|  |  |
| --- | --- |
|  |  |
| **Rådspromemoria** |
|  |  |
| 2013-05-23 |  |
|  |  |

|  |
| --- |
| **Näringsdepartementet** |
|  |
| IT-politik |
|  |
|  |
|  |
|  |
|  |
|  |

TTE (telekom) rådet den 6 juni 2013

Dagordningspunkt 5

Förslag till Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (första behandlingen)

Interinstitutionellt ärende 2012/0146 (COD)

* lägesrapport
* meningsutbyte

 10977/12 TELECOM 122 MI 411 DATAPROTECT 73
 CODEC 1576

Dokument:

Förslaget: COM(2012) 238final

Ordförandeskapets kompromissförslag: dok 8304/13, dok 8901/13

Lägesrapport:

Tidigare dokument: 2011/12:FPM162

Tidigare behandlad vid samråd med EU-nämnden: 14 december 2012 (inför riktlinjedebatt i TTE-rådet den 20 december 2012)

Bakgrund

Det övergripande syftet med förslaget är att stärka förtroendet för och säkerheten i elektroniska transaktioner samt att undanröja rättslig fragmentering och brist på interoperabilitet på området. Avsikten är att möjliggöra ett effektivt elektroniskt samspel mellan företag, medborgare och offentliga myndigheter över nationsgränserna genom att medlemsstaterna förpliktas att ömsesidigt erkänna och godta varandras system för e-legitimationer samt elektroniska signaturer och sigill från tjänstetillhandahållare inom unionen.

Förslaget till förordning presenterades den 4 juni 2012. Förslaget har sedan dess behandlas i rådsarbetsgruppen för telekom. Det cypriotiska ordförandeskapet genomförde en riktlinjedebatt vid TTE-rådet den 20 december 2012 i syfte att inhämta medlemsstaternas ståndpunkter dels kring frågan om var insatserna bör fokuseras för att säkerställa framsteg i förhandlingsarbetet, dels kring frågan om säkerhetsnivåer för e-legitimationer. Resultatet blev att det irländska ordförandeskapet har fört fram alternativa förslag till lösningar beträffande säkerhetsnivåer. Såväl en reciprocitetsprincip som en princip med minimisäkerhetsnivåer med möjlighet till högre säkerhetsnivå i vissa fall har diskuterats. Ordförandeskapet har i ett kompromissförslag bl.a. även gjort en uppdelning av skadeståndsansvaret mellan medlemsstat och utfärdare av e-legitimationer samt gjort vissa begränsningar av förpliktelserna kring e-legitimationer. Vidare har ett kompromissförslag avseende kraven på tillhandahållare av betrodda tjänster och tillsynsbestämmelser lagts fram. I denna del har bl.a. tagits in möjlighet för tjänsteleverantörer att begränsa sitt skadeståndsansvar, införts ytterligare krav på vad som ska uppfyllas av tjänsteleverantörer samt begränsat antalet delegerade akter.

Vid TTE-rådets möte den 6 juni kommer läget i förhandlingarna om förslaget till förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden att presenteras. Medlemsstaterna inbjuds också att ange sin inställning vad avser säkerhetsfrågor för e-legitimationer, närmare bestämt om man stödjer en reciprocitetsprincip eller en princip med fastställda miniminivåer. Reciprocitetsprincipen innebär att en e-tjänst ska godta en e-legitimation från en annan medlemsstat som håller samma eller högre säkerhetsnivå än den som e-tjänsten kräver av de nationella e-legitimationerna. Den senare modellen innebär att man sätter minimikrav på säkerhet av e-legitimationer som ska accepteras av merparten e-tjänster medan det finns möjlighet för högre säkerhetsnivåer för vissa e-tjänster.

Andra principiella frågor som tas upp är

- utarbetandet av en interoperabilitetsmodell enligt vissa kriterier och samarbete mellan MS för att säkerställa interoperabilitet och säkerhet avseende e-legitimationer, vilket ska ske innan det ömsesidiga erkännandet av dessa,

- att skyldigheten att ömsesidigt erkänna e-legitimationer under en inledande period begränsas till den offentliga förvaltningens e-tjänster, medan privata e-tjänster under denna period själva kan välja att acceptera andra medlemsstaters e-legitimationer,

- teknikneutralitet avseende e-legitimationer,

- att se till att erforderliga processer för att hantera säkerhetsincidenter regleras.

Rättslig grund och beslutsförfarande

Förslaget grundar sig på artikel 114 i fördraget om europeiska unionens funktionssätt (EUF-fördraget), som rör antagandet av bestämmelser beträffande funktionen av den inre marknaden.

