Nærings- og handelsdepartementet
Postbox 8014 Dep
0030 Oslo

e-post: postmottak@nhd.dep.no

Thomas Myhr

Deres

Deres ref.	Vår ref.	Dato
201203327/LHW		7. desember 2012

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

Jeg har følgende kommentarer høringen.

Generelle refleksjoner med utgangspunkt i dagen situasjon

Det er på det rene at bruken av elektroniske signaturer, herunder særlig grensekryssende bruk av elektroniske signaturer, ikke har hatt den utviklingen som mange hadde forventet og at direktiv om elektroniske signaturer fra 1999 ikke heller løst disse rettslige utfordringer. Det er mange grunner til dette, hvorav de fleste også er identifisert i de dokumenter som var vedlagt departementets høringsbrev.

Etter den erfaringer man har gjort seg etter implementeringen av direktivet om elektroniske signaturer, er at hindringen og utbredelsen av elektroniske signaturer i utgangspunktet ikke ligger i den tekniske løsningen som sådan. Her finnes det flere eksempel på brukervennlige, sikre og funksjonelle løsninger – bl.a. BankID og Buypass – som viser at den tekniske løsningen er på plass. De tilbud til elektroniske signaturer som finnes på markedet i dag er normalt knyttet til et spesielt bruksområde, eller til noen få bruksområder. Her har utstederen kontroll over hele løsningen, inkludert bl.a. utstedelse, bruk, autentisering, og revokering. Disse løsningene er normalt avtalebasert der alle det er en avtalerelasjon mellom alle aktører; sertifikat-utsteder, brukersteder og bruker. Det er når en slik elektronisk signatur skal brukes innenfor andre områder, uten å være avtalebasert, og særlig i grensekryssende kommunikasjon, som problemer oppstår. Utfordringene er herunder særlig juridiske og administrative. Er den elektroniske signaturer «god nok» for den aktuelle disposisjonen? Hvordan skal brukersteder på en sikker måte kunne verifisere identiteten til «undertegner»? Selv om man i de nordiske land knytter fødselsnummer til sertifikatet, hvordan skal f.eks. et spansk brukersted kunne bruke fødselsnummeret for autentisering og hvordan skal de få tilgang til den informasjonen dersom fødselsnummeret ikke står direkte i sertifikatet? Dette er komplisert, men ikke umulig å løse. En løsning er å etablere et såkalt samtrafikknav som kan ivareta dette for de enkelte brukerstedene, som f.eks. DIFIs ID-porten og den validerings-autoritetstjenesten som Det Norske Veritas (DNV) i en periode tilbød for bl.a. grensekryssende kommunikasjon med bruk av elektroniske signaturer.

Det finnes flere private løsninger og tilbud av «trust services providers» slik det er definert i Europakommisjonens utkast til forordning. Det er viktig at ny regulering på området ikke hindrer fortsatt bruk og utvikling av slike private løsninger. En ny forordning bør som utgangspunkt ikke hindre bruk av private «trust services» så fremt disse tjenestene oppfyller de krav som måtte stilles på dem, jf. også fortalen punkt 14. I tillegg bør det være vektige grunner for å stille ytterligere krav overfor etablerte tilbydere av kvalifiserte sertifikater og kvalifiserte elektroniske signaturer. Slike nye krav vil sannsynligvis føre til omfattende revisjonsarbeid og/eller investeringer, og det er de viktig at de nye kravene gir bedre funksjonalitet for de hensyn som den nye reguleringen ønsker å ivareta. Dette må også gjelde krav som stilles på nasjonalt eID løsninger, slik at eksisterende kravspesifikasjoner ikke må revideres i mer enn hva som er absolutt nødvendig.

Kommentarer til utkast til forordning

Det noteres at Europakommisjonen ønsker å regulere dette området ved en forordning, som ikke krever nasjonal implementering. Gjennom dette ønsker Europakommisjonen å oppnå en total harmonisering i EU/EØS, noe som man ikke oppnådde med direktivet om elektronisk signatur. Det finnes gode argumenter for en slik tilnærming. Imidlertid må det noteres at reguleringsområdet i forordningen henger tett sammen med annen nasjonal regulering, herunder bl.a. adgangen til å foreta (rettslige) disposisjoner elektronisk i det hele tatt og rettsvirkningene av en underskrift, som – i henhold til forordningen – vil kunne oppfylles av en kvalifisert elektronisk signatur (artikkel 20(2)). En forordning vil således ikke garantere en full harmonisering mellom statene innenfor alle relevante områder. På et eller annet nivå vil divergerende nasjonal regulering slå inn, og som kan hindre en harmonisert bruk av elektroniske signaturer. Konsekvensen av dette bør gjøres mer tydelig. Europakommisjonen åpner også for omfattende tilleggsregulering («delegation of power» og «delegated acts») som ytterligere vanskeliggjør en total vurdering av hvilke konsekvenser forslaget vil kunne få, jf. artikkel 38. Det kan også stilles spørsmålstegn ved om Europakommisjonen skal/kan gis et slikt omfattende «mandat».

Godkjenning av en elektronisk grensekryssende identifisering vil unektelig redusere administrative kostnader og derved transaksjonskostnadene som sådanne. Dette vil gjelde ved elektronisk kommunikasjon med og i offentlig forvaltning og i privat sektor. For at dette skal fungere er det avgjørende at identifisering/autentisering er sikker og effektiv. Et av flere problemer med direktiv om elektronisk signatur er at den i utgangspunktet ikke er teknologinøytral, men er sterkt knyttet til PKI-løsninger.

I utkastet artikkel 20 reguleres rettsvirkningen av bruken av elektroniske signaturer. I artikkel 5 reguleres felles godkjenning («mutual recognition») av elektronisk identification (eID) og i artikkel 28 den rettslige effekten av bruk av elektronisk segl. Bestemmelsene skiller seg fra hverandre uten at det finnes åpenbare grunner til det.

I artikkel 20(2) sidestilles en kvalifisert elektronisk signatur med en underskrift. Her bruker Europakommisjonen det som kalles for funksjonell ekvivalens, bl.a. bruk i UNCITRALs Model Law on Electronic Commerce[1] og også i det såkalt eRegelprosjektet[2], dog uten å identifisere hvilke hensyn og andre vilkår som må ivaretas for å kunne oppnå slik sidestilling. Bestemmelsen er til sitt innhold tilnærmet identisk med direktivet om elektroniske signaturer artikkel 5(2). Det hadde imidlertid vært hensiktsmessig å klargjøre at denne sidestillingen forutsetter at det aktuelle regelverket som krever underskrift aksepterer en elektronisk signatur. Hvorvidt det skal være mulig å bruke elektroniske signaturer eller ikke styres bl.a. av nasjonal regulering og krav i direktiv om elektronisk handel artikkel 9. Som nevnt stiller artikkel 20(2) krav om bruk av kvalifisert elektronisk signatur for å oppnå nevnte sidestilling. Det stilles ikke tilsvarende krav for eID i artikkel 5. Her oppstilles det ikke noe krav til sikkerhetsnivå, og det virker ikke å være i samsvar med Europakommisjonens intensjoner, jf. fortalen punkt 13. Det er mye som taler for at krav tilsvarende de som finnes i artikkel 20(2) burde brukes i artikkel 5 for å oppnå symmetri i regelverket. På den måten vil man også ivareta det forhold at mange staters regelverk har få krav om underskrift for å oppnå ønsket rettsvirkning, men derimot betydelig fler krav om autentisering. Forskjellen mellom signering og autentisering, samt usikkerheten om begge dekkes av direktivet om elektronisk signatur har vært diskutert lenge uten at man har kommet til enighet.[3] Tilsvarende finnes det ikke en bestemmelse om funksjonell ekvivalens for segl, jf. artikkel 28.

I artikkel 27 omhandles «preservation of qualified electronic signatures». Det er uklart hvilken rettslig virkning denne bestemmelsen vil ha. Det virker som at tanken bak denne bestemmelsen er at bruken av denne type av tjenesten skal foretrekkes, dog uten at det er klart angitt hvilke positive rettslige effekter det vi føre med seg.

I artikkel 6 står at medlemsstaten skal garantere at « person identification data" er entydig knyttet til en fysisk eller juridisk person. I tillegg, i samme artikkel, påtar seg medlemsstaten et erstatningsrettslig ansvar for at nevnte forhold. Det er uklart hva som menes med "unambiguously link the person [som kan være en fysisk eller juridisk person] to the person identification data" og at staten er erstatningsansvarlig for denne koblingen. Dersom disse bestemmelsene vil føre til at det ikke er mulig – eller vanskelig – for private aktører å utstede eID (tilby «trust services providers») som dekkes av

[1] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
[2] http://tmyhr.files.wordpress.com/2011/05/prosjektrapport-16-juni-2000-ii.pdf
[3] Jf. bl.a. Myhr, T., «Regulating a European eID: A preliminary study on regulatory framework for entity authentication and a pan European Electronic ID", 31. januar 2005. http://porvoo7.fjarmalaraduneyti.is/media/Porvoo7/Thomas_Myhr.doc

forordningens regler, vil det neppe være en hensiktsmessig utvikling. Det kan her vises til hva som er nevnt ovenfor om vekten av – så langt det lar seg gjøre – å ikke stille nye krav til private aktører på markedet.

Det er mye som taler for at det er nødvendig med en omfattende revisjon av forordningen. Samtidig er det er mye som taler for at det er hensiktsmessig å forandre den eksisterende reguleringen for å oppnå en mer harmonisert situasjon vedrørende bruk av elektroniske signaturer. Det er på det rene at 1999 års direktiv om elektroniske signaturer ikke klarte å oppfylle de ønsker som Europakommisjonen og medlemslandene hadde. De tjenester som omtales som trust services i forordningen er dyre å etablere og bygger på tillit, normalt etablert under lang tid, for å bli tatt i bruk. Det er derfor viktig at den regulering som erstatter dagens direktiv vil fungere, uten å ødelegge eksisterende fungerende løsninger og uten at det fører til regulatorisk usikkerhet. Den rettslige reguleringen må nå redusere eventuell usikkerhet og bidra til å styrke det digitale interne marked. Det finnes ikke plass til å gjøre feil én gang til. Denne gang må det bli riktig.

Med vennlig hilsen

Thomas Myhr