FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Det kongelige Nærings- og Handelsdepartement
Postboks 8014 Dep
0030 OSLO

18.12.2012

SAKSBEHANDLER:	VÅR REFERANSE:	DERES REFERANSE:
Anne Karen Seip	12/9770	201203327-1/LHW
DIR.TLF:	ARKIVKODE:	
22 93 98 46	008	

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

Finanstilsynet har følgende kommentarer til utkast til forordning om eID og e-signatur COM(2012) 238 final, 2012/0146.

Til forslaget generelt

Forslaget har formuleringer som gjør det vanskelig å forstå hva som menes. Selv i dansk språkdrakt kan ordene bety noe annet i Norge. Man trenger både juridisk kompetanse og kompetanse innen IT og informasjonssikkerhet, samt kunnskap om EU-prosessene på området, for å forstå konsekvensene av forslaget.

Forslaget har på vesentlige områder generelle formuleringer og gir Kommisjonen fullmakter som det er vanskelig å se rekkevidden av over tid, jfr. artiklene 38 og 39. Det er dermed uklart for Finanstilsynet om forslaget får konsekvenser for norsk selvråderett.

Forslaget har gode intensjoner om grensekryssende samhandling og tillit, men virker uferdig. Finanstilsynet har f.eks. behov for samordnete elektroniske tjenester for autentisering, integritet og konfidensialitet. Konfidensialitet er ikke tatt med i forslaget. Underliggende standarder er ikke ferdig utviklet. Det skaper usikkerhet om hva implementering av forordningen vil medføre. At forslaget er uferdig, ble bekreftet av Policy Officer Gerard Galler fra Kommisjonen i ETSI-møtet i Berlin 29.11.12[1]. Tillit kan ikke lovfestes, men bruk av felles prosedyrer og sikkerhetsstandarder kan bidra til tillit.

I artikkel 12 foreslås det at tillitstjenester og relevante brukerprogrammer bare skal tilpasses personer med ulike funksjonshemminger. Det harmonerer ikke med den norske diskriminerings- og tilgjengelighetsloven som har strengere krav. Det vil øke det digitale skillet og ikke ivareta funksjonshemmedes rettssikkerhet.

[1] Tekst fra hans presentasjon: "Are cross-border services technically feasible? May be..."

Finanstilsynet som forvaltningsorgan

Finanstilsynet har bl.a. behov for å tilby elektroniske tjenester med signatur ved innsending av dokumenter. Tilsynet må dermed forholde seg til forordningen hvilket ser ut til å bli et unødvendig stort og kostnadskrevende elektronisk regime/opplegg.

Forordningen krever i artikkel 6 døgntilgjengelige gratis tjenester for validering av elektroniske ID-er, og nevner ikke reserveløsninger til dette. Erfaringer viser at selv tillitstjenester kan korrumperes, stoppe og gå konkurs[2]. Finanstilsynet ser behov for reserveløsninger der brukere av tilsynets tjenester trenger rask kommunikasjon.

Finanstilsynet må i hht. forslaget akseptere signaturer fra hele EØS-området. Tilsynet kan dermed se behov for å eskalere egne krav til sikkerhet for å være trygg på at signaturer fra andre land er «gode» nok. Dette kan bli aktuelt i og med at nasjonalt «godkjente» elektroniske ID-er ikke behøver å danne grunnlaget for elektroniske sertifikater fra tillitstjenestene.

Ansvar for å spesifisere sikkerhetsnivåer for elektroniske signaturer overføres til Kommisjonen i artikkel 20. Finanstilsynet kan ikke se at sikkerhetsnivåene er spesifisert eller definert. Et offentlig organ som tilbyr grenseoverskridende tilgang til elektroniske tjenester,

- må anerkjenne alle elektroniske signaturer som minst har samme sikkerhetsnivå, og
- kan ikke kreve en elektronisk signatur med et høyere sikkhetsnivå enn en kvalifisert elektronisk signatur.

Det vil sannsynligvis medføre at krav til PKI i offentlig sektor, med underliggende eksisterende standarder, må avvikles, og at verken staten Norge eller Finanstilsynet kan sette egne sikkerhetskrav høyere enn Kommisjonen bestemmer. I krisesituasjoner kan det bli et problem for tilsynet.

Tilbydere av kvalifiserte tillitstjenester kan i hht. artikkel 19 lagre informasjonen som er grunnlag for en elektronisk signatur. Finanstilsynet ser at denne bestemmelsen kan senke tilliten til utveksling av konfidensiell informasjon mellom tilsynet og dets brukere.

Tillit til elektroniske signaturer kan styrkes ved at signaturframstillingssystemer sertifiseres, men det er ikke et krav i f.eks. artikkel 23.

Ettersom identifisering av fysiske personer ikke er definert og spesifisert i forordningen nå og vil variere fra stat til stat, blir selve grunnlaget for tillit svekket. Det er motstand fra flere hold[3] om å være nødt til å akseptere andre staters eID-er. Denne underliggende uenigheten om forordningen medførte en diskusjon på møtet i Berlin om ordet *akseptere* i bl.a artikkel 1 og 7 som ikke ga avklaring. Begrepet er ikke definert. Både Galler og andre ga uttrykk for at det åpnet for ulik forståelse, definisjon og bruk av ordet. Dette gjør det uklart for Finanstilsynet om hva som må

---

[2] DigiNotar 2011, http://www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update.html..

[3] Juristen *Hans Graux*, tilknyttet Leuvenuniversitetet i Belgia skrev i *The proposend European approach to regulating eID* at det sentrale punktet om å anerkjenne eID-er fra alle EØS-land, kan bli vanskelig å akseptere for alle statene selv om det er et krav.

godtas av signerte grensekryssende dokumenter og pålogging der tilsynet er usikker på tilliten til de underliggende elektroniske tjenestene fra andre stater.

Tilsyn med finansforetaks IT-tjenester og betalingstjenester

Gjennom tilsyn med foretak og markeder skal Finanstilsynet bidra til bl.a. finansiell stabilitet. Ett grunnlag for finansiell stabilitet er trygge og sikre datasystemer. BankID utsteder nå elektroniske sertifikater som også kan benyttes mot offentlige tjenester blant annet AltInn, NAV, Skatteetaten, Lånekassen og kommunenes nettsider. Hittil har BankID hatt god kontroll med bruk som har vært utenfor banksektoren. Hvis Norge aksepterer BankID på tillitslisten (artikkel 18), kan systemer fra alle EØS-stater kreve å få tilgang til BankID for autentisering av brukere med BankID. En slik bruk der BankID skal benyttes på samme måte for bankkunder og for alle andre tjenester på internett, kan gi en konsentrasjonsrisiko som bør vurderes i forhold til finansiell stabilitet.

Den som signerer med BankID, har et teknisk krav om å laste ned Java. Forordningen sier i artikkel 6 at elektronisk autentisering skal kunne skje uten å stille bestemte tekniske krav. Det er vanskelig å se ut fra forordningens ordlyd, om BankID må gjøre vesentlige tilpasninger for å kunne komme på tillitslisten, men det er Kommisjonen som bestemmer de tekniske standardene.

Finanstilsynet ser en uklarhet hvis private aktører, som BankID, skal utstede elektroniske ID-er. Det finnes folk i Norge som ikke har bankkonto. Hva vil det innebære at personer som vil bruke en offentlig elektronisk tjeneste, må inngå avtale med en bank om økonomisk ansvar og betaling for all bruk. Validering av sertifikater skal i hht. artikkel 6 være gratis.

Langsiktige konsekvenser

Selv om Kommisjonen hittil ikke har bestemt f.eks. felles måte å identifisere fysiske personer på, så kan den godt gjøre det senere for å harmonisere praksis og styrke gjennomføringen av forordningens intensjoner. Det kan gå på tvers av norske interesser og selvråderett.

Dette kan bl.a. gjelde tilgang til offentlige elektroniske tjenester via håndholdte medier og signering i skyen (Cloud Computing). Det er ikke avklart hva slags krav som skal stilles slik at signatar får kontroll med signeringsapplikasjoner der tjenesten og lagring av f.eks. biometriske kjennetegn som skal inngå i en eID, foregår i skyen. Det mangler også krav til tilbydertjenestene.

For Finanstilsynet

Gun Margareth Moy
administrasjonsdirektør

Lone Tudborg Lakhan
seksjonssjef

Kopi: Finansdepartementet

FINANSTILSYNET
REVIERSTREDET 3
POSTBOKS 1187 SENTRUM
0107 OSLO

TELEFON: 22 93 98 00
TELEFAKS: 22 63 02 26

post@finanstilsynet.no
www.finanstilsynet.no