FNO
Finansnæringens Fellesorganisasjon

Nærings- og
handelsdepartementet
Postboks 8014 Dep
0030 OSLO
postmottak@nhd.dep.no

Dato: 19.12.2012
Vår ref.: 12-966
Deres ref.: 20120 3327/LHW

Høringsuttalelse - Europakommisjonens forslag til forordning om eID og e-signatur mm

Det vises til Nærings- og handelsdepartementets brev av 13. september 2012 der forslag til forordning om eID og e-signatur ble sendt på høring, med frist til å avgi uttalelse 1. desember 2012. FNO har gjennom e-postdialog med underdirektør Westrheim i NHD fått utsettelse med å avgi uttalelse til 19. desember 2012.

FNO ser behovet for å oppgradere dagens e-signaturdirektiv og e-signaturlov, ikke minst på bakgrunn av ønsket om at tillitstjenestene skal kunne brukes over landegrensene. Vi er også positive til at flere tillitstjenester – og leverandører av disse – lovreguleres. Vi peker for eksempel på behovet for gode og grensekryssende måter å autentisere websteder på (webstedsautentifikasjon).

FNO beklager imidlertid hvis reguleringen skjer gjennom en EU-forordning. Vanligvis blir forordninger gjort gjeldende for Norge gjennom en lov eller forskrift som sier at den angitte forordningen skal gjelde som norsk lov. Det skjer altså ingen bearbeiding eller tilpasning av bestemmelsene til norske forhold og rettstradisjon. Det er vår erfaring at reglene da blir unødvendig vanskelig tilgjengelig for norske brukere. Blant annet har vi i norsk rett – i motsetning til enkelt andre land – stor grad av formfrihet ved avtaleinngåelse og fri bevisbedømmelse ved norske domstoler. Dette innebærer at flere av de foreslåtte reglene i forordningen, blant annet om rettsvirkning av elektroniske signaturer forutsatt at disse har visse nivåer/kvaliteter samt plikt til å akseptere elektronisk signatur forutsatt bruk av tekniske løsninger, ikke passer særlig godt for norske forhold. Vi ser selvsagt fordelene med en forordning i de tilfeller harmoniseringsbehovet landene i mellom er stort. Vi mener imidlertid at det burde vært tilstrekkelig om bare de forhold som omhandles i utkastet

kapittel II om gjensidig anerkjennelse av eID, eventuelt de deler av forordningen som gjelder tilsynsbestemmelsene, hadde blitt regulert som en forordning.

Forslaget om gjensidig anerkjennelse av eID over landegrensene (kapittel II) og plikt til aksept av elektronisk signatur med angitt sikkerhetsnivå (blant annet artikkel 20) vil, så vidt vi kan forstå, medføre at dagens norske kravspesifikasjon for PKI i offentlig sektor må avvikles. Dette igjen vil blant annet få konsekvenser for hvitvaskingslovens regler om at bare elektroniske sertifikater som oppfyller kravene til sertifikatklasse Person-Høyt, kan benyttes for elektronisk legitimasjon ved etablering av kundeforhold, jf hvitvaskingsforskriften § 6. Vi mener det vil være uheldig dersom for eksempel bare eID'er utstedt av eller under ansvar av det offentlige, skal kunne benyttes for elektronisk etablering av kundeforhold etter hvitvaskingsreglene. Også eID'er utstedt av finansnæringen selv som oppfyller visse objektive krav – for eksempel norske bankers BankID – må etter vår mening også kunne brukes for elektronisk etablering av kundeforhold i finansinstitusjoner. Dette er imidlertid et spørsmål som vi går ut fra vil bli tatt opp i en eventuell egen høringsrunde om endringer i hvitvaskingsreglene og som vi forutsetningsvis vil få komme tilbake til.

Det foreslås at kommisjonen skal få svært vide fullmakter til å fastsette nærmere krav og spesifikasjoner, se utkastet kapittel IV. Slike vide fullmakter kan medføre lite forutberegnelighet og et regelverk på flere "nivåer" vil ytterligere vanskeliggjøre tilgjengeligheten for regelverket for eID og elektroniske tillitstjenester.