Beslut fattas av parlamentet och rådet i enlighet med det ordinarie lagstiftningsförfarandet (artikel 294 EUF). I rådet krävs kvalificerad majoritet.

*Svensk ståndpunkt*

Ordförandeskapets redogörelse i lägesrapporten återspeglar de diskussioner som förts i rådsarbetsgruppen för telekom.

Regeringen är övergripande positiv till förslagets ansats att reglera det ömsesidiga erkännandet av e-legitimationer och att reglera rättslig verkan och godtagande av vissa betrodda tjänster.

Det är nödvändigt att i regleringen hantera frågor om säkerhet för e-legitimationer. Regeringen anser att detta kan uppnås antingen genom att fastställa minimisäkerhetsnivåer eller genom att i förslaget ta in en princip om reciprocitet avseende vilka säkerhetsnivåer som ska godtas. Oavsett vilken lösning som väljs anser regeringen att det är en grundläggande princip att den som står risken för en verksamhet/e-tjänst också måste ha rätten att bestämma vilken säkerhetsnivå för e-legitimationer som ska krävas.

Regeringen ser i huvudsak positivt på hur förslaget i den del som berör e-legitimationer har förändrats under behandlingen i arbetsgruppen. För att få ett effektivt genomslag av den gränsöverskridande användningen av e-legitimationer behöver regleringen ta hänsyn till de system för e-legitimationer som redan utvecklats i medlemsländerna. Villkoren för möjligheten att använda och acceptera e-legitimationer över nationsgränserna måste därför vara acceptabla för medlemsstaterna. Ytterligare justeringar i regleringen kan därför komma att behövas, bl.a. förtydligande av skadeståndsansvar och hur säkerhetsaspekter garanteras. Regeringen vill också framhålla att förslagets ekonomiska konsekvenser vad avser e-legitimationer alltjämt måste analyseras och värderas i förhållande till förslagets mervärde. Detta kan komma att innebära att det ömsesidiga erkännandet av e-legitimationer kan behöva begränsas till sådana e-tjänster som har gränsöverskridande betydelse. Slutligen menar regeringen att det är viktigt att bestämmelserna avseende e-legitimationer hålls teknikneutrala för att framtidssäkra regleringen.

Beträffande de övriga principer som tas upp i lägesrapporten anser regeringen att det är en nödvändig förutsättning för det ömsesidiga erkännandet av e-legitimationer att interoperabilitets- och säkerhetsfrågor måste lösas innan medlemsstaterna kan anmäla sina system för gränsöverskridande användning. Regeringen stödjer vidare att skyldigheten att ömsesidigt erkänna andra medlemsstaters e-legitimationer begränsas till offentliga förvaltningens e-tjänster. Vad gäller skyldigheten för privata e-tjänster att i framtiden ömsesidigt erkänna e-legitimationer från andra medlemsstater bör detta – i enlighet med kommissionens förslag – vara begränsad till sådana e-tjänster där det enligt lag eller administrativa förfaranden krävs e-legitimation för åtkomst. Övriga privata e-tjänster kan på frivillig basis välja att acceptera andra medlemsstaters e-legitimationer. Villkoren för detta kan dock behöva anpassas. Slutligen anser regeringen att det är viktigt att principen om teknikneutralitet upprätthålls och att det i förordningen säkerställs att erforderliga processer för att hantera incidenter regleras.

Vad gäller de betrodda tjänsterna menar regeringen att förslaget alltjämt behöver justeras för att uppnå en lämplig avvägning mellan säkerhetskrav och kostnadsåtaganden. Regeringen avser därför att fortsatt verka för att kraven på tjänstetillhandahållare inte får vara så höga att tillträdet till marknaden försvåras för nya aktörer eller att utvecklingen av nya tjänster hindras.

Europaparlamentets inställning

ITRE respektive IMCO har presenterat förslag till betänkanden. Betänkandena kan alltjämt komma att justeras. Utskotten kommer att rösta över förslagen i juni (IMCO) respektive september (ITRE) 2013.

*Förslaget*

Förslaget är ämnat att ersätta direktivet 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer och utvidga lagstiftningen till att utöver signaturer även omfatta andra s.k. betrodda tjänster samt elektronisk identifiering. Avsikten är att stärka förtroendet för och säkerheten i elektroniska transaktioner samt att undanröja rättslig fragmentering och brist på interoperabilitet på området. Syftet är att möjliggöra ett effektivt elektroniskt samspel mellan företag, medborgare och offentliga myndigheter över nationsgränserna.

Vad avser elektronisk identifiering (e-legitimationer) reglerar förslaget inte de nationella systemen utan bygger på principen om ömsesidigt erkännande. Medlemsstaterna kan själva välja att anmäla sitt – eller sina – e-legitimationssystem för gränsöverskridande användning. Samtliga system som har anmälts måste dock accepteras av alla medlemsstater, oaktat om en medlemsstat själv valt att anmäla sitt system eller inte. Sådana e-tjänster i medlemsstaterna där e-legitimation krävs för åtkomst ska alltså acceptera samtliga e-legitimationer som har anmälts för gränsöverskridande användning av andra medlemsstater. För att kunna anmäla ett system krävs att vissa villkor är uppfyllda. Medlemsstaterna förpliktas också att samarbeta för att säkerställa interoperabilitets- och säkerhetsfrågor.

Förslaget omfattar även ett antal s.k. betrodda tjänster och de leverantörer som tillhandahåller sådana tjänster. Betrodda tjänster är bland annat elektroniska signaturer och sigill, certifikat för dessa samt till signaturer och sigill angränsande tjänster såsom validering och bevarande. Vidare omfattas elektronisk tidsstämpling, elektroniska leveranstjänster, elektroniska dokument och certifikat för autentisering av webbplatser. Förslaget reglerar b.la. organisatoriska krav, säkerhetskrav och skadeståndsfrågor för samtliga leverantörer av betrodda tjänster. Även tjänsterna som sådana regleras, om de anges vara av en viss säkerhetsnivå. Medlemsstaterna förpliktigas att erkänna och godta sådana tjänster från andra medlemsstater. Förslaget innehåller även bestämmelser om tillsyn och incidentrapportering.

*Gällande svenska regler och förslagets effekter på dessa*

Signaturdirektivet är genomfört i svensk rätt genom lagen (2000:832) om kvalificerade elektroniska signaturer, som i huvudsak reglerar kvalificerade certifikat och krav på dem som utfärdar sådana certifikat samt tillsynsregler. Enligt förslaget ska signaturdirektivet upphävas. Det medför att lagen om kvalificerade elektroniska signaturer också behöver upphävas. Vidare krävs följdändringar i ett antal författningar som hänvisar till lagen.

Ekonomiska konsekvenser

Kommissionen har gjort en konsekvensanalys av förslaget (SWD(2012) 135 final) där det bl.a. anges att förslaget är förenligt med den gällande fleråriga budgetramen och att förslaget inte påverkar budgetens inkomstsida.

För svensk del kommer förslaget att påverka kostnader för staten, tillhandahållare av betrodda tjänster och tillhandahållare av
e-tjänster (främst statliga och kommunala myndigheter). En ökad användning av elektroniska tjänster kan dock väntas medföra samhällsekonomiska vinster och kan leda till kostnadsbesparingar för såväl offentliga som privata aktörer.

Förslaget innebär att medlemsstaterna ska se till att e-legitimationer ska kunna autentiseras kostnadsfritt för förlitande parter i andra medlemsstater. Detta kommer att innebära ökade statliga kostnader för användningen av e-legitimationer. Hur stora dessa kostnader kan bli beror på transaktionsvolymen.

Förslaget innebär vidare att medlemsstaterna ska ta på sig visst skadeståndsansvar avseende sådana e-legitimationer som anmäls för gränsöverskridande användning. Detta innebär en risk att drabbas av kostnader, i den mån en förlitande part i annan medlemsstat lider skada av en brist i e-legitimationssystemet. Det är svårt att bedöma vilka budgetära konsekvenser detta skadeståndsansvar kan få.

Kostnader för att utveckla de gränssnitt och den infrastruktur som behövs för interoperabilitet mellan olika medlemsstaters e-legitimation kommer att uppstå. Dessa kostnader kommer för svensk del sannolikt framför allt att träffa tillhandahållare av e-tjänster (dvs. framför allt myndigheter). Sverige har ett stort antal tillhandahållare av e-tjänster. Den sammanlagda kostnaden för anpassning av svenska e-tjänster kan därför komma att bli hög. Kostnaden för anpassning av systemen kommer dessutom att vara beroende av vilka närmare krav som kan komma att ställas upp. Det finns idag inget tekniskt stöd för att hantera e-legitimationer utan personnummer som identifieringsverktyg.

Ökade kostnader för tillsyn kan också förutses. Det uppskattas att ytterligare tre årsarbetskrafter till tillsynsmyndigheten kan komma att behövas.

Tillhandahållare av betrodda tjänster kan drabbas av ökade kostnader bl.a. till följd av bestämmelserna om skärpta säkerhetskrav, säkerhetsrevisioner, anmälningsplikt avseende säkerhetsöverträdelser samt utvidgat skadeståndsansvar.

Övrigt