldig enligt 14 §.

”Den som förlitar sig på certifikatet” är inte begränsat till mottagaren av en elektronisk signatur. Även undertecknaren, som ingått avtal med certifikatutfärdaren att den sistnämnde skall möjliggöra för undertecknaren att unikt kunna identifiera sig vid elektronisk kommunikation, kan lida skada på grund av t.ex. felaktigheter eller brister i ett certifikat. Även detta regleras i viss mån genom paragrafen. Det är således inte möjligt för certifikatutfärdaren att genom avtal med undertecknaren begränsa sitt ansvar för att en privat nyckel och en öppen nyckel som certifikatutfärdaren tillhandahållit verkligen fungerar, dvs. kan användas som komplement till varandra.

Av andra meningen i första stycket framgår att certifikatutfärdaren kan undgå skadeståndsansvar om utfärdaren kan visa att skadan inte beror på vårdslöshet hos denne. Certifikatutfärdaren har således ett s.k. presumtionsansvar med möjlighet att exculpera sig. Enligt allmänna skadeståndsrättsliga principer är det dock alltid den skadelidande som i dessa fall har att bevisa skadan och sambandet mellan skadan och exempelvis felet i certifikatet, se avsnitt 6.11.

Enligt artikel 6.3 och 6.4 i direktivet skall medlemsstaterna säkerställa att det i viss mån är möjligt för certifikatutfärdarna att genom att i certifikatet ange begränsningar för användningsområde eller transaktionsbelopp begränsa sitt skadeståndsansvar. Begränsningarna måste då vara tydliga för tredje man. Genom *andra stycket* i paragrafen regleras denna möjlighet.

I 3 § 9 anges att eventuella begränsningar måste anges i certifikatet. I förevarande paragraf anges att begränsningarna måste vara tydliga. Detta innefattar att de måste vara tydliga för den som certifikatet utfärdas till och, inte minst, för den mottagare som skall

förlita sig på certifikatet. Certifikatutfärdaren är inte skadeståndsskyldig för skada som härrör från att certifikatet använts i strid med de begränsningar som på detta sätt angivits för det.

Se vidare avsnitt 6.11.2.

Behandling av personuppgifter

15 § Genom paragrafen, som behandlas i avsnitt 6.10, genomförs artikel 8.2 i direktivet.

Personuppgiftslagen (1998:204) är tillämplig på certifikatutfärdare. I paragrafen anges i vilka avseenden begränsningarna för hur den som utfärdar certifikat till allmänheten får behandla personuppgifter är snävare än vad som stadgas i personuppgiftslagen. Bestämmelsen är inte begränsad till att avse endast den som utfärdar kvalificerade certifikat.

Rättslig verkan för elektroniska signaturer

16 §

Paragrafen behandlar rättslig verkan av kvalificerade elektroniska signaturer enligt artikel 5 i direktivet. Därvid regleras endast frågan om elektroniska signaturers verkan vid uppfyllande av formkrav för giltighet av viss rättshandling eller för att en viss förpliktelse skall anses fullgjord. Frågan om i vilken mån artikel 5 i direktivet kräver lagstiftningsåtgärder i Sverige behandlas i avsnitt 6.12.

Paragrafen innebär endast att kvalificerade elektroniska signaturer – dvs. elektroniska signaturer som uppfyller en viss säkerhetsnivå – ges en viss särställning i de fall krav på underskrift kan uppfyllas genom elektronisk kommunikation med användning av elektroniska signaturer. Bestämmelsen innebär därvid att om en kvalificerad elektronisk signatur används är alltid formkravet avseende själva signaturen uppfyllt. Det betyder alltså att högre krav inte kan ställas på den elektroniska signaturen i sig för att anse formkravet uppfyllt.

Bestämmelsen påverkar inte krav i lag eller annan författning som utesluter användning av elektroniska rutiner, oavsett hur detta har kommit till uttryck.

Paragrafen utgör inget hinder mot användning av elektroniska signaturer som inte är kvalificerade. Användningen av s.k. elektroniska dokument inom t.ex. tullområdet (jfr. avsnitt 6.3), där elektroniska signaturer som inte uppfyller denna lags krav används, påverkas inte. Inte heller utesluter paragrafen att andra formkrav för att en rättshandling skall anses giltig eller en åtgärd anses vidtagen kan uppfyllas med elektroniska signaturer som inte är kvalificerade.

Enligt direktivet skall en pseudonym kunna anges i ett certifikat. Denna möjlighet anges också i 3 §. Detta innebär givetvis inte att formkrav på underskrift vid elektronisk kommunikation kan uppfyllas genom att en pseudonym används, annat än om detta till äventyrs godtas även i övrigt.

Tillsyn

Genom tillsynsbestämmelserna genomförs direktivets artikel 3.3. Bestämmelserna har behandlats utförligt i avsnitt 6.9.

17 §

Tillsynsmyndigheten har i uppgift att övervaka att de certifikatutfärdare som utfärdar kvalificerade certifikat till allmänheten uppfyller lagens krav, inbegripet att de kvalificerade certifikaten uppfyller kraven. Däri ligger också att myndigheten skall kunna ingripa mot den som falskeligen påstår att ett certifikat är kvalificerat. Myndigheten har också att övervaka att anordningar som anges vara säkra anordningar för signaturframställning uppfyller lagens krav och är godkända av ett sådant organ som anges i 6 §.