Vi ønsker for øvrig å gi følgende kommentarer til enkelte av artiklene i utkastet:

Artikkel 2 nr 1:
For det første regulerer utkastet til artikkel 2 nr 1 eID som er utstedt av, på vegne av eller under ansvar av offentlige myndigheter i medlemsstatene. Kravet om at det skal være av, på vegne av eller under ansvar av en medlemsstat, gjentas i artikkel 6 nr 1 bokstav a). I Norge er det i dag kun MinID som vil omfattes av dette alternativet i artikkel 2 nr 1. Dette betyr for eksempel at hvis BankID som utstedes av norske banker, bare blir brukt som "ren" eID til autentisering, ikke omfattes av forordningen. BankID vil likevel kunne omfattes dersom offentlige myndigheter og banknæringen inngår en avtale om at offentlige myndigheter påtar seg et ansvar for BankID, se mer om dette under vår kommentar til kapittel II.

Som en sidebemerkning reiser vi spørsmål om det ligger noen føringer i eller konsekvenser av at det som foreslås omfattet av artikkel 2 nr 1 er "electronic identification" ("elektronisk identifikation" i dansk versjon), altså selve prosessen å legitimere seg elektronisk, se definisjon i artikkel 3 nr 1, og ikke selve "electronic identifation means" se definisjonen i artikkel 3 nr 2.

Dernest omfatter utkastet til artikkel 2 nr 1 tilbydere av tillitstjenester. Tillitstjenester er definert i artikkel 3 nr 12. Det er for oss ikke helt klart om en "ren" eID – for eksempel dersom et elektronisk sertifikat kun inneholder autentiseringsnøkler – kan anses som en tillitstjeneste etter denne definisjonen. Det alternativet i definisjonen av tillitstjeneste som eventuelt kunne tenkes å omfatte eID, er elektronisk sertifikat, se her definisjonen i artikkel 3 nr 10. Et sentralt element i definisjonen av sertifikat er imidlertid knytningen av valideringsdataene til en elektronisk signatur. Dette i motsetning til dagens e-signaturdirektiv og norsk e-signaturlov som definerer en elektronisk signatur som en autentiseringsmetode, altså også en eID. Vi oppfatter derfor at forordningsutkastets definisjonen av elektronisk signatur i artikkel 3 nr 6 er snevrere enn dagens e-signaturdirektiv da den nye definisjonen forutsetter at sertifikatet skal brukes for å "skrive under" (engelsk "to sign"). Vår antagelser er derfor at begrepet elektroniske tillitstjenester ikke omfatter eID.

Ovenstående betyr blant annet at utkastet til forordning artikkel 2 nr 1 ikke omfatter BankID brukt som eID. Derimot omfattes BankID brukt som signering. Vi kan heller ikke se at forordningen vil gjelde for elektroniske sertifikater som kun inneholder krypteringsnøkler som bare skal brukes til å beskytte innholdet i meldingen mot innsyn fra uvedkommende.

Konsekvensen av ovenstående forståelse er blant annet at det i forordningsutkastet ikke stilles noen konkrete krav til legitimasjonskontrollen ved utstedelse eID. Utkast til artikkel 19 gjelder jo "bare" for tillitstjenester – som (vi oppfatter) ikke omfatter eID. Det blir i så fall bare artikkel 6 nr 1 bokstav c som helt generelt sier at medlemsstaten "sikrer" (engelsk "ensures") rett identitet.

Artikkel 2 nr 2:

Vi er usikre på hva det innebærer at forordningen ikke skal gjelde levering av elektroniske tillitstjenester på grunnlag av frivillige avtaler basert på privatrettslige regler. I BankID-samarbeidet har vi "alltid" hevdet at BankID er en avtalebasert PKI-tjeneste, det vil si at så vel underskriver som signaturmottaker må ha en (ramme)avtale med en utsteder av BankID for å kunne benytte BankID. Selv om det ikke tydelig står, synes flere av bestemmelsene i utkastet å forutsette at en signaturmottaker alltid skal ha rett til få validert en eID eller sertifikatet som er benyttet for å skape en elektronisk signert melding, uansett om vedkommende har en (ramme)avtale om dette med sertifikatutsteder eller ikke. I fortalen punkt 17 står blant annet at selve avtaleinngåelsen ved bruk av sertifikatet ikke omfattes av forordningen, noe som er nokså selvsagt. Det er imidlertid ikke dette forholdet som foreslås regulert i artikkel 2 nr 2.

Vi ser selvsagt gode grunner for å unnta fra forordningen tilfeller der en aktør utsteder en form for avansert påloggingsmekanisme eller lignende som kun skal brukes på utsteders eget brukersted, eventuelt på noen svært få andre steder, altså unntak for såkalte "lukkede"

tillitstjenester som bare tilbys til en begrenset krets. Vi hadde forstått det dersom det var dette forholdet man ønsket å unnta i artikkel 2 nr 2. Slik forslaget er utformet, kan det derimot ses som at norske bankers BankID (også den delen som benyttes for å skape digitale signaturer) vil være unntatt fra hele forordningen.

