

Remissvar avseende promemorian kompletterande bestämmelser till EU-förordningen om elektronisk identifiering

Post- och telestyrelsen (PTS) har enligt 4 § 14 förordningen (2007:951) med instruktion för Post- och telestyrelsen till uppgift att utöva tillsyn enligt lagen (2000:832) om kvalificerade elektroniska signaturer (signaturlagen) samt meddela föreskrifter enligt förordningen (2000:833) om kvalificerade elektroniska signaturer. PTS lämnar med utgångspunkt från myndighetens verksamhetsområde följande synpunkter.

Angående nationella insatser i avvaktan på genomförandeakter

PTS anser att nationella initiativ som tas när genomförandeakter saknas på ett område, behöver baseras på det arbete som sker inom främst europeisk standardisering för att minska behovet av eventuella anpassningar för de fall att genomförandeakter tas fram i ett senare skede.

Sanktionsmöjligheter

Enligt förordningen ska medlemslandet säkerställa ”effektiva, proportionella och avskräckande sanktioner för överträdelser av förordningen”. Den föreslagna kompletterande nationella lagstiftningen ger tillsynsmyndigheten rätt för att begära rättelse, använda föreläggande och förbud förenade med vite. PTS menar att det kan ifrågasättas om det är tillräckligt avskräckande att sanktionerna bara kan omfatta begäran om rättelse inom rimlig tid med vite om rättelse inte görs. PTS tycker därför att sanktionerna med fördel kan kompletteras med sanktionsavgift för betydande avvikelser från bestämmelserna i förordningen.

Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter m.m.

Förslaget är att ge tillsynsmyndigheten rätt att meddela de föreskrifter som behövs. Föreskrifter kommer att behövas om kommissionen inte tar fram genomförandeakter på området. Här kan en anordning vara, t.ex. ett smart kort eller en signeringsserver. Gällande smarta kort och andra IT-säkerhetsprodukter som HSM-moduler i signeringsservrar kommer dessa troligen att vara baserade på s.k. skyddsprofiler enligt standarden Common Criteria som sedan skulle kunna användas vid krav i samband med offentlig upphandling för att stärka säkerheten. När signaturservrar används kommer skyddsprofilerna att behöva kompletteras även med administrativa regelverk gällande t.ex. loggning, inpassering, behörighetskontroller m.m.

PTS anser att skyddsprofiler bör arbetas fram i öppna standardiseringsorgan, i Europa, t.ex. inom CEN och ETSI. I Sverige används Common Criteria idag främst av försvarsmyndigheterna och i civila sammanhang i samband med generering och lagring av krypteringsnycklar i smarta kort och HSM-moduler. Det finns en önskan att öka användningen av CC evaluerade produkter även i den civila statsförvaltningen och på fler områden, se (SOU 2015:13) betänkandet, Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten. Arbeta med att ta fram skyddsprofiler i Sverige sker idag främst inom ramen för Samverkansgruppen för informationssäkerhets¹ arbetsgrupp för skyddsprofiler.

Med tanke på att det finns en existerande gruppering som arbetar med skyddsprofiler anser PTS att det inte är lämpligt att den tilltänkta tillsynsmyndigheten, e-legitimationsnämnden, i samtliga fall ensamt utfärdar de föreskrifter som behövs på området anordningar för skapande av kvalificerade underskrifter. PTS anser att nämnden är lämplig organisation för att ta fram ett administrativt regelverk för signeringsservrar. Detta med tanke på att uppgifterna påminner om de krav som kvalificerade tillhandahållare av kvalificerade betrodda tjänster granskas emot innan de kan påbörja sin verksamhet. PTS anser att MSB kan vara lämplig instans att ta fram föreskrifter som pekar ut befintliga skyddsprofiler och för att ta fram skyddsprofiler. Detta är ett väldigt specifikt kompetensområde och MSB driver en befintlig arbetsgrupp som arbetar med skyddsprofiler och de har därmed kompetens på området och de är involverade i det arbete som sker internationellt på området.

Val av tillsynsmyndighet

PTS delar bedömningen att det är ändamålsenligt att samla kompetensen på området på en myndighet. PTS ser dock en fara med att om e-legitimationsnämnden tillhandahåller tjänster som omfattas av bestämmelserna i förordningen att de också

¹ Samverkansgruppen för informationssäkerhet (SAMFI) består av ett antal myndigheter som alla har ett särskilt ansvar för samhällets informationssäkerhet.

ska bedriva tillsyn över tjänsterna. Om det blir aktuellt att e-legitimationsnämnden tillhandahåller tjänster som omfattas av förordningen tycker PTS att utförandet av tjänsterna bör placeras i annan organisation än e-legitimationsnämnden.

PTS vill i sammanhanget också framhålla att myndigheten är beredd att bidra på det sätt regeringen finner lämpligt under en övergångsperiod för att säkerställa ett skifte av ansvar och för att hålla nere överflyttningskostnader till dess tillsynsmyndigheten finns på plats.

Övergången från signaturlagen till förordningen

Tidigareläggning av ansvaret som tillsynsmyndighet enligt förordningen

Förordningen börjar gälla den 1 juli 2016. Arbetsgången enligt förordningen innebär att en tillhandahållare som vill ha status som kvalificerad respektive tillhandahålla kvalificerade betrodda tjänster från den 1 juli 2016 behöver anmäla sig till tillsynsmyndigheten före den 1 juli 2016. Det innebär att det finns behov av att tillsynsmyndigheten utses i tid alternativt ges i uppdrag att arbeta med frågan innan förordningen börjar gälla.

Övergång och överlämning av uppgifter i övrigt

En arbetsordning för en ordnad övergång och överlämning av uppgifter behöver ske innan signaturlagen upphävs och förordningen börjar gälla. Några olika aktiviteter kan identifieras, information om övergångsregler för nuvarande tillhandahållare av kvalificerade certifikat och hantering av förteckning över dessa tillhandahållare.

Det finns för närvarande tre anmälda aktörer enligt lagen om kvalificerade elektroniska signaturer. För dessa aktörer finns övergångsregler i enlighet med artikel 51 i förordningen. Det finns ett informationsbehov för dessa så att de medvetandegörs om den nya förordningen och de nya krav som börjar gälla.

PTS har som tillsynsmyndighet tillhandahållit den svenska förteckningen över utfärdare av kvalificerade certifikat i enlighet med 17§ signaturlagen. PTS har även tillhandahållit den svenska s.k. trusted list inom ramen för det s.k. tjänstedirektivet, i enlighet med kommissionens beslut 2009/767/EG². Behovet av denna förteckning torde försvinna och ersättas av den förteckning som ska tillhandahållas i enlighet med förordningen. Det behöver säkerställas att en svensk trusted list upprätthålls och publiceras även efter 1 juli 2016.

² Kommissionens beslut 2009/767/EG av den 16 oktober 2009 om åtgärder som underlättar användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden

Göran Marby

Generaldirektör

Yttrandet har beslutats av generaldirektören Göran Marby. I ärendets slutliga handläggning har även divisionschefen Catarina Wretman, avdelningschefen Annica Bergman och handläggaren Björn Scharin (föredragande) deltagit