Avsikten är att genom den statliga tillsynen bidra till att certifikat som betecknas som kvalificerade får en sådan kvalitets- och säkerhetsnivå att allmänheten, företagen och andra har förtroende för dem och för de signaturer som baseras på dem.

Någon praktisk möjlighet för myndigheten att i detalj granska varje certifikatufärdare och dennes certifikat torde inte finnas och är knappast heller önskvärd. Myndigheten kommer däremot att kunna fungera som en garant för att uppdagade missförhållanden åtgärdas.

Myndigheten kommer att kunna ta befintliga och kommande standarder till hjälp för att bedöma certifikatutfärdarnas verksamhet. Det skall dock vara möjligt att klara lagens krav utan att använda sig av de standarder som finns.

De certifikatutfärdare som certifierar sig och sina produkter kommer i många avseenden att stå under tillräcklig löpande kontroll därigenom, även om även dessa givetvis också står under myndighetens tillsyn. Tillsynsmyndigheten har också sanktionsmöjligheter som inte står certifieringsorganen till buds.

Vidare finns möjlighet för myndigheten att anlita externa konsulter. Det finns anledning att förutse förekomsten av organisationer som i och för sig kommer att ha erforderlig kompetens att certifiera cetifikatutfärdarna, men av olika skäl inte kommer att uppträda som certifieringsorgan, t.ex. revisionsbolag och datakonsultföretag. Denna kompetens bör kunna utnyttjas.

Utöver myndighetens formella befogenheter torde den kunna offentliggöra en förteckning över anmälda certifikatutfärdare och även ange vilka certifikatutfärdare som förelagts att upphöra med verksamheten eller att kalla sina certifikat för kvalificerade. En sådan förteckning skulle också kunna innehålla signaturverifieringsdata (den öppna nyckeln) för certifikatutfärdarens avancerade elektroniska signatur, som skall finnas i de kvalificerade certifikaten (jfr. kommentaren till 3 §).

18 §

I paragrafen ges myndigheten vissa befogenheter som är nödvändiga för att en effektiv tillsyn skall kunna utövas. Det kan vara fråga om att inhämta uppgifter som myndigheten anser att den behöver för att kunna bedöma verksamheten. Initiativet kan vara myndighetens eget, men det kan också ha sin grund i en anmälan till myndigheten.

Uppgifter torde i många fall kunna hämtas in formlöst vid kontakter mellan myndigheten och aktörer på marknaden. Enligt 19 och 21 §§ finns dock möjlighet för myndigheten att begära uppgifter efter föreläggande som får förenas med vite. I sista hand kan myndigheten få verkställighet hos kronofogdemyndigheten. Genom hänvisningen till utsökningsbalken blir dennas bestämmelser om bl.a. tvång i 2 kap. 17 § tillämpliga.

19 §

Paragrafen anger tillsammans med 21 § vilka sanktioner som får tillgripas av myndigheten. Den får själv bestämma när ett föreläggande skall förenas med vite. Det normala torde vara att myndigheten dessförinnan försökt få till stånd en frivillig rättelse.

I fråga om föreläggande och utdömande av vite är lagen (1985:206) om viten tillämplig.

20 §

Enligt paragrafen ges tillsynsmyndigheten möjlighet att förelägga den som utfärdar certifikat till allmänheten och påstår att det är kvalificerade certifikat, att upphöra med verksamheten. Möjligheten är således inte begränsad till att endast avse dem som anmält sig enligt 7 §. Ett sådant beslut kan givetvis i vissa fall få långtgående konsekvenser och bör därför meddelas endast sedan andra mindre ingripande åtgärder visat sig verkningslösa. Detta är inte minst viktigt med hänsyn till att ett alltför snabbt eller svagt motiverat ingripande skulle kunna strida mot direktivets förbud mot krav på förhandstillstånd.

Tillsynsmyndigheten kan, och bör, därvid föreskriva hur verksamheten skall avvecklas. Ett föreläggande skall givetvis inte avse mer än den delen av verksamheten som omfattas av tillsynen. Det väsentliga är att certifikatutfärdaren inte utan att uppfylla lagens krav påstår att till allmänheten utfärdade certifikat är kvalificerade. Det är därför naturligt att tillsynsmyndigheten koncentrerar sig på detta. Om certifikatutfärdaren väljer att fortsätta att utfärda certifikat till allmänheten, men inte längre påstår att de är kvalificerade, omfattas verksamheten inte av tillsyn enligt denna lag.

21 §
Se kommentaren till 19 §.

Avgifter

22 §
Paragrafen ger möjlighet för regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten att införa ett avgiftssystem för bekostande av tillsynsmyndighetens verksamhet, se avsnitt 7.

Överklagande

23 §
Paragrafen reglerar rätten att överklaga tillsynsmyndighetens beslut i särskilda fall enligt lagen och enligt föreskrifter som meddelats med stöd av lagen. Myndighetens beslut får överklagas till allmän förvaltningsdomstol. Krav på prövningstillstånd gäller vid överklagande till kammarrätten.