Artikkel 3

Nr 6; vi oppfatter, som foran nevnt, forslaget til definisjon av elektronisk signatur til å være snevrere enn i gjeldende e-signaturdirektiv. I gjeldende direktiv (og norsk e-signaturlov) omfatter definisjonen av elektronisk signatur også autentiseringsmetoder, for eksempel pin-kode, noe vi ikke oppfatter er tilfellet i forordningsutkastet.

Nr 12; som nevnt foran under vår kommentar til artikkel 2 nr 1, er vi usikre på om begrepet "tillitstjeneste" skal omfatte eID.

Kapittel II - Artikkel 5 til 8

Dette kapittelet foreslås å gjelde eID utstedt av, på egne av eller under ansvar av nasjonal myndighet. I Norge vil således MinID omfattes. Utkastets artikkel 5 om plikt til gjensidig anerkjennelse, foreslås bare å gjelde for en slik offentlig/nasjonal eID som brukes mot brukersted tilhørende offentlig myndighet/etat. Vi oppfatter kapittelet som et godt initiativ for å skape mulighet for grensekryssende bruk.

Et naturlig spørsmål er i hvilken grad et for en privatutstedt eID skal kunne omfattes av kapittel II og registreres som nevnt i utkastet til artikkel 7 og dermed falle inn under bestemmelsen om gjensidig anerkjennelse i artikkel 5. Vi legger til grunn at det i begrepet under ansvar av vedkommende medlemsstat i artikkel 6 nr 1 bokstav a), ligger at medlemsstaten må påta seg fullt ansvar etter artikkel 6 for den privatutstedte eID, herunder fullt erstatningsansvar i samsvar med utkastet til artikkel 6 nr 1 bokstav e) om at eID'en er utstedt til rett person, for at det finnes et velfungerende valideringssystem osv.

Vi mener – som også nevnt innledningsvis - at forvaltningens kravspesifikasjon for PKI i offentlig sektor og det risiko-/sikkerhetsklassifiseringssystem som er bygd opp etter dagens e-signaturlov § 16a ikke kan videreføres med de bestemmelser som fremgår av utkastet kapittel II.

Som også nevnt foran, kan vi ikke se at det i forordningsutkastet stilles noen konkrete krav til legitimasjonskontrollen ved utstedelse eID. Utkast til artikkel 19 der det blant annet stilles krav om personlig fremmøte, gjelder jo "bare" for tillitstjenester – som (vi oppfatter) ikke omfatter eID. Den eneste bestemmelsen om legitimasjonskontroll for utstedelse av eID blir i så fall artikkel 6 nr 1 bokstav c som helt generelt sier at medlemsstaten "sikrer" (engelsk "ensures") rett identitet.

Artikkel 9
Det hefter flere uklarheter ved forordningsutkastets ansvarsbestemmelse. For det første vil det ofte være svært vanskelig å avgjøre om en taps- eller skadevoldende situasjon er oppstått på grunn av brudd på en eller annen bestemmelse i et til dels uklart og i stor grad skjønnspreget forordingsregelverk. Videre er det ikke entydig hvilket økonomisk tap som faller inn under begrepet "direkte" skade. Vi antar blant annet at "bakgrunnsjussen" med hensyn til hva som anses som "direkte" skade vil variere fra land til land.

Det er videre uklart for oss om utkastet vil innebære at det ikke er mulig for en sertifikatutsteder å beløpsbegrense sitt erstatningsansvar. I dagens ordning kan utsteder av kvalifiserte sertifikater beløpsbegrense sitt erstatningsansvar tilsvarende en i sertifikatet angitt bruksbegrensning. Vi legger blant annet merke til at det i vedlegg I til forordningsutkastet, som stiller krav til kvalifiserte sertifikater, ikke foreslås at det i sertifikatet kan oppføres beløpsbegrensninger for sertifikatets bruk, slik det er i dagens e-signaturdirektiv. I følge begrunnelsen innledningsvis i forordningsutkastet, er kravet om beløpsbegrensning fjernet fordi den likevel ikke fungerte i praksis.

Vi vil sterkt understreke behovet for en sertifikatutsteder til å kunne beløpsbegrense sitt ansvar. Dette har alle norske utstedere av PKI-sertifikater gjort i dag. Uten mulighet for å beløpsbegrense ansvaret, vil utstederne måtte gjøre betydelige risikopåslag som vil kunne medføre priser for bruk av elektroniske tillitstjenester som i hvert fall ikke vil fremme økt bruk av disse.

I denne sammenheng merker vi oss at utkast til artikkel 19 – som det henvises til fra artikkel 9 nr 2 – forutsetter at det overfor brukeren av tillitstjenesten skal angis vilkår for bruk av tjenesten, se artikkel 19 nr 2 bokstav c). Vi reiser spørsmål om denne bestemmelse vil kunne hjemle eventuell avtale om ansvarsgrenser. I så fall vil slike beløpsgrenser forutsetningsvis måtte avtales uten at det angis i sertifikatet.

Artikkel 10
Det virker ikke logisk at kvalifiserte tillitstjenester og kvalifiserte sertifikater nevnes som alternativer når en tillitstjeneste ifølge definisjonen også omfatter sertifikater, se definisjonen i utkast til artikkel 3 nr 12.

Artikkel 11
I nr 2 foreslås at tillitstjenesteyter kun skal registrere et minimum av personopplysninger. Vi peker her på behovet for løpende å registrere en del informasjon om bruk av elektroniske sertifikater for hele tiden å sikre mot uberettigede personers misbruk. Det kan således være aktuelt for en usteder å registrere opplysninger som identifisere den IP-adresse som underskriver benytter til tillitstjenesten, brukeradferd (for eksempel "tastebiometri"), avvik fra normalt brukermiljø og datamaskinens tilstand (for eksempel om det benyttes

oppgradert programvare) mv. Vi forutsetter at forslaget ikke er til hinder for registrering av slike opplysninger til nevnte formål. Vi antar videre at "programerklæringen" i nr 2 strengt tatt ikke vil rekke lengre enn det som følger av personverndirektivet, og vi skulle derfor blant annet av regeltekniske grunner ønsket at man nøyde seg med å henvise til personverndirektivet.

I nr 4 åpnes det for å bruke psevdonym på innehaver. Vi forutsetter at det er fritt opp til den enkelte tilbyder om vedkommende ønsker å akseptere bruk av psevdonym for tillitstjenester vedkommende leverer.

Artikkel 12

Vi reiser spørsmål om forslaget om universell utforming også vil innebære at utsteder av kvalifiserte sertifikater må etablere en ordning der utsteder eller en representant for denne må møte opp hos en kunde som ikke er i stand til å bevege seg utenfor sitt eget hjem, for å oppfylle kravet om fysisk fremmøte i artikkel 19 nr 1 bokstav a). Vi finner det ellers underlig at kravet om universell utforming bare foreslås å gjelde for tillitstjenester og ikke også for utstedelse av "rene" eID'er (se vår forståelse av utkastet til artikkel 2 nr 1).

Artikkel 16

I nr 1 forutsettes at et anerkjent og uavhengig organ hvert år skal foreta en kontroll av kvalifiserte tillitstjenesteytere. Dette må antas å være unødvendig ofte, og vil etter vår mening innebære forholdsvis store merkostnader og dermed fordyre tjenestene. Man bør isteden stille nærmere krav til utsteders egenkontroll og internrevisjon samt at det kan fremlegges dokumentasjon for dette.

Artikkel 18

Hver medlemsstat skal offentliggjøre lister over kvalifiserte tillitstjenesteytere som medlemsstaten "har ansvar for" (dansk oversettelse). Vi legger til grunn, blant annet ut fra den engelske teksten "for which ..[the Member State] is competent", at det her menes tjenesteyter som vedkommende medlemsstat har tilsynsansvar overfor.

Artikkel 19

Etter utkastet til artikkel 19 nr 1 annet ledd bokstav a) forutsettes at ved utstedelse av et kvalifisert sertifikat (for elektroniske signaturer eller segl), skal identitetskontroll skje ved fysisk fremmøte.

Som antydet foran under våre kommentarer til utkast til artikkel 2 nr 1, vil vår antakelse om at tjenesteytelser ikke omfatter utstedelse av eID, innebære at denne bestemmelse ikke vil få anvendelse på utstedelse av rene eID'er.

Etter dagens norske regler vil det være tilstrekkelig at vedkommende har møtt personlig fram for utsteder av kvalifiserte sertifikater på et tidligere tidspunkt enn ved selve utstedelsen, for eksempel i forbindelse med etablering av kundeforholdet i banken, se e-signaturforskriften § 7. Dette er en meget praktisk situasjon, og vi forutsetter at den foreslåtte regelen ikke er til hinder for at denne praksisen videreføres. Vi forutsetter videre at ved reutstedelse av et sertifikat, eventuelt ved en "oppgradering" av et sertifikat, for eksempel overgang til annet lagringsmedium for krypteringsnøkler, behøver kunden heller ikke møte personlig fram på nytt.

I nr 1 annet ledd bokstav b) foreslås at legitimasjonskontroll av mottakere av kvalifiserte sertifikater også kan skje uten personlig fremmøte dersom det benyttes en eID som er "notified" ("anmeldt" på dansk). Vi antar dette må leses slik at det kun kan benyttes en eID som er registrert etter reglene i artikkel 6 og 7, altså en eID utstedt av, på vegne av eller under ansvar av offentlig myndighet.

Det foreslås videre i nr 1 bokstav b) at den eID som skal benyttes for elektronisk legitimasjon for utstedelse av et kvalifisert sertifikat, må være utstedt på grunnlag av personlig fremmøte. Dette leser vi slik at dersom en eID er utstedt uten personlig fremmøte (slik som MinID er) eller på grunnlag av en annen eID (altså elektronisk legitimasjonskontroll), ikke kan benyttes for formålet. Vi er tvilende til om det lar seg gjøre for sertifikatutsteder å kontrollere om den eID som benyttes er utstedt på grunnlag av personlig fremmøte.

Selv om utkastet åpner for å utstede et kvalifisert sertifikat på grunnlag av elektronisk legitimasjon, forutsetter vi at den enkelte tjenesteyter selv må avgjøre om dette er ønskelig for sine sertifikater. For eksempel er det i reglene for norske bankers BankID bestemt at en BankID ikke kan utstedes på grunnlag av en elektronisk legitimasjon.

Artikkel 20

I nr 3 foreslås at kvalifiserte sertifikater for elektroniske signaturer skal anerkjennes i alle medlemsstater. Vi er usikre på rekkevidden av en slik "programerklæring". Er dette først og fremst ment som et påbud rettet bare mot medlemsstatens lovgivning, eller er det ment som et direkte påbud til private elektroniske brukersteder som dermed pålegges å akseptere signaturer skapt med alle kvalifiserte sertifikater utstedt i EØS-området? Vi antar at det er førstnevnte forståelse som må legges til grunn.

I nr 4 foreslås at dersom det kreves elektronisk signatur med lavere sikkerhetsnivå enn kvalifisert elektronisk signatur, skal alle elektroniske signaturer med minst samme sikkerhetsnivå anerkjennes og aksepteres. Vi merker oss ellers at forslaget er generelt utformet til å omfatte alle brukersteder, samtidig som det henges på at dette gjelder særlig (i den engelske versjonen "in particular", i den danske versjonen "navnlig") offentlige organers online-tjenester. Igjen er vi usikre på om dette er et påbud rettet mot

medlemsstatens lovgivning eller mot den enkelte borger/bedrift. I sistnevnte tilfelle skulle dette satt på spissen for eksempel bety at en bank som tilbyr sine kunder å inngå låneavtaler elektronisk i nettbanken med BankID, må akseptere alle andre løsninger for elektronisk signatur med samme sikkerhetsnivå som BankID. Et annet eksempel – signering av selvangivelse kan skje med sertifikat Person-Standard. Må da skatteetaten akseptere alle elektroniske signaturer med sikkerhetsnivå over dette, det vil si også BankID – og i så fall selv uten at Difi og BankID Norge hadde inngått avtale om bruk av BankID i ID-porten? Dette antar vi ikke kan være riktig forståelse av forslaget, selv om fortalen punkt 46 for så vidt støtter en slik forståelse hva gjelder det offentlige som mottaker av signerte dokumenter.

Vi er – som også nevnt innledningsvis - også usikre på i hvilken grad forvaltningens kravspesifikasjon for PKI i offentlig sektor og det risiko-/sikkerhetsklassifiseringssystem som er bygd opp etter dagens e-signaturlov § 16a kan videreføres med de bestemmelser som fremgår av artikkel 20.

Artikkel 22 til 27
Disse bestemmelsene regulerer eller stiller krav til kvalifiserte elektronisk signaturer, altså der det i tillegg til kvalifisert sertifikat er benyttet et kvalifisert system til generering av elektroniske signaturer. