Post- og teletilsynet
Norwegian Post and Telecommunications Authority

Nærings- og handelsdepartementet
Postboks 8014 Dep
0030 OSLO

Vår ref.: 1204793-4 - 414.2
Vår dato: 18.12.2012

Deres ref.:
Deres dato: 13.9.2012

Saksbehandler:
Kristina Mari Rognmo

www.npt.no

Høringssvar - Europakommisjonens forslag til forordning om eID og e-signatur m.m.

Post- og teletilsynet (PT) viser til høringsbrev av 13.september 2012, hvor Nærings- og handelsdepartementet ber om høringsinstansenes syn på Kommisjonens forslag til forordning om eID og e-signatur m.m.

PT er i henhold til esignaturloven § 17, 1. ledd jf. forskrift om krav til utstedere av kvalifiserte sertifikater mv. § 8, utpekt som tilsynsorgan for registrerte sertifikatutstedere i Norge. PT er også utpekt som tilsynsorgan for utstedere som er registrert i henhold til selvdeklarasjonsordningen i esignaturlovens § 16a jf. forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere § 6.

Som norsk tilsynsmyndighet på esignaturområdet er PT deltaker i Forum of European Supervisory Authorities for Electronic Signatures (FESA). PT har gjennom sin deltakelse i FESA fått kunnskap om hvor ulikt det gjeldende esignaturdirektivet har blitt implementert i medlemslandene. Dette gjelder både i forhold til utstedelse og utstedelsesprosedyrer, bruk av elektroniske signaturer og også i forhold til nivået på gjennomførte tilsyn. PT har også kunnskap om at bruk av elektronisk signatur i mange medlemsland ikke har fått den utbredelsen som er ønsket. Dette kan bero på manglende tillit til systemet, men også dårlig brukervennlighet. I så måte vil forordningsforslaget bidra til å harmonisere det europeiske markedet, og kanskje også stimulere til økt bruk.

Regjereringens digitaliseringsprogram, som ble presentert i april 2012, understreket at kommunikasjon mellom forvaltningen og Norges befolkning som hovedregel vil være digital. PT oppfatter at det fremlagte forslag til forordning vil være en positiv bidragsyter til ivaretakelse og videreutvikling av gode løsninger for elektronisk kommunikasjon.

I tiden etter Kommisjonens offentliggjøring av forordningsforslaget har PT deltatt på ulike konferanser og workshops hvor valget av forordning som regulatorisk virkemiddel har vært kritisert. PT har ikke veldig sterke meninger om dette, men ser at en slik forordning kan være fornuftig for å oppnå økt interoperabilitet og bruk av tjenester for sikker elektronisk kommunikasjon. PT ser også at en forordning vil harmonisere nivået på tilsynsaktivitet i alle EØS land som vil kunne øke tilliten til tillitstjenester og stimulere til bruk av tillitstjenester på tvers av landegrensene. Dersom forordningen besluttes i EU, må imidlertid Norge være oppmerksom på at det for mange prosesser ikke vil være anledning å delta i og dermed vil Norge ha mindre mulighet for å påvirke ytterligere detaljerte regler på området. Dette gjelder særlig for forordningsforlagets bruk av «implemented acts», som vil kunne være en ulempe for Norge og det norske markedet.

Besøksadresse | Office address
Nygård 1 Lillesand

Postadresse | Postal address
Postboks 93, 4791 Lillesand

+47 22 82 46 00
firmapost@npt.no

Fax: +47 22 82 46 40
Org.nr: NO 974 446871

Kommisjonens forordningsforslag dekker to områder/ordninger. Dette er eID og nærmere bestemte tillitstjenester. Disse ulike områdene dekkes i forordningens kapittel II for eID og kapittel III for tillitstjenester.

Ved implementering av forordningsforslaget vil dagens esignaturdirektiv oppheves og byttes ut med forordningen som gjeldende regelverk. Dette vil også få følger for det norske regelverket med esignaturloven som hjemler utstedelse av kvalifiserte sertifikater, og også utstedelse av sertifikater etter selvdeklarasjonsordningen. PTs tilsynsoppgaver er finansiert gjennom gebyrer pålagt de som det føres tilsyn over. For utstedere av sertifikater er hjemmelen for å pålegge slikt gebyr å finne i esignaturlovens §§ 24 og 16a, jf. forskrift om krav til utstedere av kvalifiserte sertifikater mv. § 9, forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere § 14, samt forskrift av 21. februar 2005 nr. 168 om gebyr til Post- og teletilsynet § 5. For PT er det viktig at dette hjemmelsgrunnlaget videreføres i fremtidig regelverk dersom PT skal være tilsynsorgan for forordningens regulerte tillitstjenester. Dersom gjeldende norsk regelverk oppheves i forbindelse med implementeringen av forordningen, vil det måtte gjøres en ny utpeking av tilsynsmyndighet for området og det må sørges for at hjemmelsgrunnlaget for gebyrordningen videreføres.

PT er som tilsynsmyndighet forpliktet i henhold til esignaturloven § 1 til å bidra til å legge til rette for en sikker og effektiv bruk av elektroniske signaturer. Det norske markedet for utstedelse av elektroniske signaturer er i dag relativt godt etablert, og bruksområder for elektronisk signatur utvides. Per i dag er det 12 registrerte utstedere av kvalifiserte sertifikater og 11 registrerte utstedere etter selvdeklarasjonsordningen. PT er opptatt av at det norske markedet ikke skal oppleve en negativ utvikling ved implementering av forordningen med tilhørende negativ konsekvens for digitale tjenester og bruk av tillitstjenester i offentlig og privat sektor.

Gjennomgang av forordningsforslaget

PT vil i det følgende gi tilbakemelding på de ulike artikler som er presentert i forordningsforslaget. For best mulig oversikt vil forslaget gjennomgås i henhold til de ulike kapitler.

I det følgende vil kun de artikler der PT har bemerkninger og kommentarer gjennomgås og behandles.

Kapittel 1 - artiklene 1 til 4:

I forordningsforslagets **artikkel 2 nr. 2** kan det synes som at artikkelens innhold kan tolkes ut over artikkelens faktiske meningsinnhold og virkeområde. Nevnte artikkel kan leses som at forordningen ikke skal gjelde for bruk av elektroniske tillitstjenester hvor disse er basert på frivillige avtaler under privatretten, og med dette kan «alle» privatrettslige avtaler om bruk av elektroniske tillitstjenester falle utenfor. I forslagets fortale punkt 17 beskrives artikkelens meningsinnhold dit hen at det ikke foreligger en plikt til å bruke tillitstjenester utstedt under forordningen, og at to parter fritt kan avtale andre regler enn det som fremkommer i forordningen. Etter PTs mening kan det være hensiktsmessig å presisere og gjøre endringer i ordlyden gjeldende denne bestemmelsen slik at de overfor nevnte tilfellene ikke inntrer.

For **artikkel 3 nr. 6** har det blitt bemerket at forordningens definisjon av elektronisk signatur er endret i forhold til gjeldende definisjon i dagens esignaturdirektiv. I gjeldende esignaturdirektiv er elektronisk signatur definert som *""electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"*. I forordningsforslaget er det imidlertid definert som *""electronic signature" means data in electronic form which are attached to or logically associated with other electronic data which are used by the signatory to sign"*. PT har fått kunnskap om at denne endringen er en bevisst endring fra Kommisjonens side, da det etter Kommisjonens mening var noe underlig at elektronisk signatur ble definert i forhold til hva du kunne bruke denne til. I følge Kommisjonen utelukker ikke forordningsforlagets definisjon at elektronisk signatur kan brukes for autentisering, men det er ikke bruksområdet som definerer elektronisk signatur.

PT ønsker også å presisere at det i følge forslagets definisjoner kun er fysiske personer som kan bruke elektronisk signatur for signering, mens juridiske personer må benytte elektroniske segl for å forsikre opprinnelse og integritet.

Kapittel 2 – artiklene 5 til 8:

Kapittel 2 i forordningsforslaget gir bestemmelser om medlemslandenes forpliktelse for å anerkjenne andre medlemslands notifiserte eID, dersom en selv har notifisert en ordning for utstedelse av eID til Kommisjonen. I forordningsforslaget fremkommer det, i nærmere bestemt **artikkel 5, siste setning**, at notifiserte eID- ordninger *«shall be recognised and accepted»*. PT finner denne formuleringen noe uklar gjeldende hva som er forskjellen mellom *recognised and accepted*, og om det i det hele tatt er nødvendig med begge disse uttrykkene for å gi mening, da *«recognised»* etter vår mening omfatter begge situasjoner.

Kapittel 3 – artiklene 9 til 37:

I forordningens **kapittel 3, artikkel 12** gis tilbydere av tillitstjenester plikt til å tilgjengeliggjøre disse for mennesker med ulike fysiske hindringer, der dette er mulig. PT er opptatt av viktigheten med utforming av elektroniske tjenester som dekker alles behov, særlig i forhold til at utgangspunktet for fremtidig kommunikasjon mellom medlemslandenes borgere og offentlig sektor skal være elektronisk. Slik PT leser denne artikkelen skal universal utforming gjennomføres der dette er mulig. Etter PTs mening er dette en vag beskrivelse som heller gir anledning til å unnlate og gjennomføre slik utforming, og at det i artikkelen heller burde stilles krav om at tillitstjenester skal utformes og tilgjengeliggjøres i henhold til prinsipper om universal utforming.

Forordningens **artikkel 13** gir bestemmelser om tilsyn og tilsynsmyndighet. Innledningsvis, og som også tidligere nevnt, vil PT bare nevne at vår tilsynsrolle per i dag utledes fra gjeldende regelverk, og derfor vil PTs tilsynskompetanse også oppheves dersom esignaturloven ikke vil være gjeldende ved implementering av forordningen.

Gjennom forordningen gis tilsynsmyndigheten *«all supervisory and investigatory powers that are necessary for the exercise of their tasks»*. Etter PTs mening må dette spesifiseres og presiseres nærmere slik at tilsynshjemler og sanksjonsbestemmelser blir like for alle som omfattes av forordningen. Ved en formulering som dette vil det også være vanskelig for de virksomheter som er i markedet å forholde seg til hvilken tilsynskompetanse og sanksjoner som kan anvendes.

I **artikkel 13, nr 2**. har tilsynsmyndigheten ansvar for *«monitoring»* av tilbydere av tillitstjenester, for å forsikre seg om at de oppfyller de sikkerhetskrav som fremkommer i forordningens artikkel 15. Etter PTs syn burde kravene for hva som omfattes av *«monitoring»* komme tydeligere frem gjennom forordningen. PT har fått forståelsen av at dersom tilbydere av tillitstjenester er sertifisert i henhold til nærmere bestemte sikkerhetsstandarder, vil kravet om *«monitoring»* være oppfylt. Dersom dette er tilfelle burde det fremkomme tydeligere av forordningen. Forordningsforslaget presenterer et svært aktivt og strengt regime for tilsyn og revidering av utstedere av tillitstjenester. En sertifisering i forhold til sikkerhetsstandarder er kostnads- og ressurskrevende og PT er opptatt av at det skal skapes balanse mellom behov for sikre tjenester og krav til tilsyn og revisjon. Dersom det stilles unødvendig strenge krav til tilsyn, revisjoner og sertifisering kan dette få betydning for det norske og europeiske markedet og nyetablering av tilbydere av tillitstjenester.

Artikkel 13 nr. 2 bokstav c stiller krav om langtidslagring av opplysninger også etter en tilbyders avvikling av virksomheten. Lengden på denne lagringsplikten er uttrykt som *«appropriate time»,* uten noen nærmere presisering av hva dette er eller hvor lang tid dette er. Personvernhensyn tilsier kortest mulig lagringstid, mens det i dagens lov om elektronisk signatur § 14 fremkommer minst 10 år. For best mulig lik praksis i landene som omfattes av forordningen, kan det være viktig å uttrykke et minstekrav for lagring.

Et annet uttrykk som PT også finner noe uklart er begrepet *«general description of their customers»,* som fremkommer i **artikkel 13 nr. 3, bokstav c**. Dette begrepet nevnes i sammenheng med tilsynsmyndighetenes plikt om innhenting av ulik type statistikk fra tilbyderne for årlig rapportering til Kommisjonen. PT finner det noe uklart hva slags informasjon det her er snakk om og ønsker dette nærmere presisert.

Forordningens **artikkel 14** gir bestemmelser om gjensidig bistand og tverrnasjonal utveksling av god praksis og relevant informasjon mellom tilsynsmyndigheter. I henhold til artikkelens ordlyd plikter tilsynsmyndighetene i de ulike medlemsland å samarbeide med hverandre, samt gi hverandre relevant informasjon og bistand for best å kunne gjennomføre tilsynsaktiviteter. Artikkelen pålegger opplysningsplikt mellom medlemsland, men PT er usikker på hvilken betydning denne bestemmelsen får i forhold til de begrensinger i opplysningsplikten som ligger i forvaltningslovens bestemmelser om taushetsplikt.

I følge artikkelens punkt to plikter tilsynsmyndigheter å bistå hverandre, men kan avslå under nærmere gitte forutsetninger. PT synes ikke at dette er noen god løsning da det vil være uoversiktlig og en uforutsigbar forpliktelse som er vanskelig å etterkomme for tilsynsmyndighetene. Dette gjelder særlig med hensyn til ressurser og kostnader knyttet til oppgavene, og det er etter PTs mening mest hensiktsmessig at en slik bistand bør være en oppfordring og basert på frivillighet for hvert medlemsland.

Forordningens **artikkel 15** gir bestemmelser om sikkerhetskrav til tilbydere av tillitstjenester. Gjennom denne bestemmelsen pålegges utstedere av tillitstjenester å rapportere om hendelser som kan ha betydning for sikkerheten for den aktuelle tjenesten. Denne plikten er ny i forhold til tidligere regelverk, og PT mener at denne kan bidra til å øke tilliten til slike tjenester. I tillegg får tilsynsmyndighetene en mulighet til å iverksette tiltak dersom dette er nødvendig på tidligst mulig tidspunkt, noe som også vil gagne tilbyderne av slike tjenester i form av økt tillit i markedet.

I denne artikkelen gis også tilsynsmyndighetene kompetanse til å avsi vedtak for å oppnå samsvar med artikkelens punkter 1 og 2. PT savner noe mer om hvilket innhold disse vedtakene kan ha, og også er det viktig å ivareta tilbyders rettigheter i form av klageadgang for tilsynsmyndighetenes vedtak.

Artikkel 16 i forordningen gir bestemmelse om årlig tredjepartsrevisjon av tilbydere av tillitstjenester for å påse at vedkommende virksomhet oppfyller forordningen. I tillegg til dette kan tilsynsmyndighetene når som helst gjennomføre tilsyn hos tilbyderne av tillitstjenester. PT er noe usikker på om årlige revisjoner av utstedere av tillitstjenester er nødvendig. Det er dyrt, ressurskrevende og tidkrevende å gjennomføre slike tredjepartsrevisjoner, og PT er ikke overbevist om at gjennomføring av så hyppige revisjoner nødvendigvis vil gi sikrere tjenester. Også etterarbeidet av slike samsvarsrevisjoner er omfattende og ved foreslått hyppighet kan en risikere at en akkurat er ferdig med etterarbeid av en rapport da neste revisjon er i gang. Etter PTs mening vil en full samsvarsrevisjon hvert andre år kunne være tilstrekkelig. I tillegg vil det være andre aktiviteter som kan iverksettes dersom dette viser seg nødvendig, dette være seg både tilsyn utført av tilsynsmyndigheten eller vedtak fra tilsynsmyndigheten om gjennomføring av tredjepartsrevisjon. Ved for eksempel store omstruktureringer i systemer og prosesser, skal dette meldes fra om til tilsynsmyndigheten og vedkommende myndighetsorgan kan iverksette tilsyn på eget initiativ eller pålegge tredjepartsrevisjon. Hendelsen med DigiNotar i Nederland var alvorlig og fikk store konsekvenser. Med denne saken i tankene og et stadig endret trusselbilde viser viktigheten med tett kontakt og kontroll med tilbydere av tillitstjenester. Men, ut fra et norsk perspektiv tilsier erfaringen med det markedet som PT fører tilsyn med, at årlige revisjoner kan være unødvendige, mens plikter som sikrer tett dialog mellom utstedere og tilsyn er desto viktigere.

Også for **artikkel 16** har tilsynsmyndigheten kompetanse til å fatte vedtak om pålegg overfor utstedere av tillitstjenester, men heller ikke her fremkommer sanksjonsmulighetene ei heller klagerett for tilbyder.

Artikkel 17 pålegger tilbydere av tillitstjenester å sende notifikasjon til tilsynsmyndighetene med en vedlagt sikkerhetsrapport ved oppstart av drift. PT er svært positive til dette og synes at dette er en hensiktsmessig bestemmelse.

Gjeldende **artikkel 18** om Trusted List er PT noe usikker på om inntaket av denne bestemmelsen medfører at dagens Kommisjonsbeslutning 2009/767/EF og 2010/425/EF skal oppheves eller om disse kommer i tillegg til gjeldende artikkel i forordningen.

Forordningens **artikkel 20** har bestemmelser om elektroniske signaturers rettsvirkninger og aksept. I følge artikkelen kan ikke elektroniske signaturer avvises som bevis med begrunnelse om at de er elektroniske. Det finnes en tilsvarende bestemmelse i esignaturdirektivet artikkel 5 nr. 1 bokstav b, men denne bestemmelsen er ikke inntatt i esignaturloven. Slik PT leser artikkel 20 uttrykkes det ikke et krav for domstolene om å akseptere elektronisk signerte beviser, men det fremkommer at disse ikke kan avvises som bevis med begrunnelse om at de er elektroniske.

Det fremkommer videre i artikkelen at en kvalifisert elektronisk signatur har samme rettsvirkning som en håndskrevet signatur. Dersom et dokument har bestemte formkrav knyttet til signaturen, for eksempel krav om håndskrevet signatur, vil ikke en kvalifisert elektronisk signatur kunne være gyldig. Det er kun i de tilfeller der det ikke foreligger bestemte formkrav knyttet til signaturen at en kvalifisert elektronisk signatur sidestilles med en håndskrevet signatur. Etter PTs mening kan dette være en klargjørende presisering i gjeldende artikkel.

Utviklingen i det norske markedet har ikke per d.d identifisert behov for sikre signaturfremstillingssystemer for å generere kvalifiserte elektroniske signaturer jf. esignaturloven § 3 nr 3 og §§ 8 og 9. Det som brukes på det norske markedet i dag er derfor avanserte elektroniske signaturer jf. esignaturloven § 3 nr 2. Etter PTs mening dekker den foreslåtte artikkel 20 dårlig rettsvirkninger til avanserte elektroniske signaturer. Artikkelens punkt 4 uttrykker krav om anerkjennelse av signaturer på samme sikkerhetsnivå der dette er lavere enn kvalifisert elektronisk signatur, særlig i forhold til tilgang til offentlige tjenester, men artikkelen sier lite om anerkjennelse av elektronisk signatur på andre områder. Etter PTs mening bør innholdet i denne artikkelen tilsvare innholdet i dagens esignaturlov § 6, og kanskje særlig presisere avanserte elektroniske signaturers rettsvirkninger.

Også for **artikkel 28** om rettsvirkninger av elektroniske segl, er formuleringen tilsvarende den om juridisk anerkjennelse av elektronisk signatur, og PTs kommentarer gjelder tilsvarende. Ut over dette har ikke PT kommentarer til denne artikkelen.

Forordningens **artikkel 29** hjemler kravene til kvalifiserte elektroniske segl. Artikkelen henviser til kravene som fremkommer i annex III, og ved gjennomgang av denne finner PT det vanskelig å forstå punkt b og hva som menes med dette. Elektroniske segl er for signering for juridiske personer, mens det i annex III bokstav b fremkommer at det i kvalifiserte sertifikaters innhold skal være identifisering av den juridiske person ved navn og organisasjonsnummer, og for fysiske personer vedkommendes navn. Av denne grunnen er PT noe usikker på hva som menes med dette.

Også for **artikkel 32** om juridisk anerkjennelse for elektroniske tidsstempling fremkommer det at heller ikke disse kan avvises som bevis på grunn av at de er elektroniske. Dette tilsvarer PTs tidligere kommentarer til lignende bestemmelser.

Forordningens **artikkel 34** hjemler rettsvirkninger og aksept av elektroniske dokumenter. PT leser denne bestemmelsen slik at alle typer elektroniske dokumenter skal sidestilles med papirdokumenter og tillates som bevis i retten, hensyntatt dokumentets sikkerhetsnivå i forhold til autentisitet og integritet. PT finner denne formuleringen noe spesiell og ut i fra et norsk perspektiv overflødig. Norsk rett baseres på prinsippene om fri bevisførsel, herunder også elektroniske dokumenter, og hvorvidt retten vil akseptere beviset vil være opp til retten selv å bestemme.

For forordningens **artikkel 35** fremkommer det at data sendt eller mottatt ved bruk av en elektronisk leveringstjeneste skal tillates brukt som bevis i retten. PT er noe usikker på om dette kan skape problemer for norsk rett, sett hen til det ulovfestede prinsippet om fri bevisførsel.

Artikkel 36 stiller krav til kvalifiserte elektroniske leveringstjenester, og ved gjennomgang av gjeldende krav kan det, etter PTs mening, se ut som at Postens tjeneste Digipost kan omfattes av denne. Dersom Posten ønsker å registrere seg som utsteder av kvalifisert elektronisk leveringstjeneste etter at forordningsforslaget er vedtatt, vil de også omfattes av tilsyn.

Forordningens **kapitler IV og V** hjemler Kommisjonens adgang til bruk av delegerte eller gjennomføringsrettsakter. Slik PT har forstått disse, vil det for delegerte rettsakter være anledning for Kommisjonen selv til å gjøre mindre endringer som skal tjene som presiseringer/korrigeringer i forhold til nærmere bestemte artikler. For gjennomføringsrettsakter må medlemslandene delta i prosessen. Norge vil ikke ha anledning til å delta i disse beslutninger eller prosesser. Det er for ganske mange bestemmelser i forordningen inntatt Kommisjonens kompetanse for delegerte- eller gjennomføringsrettsakter, og dette gjør det i mange tilfeller utfordrende å vite hva som kan komme og hva som kan bli gjeldende for Norge, både tilsynsmyndigheter og markedet. På samme tid er prosessen med å endre en forordning tidkrevende og omfattende og på den måten kan det for enkelte mindre beslutninger være hensiktsmessig å ha mer presise bestemmelser i tilhørende regulering som vil være lettere å endre dersom dette finnes nødvendig.

<u>Generelle kommentarer til forordningsforslaget:</u>

Esignaturloven § 16a hjemler dagens adgang for blant annet selvdeklarasjonsordningen. PT er noe usikker på hvordan det blir med denne ordningen ved implementering av forordningsforslaget. Det kan synes som at selvdeklarasjonsordningens virksomhetssertifikater blir elektroniske segl, men utover dette kan ikke PT se at det foreligger ulike sikkerhetsnivåer for sertifikattjenester. Dersom det er tenkt at selvdeklarasjonsordningen fortsatt skal eksistere må også dette hensyntas i det regelverket som overtar etter dagens regelverk.

Forordningsforslaget er uklart på en del punkter som PT har forsøkt å belyse gjennom dette høringssvaret. PT er også kjent med at det ikke nødvendigvis for alle artikler er bestemt hvordan disse skal gjennomføres. Det er derfor et mål å belyse synspunkter som kan brukes i prosessen videre med forordningsforslaget som foreligger.

Samtidig er PT i hovedsak positiv til det foreslåtte forordningsforslaget, og synes at det er spennende og har et godt potensial. PT ønsker å fortsette å være tilsynsmyndighet og dersom PT blir utpekt som tilsynsmyndighet ved en implementering av forordningen, vil de tilsynsoppgaver som vi allerede utfører i dag utvides og bli av en mer omfattende karakter. PT finner dette interessant, sett hen til at det blir fastslått et akseptabelt revisjonsregime som vil bidra til økt tillit til markedet og på den måten økt bruk av tillitstjenester for sikker elektronisk kommunikasjon. Når det gjelder utføring av tilsynsoppgavene vil nok det foreslåtte revisjons- og tilsynsregimet tilsi at PT vil måtte øke bemanningen. Av denne grunnen er PT også opptatt av at de generelle bestemmelser som er å finne i dagens esignaturlov som gjelder finansiering av tilsynet, også må videreføres i det fremtidige regelverket.

Med hilsen

Post- og teletilsynet
Norwegian Post and Telecommunications Authority

Geir Jan Sundal (e.f.)
fung. direktør

Einar Lunde
avdelingsdirektør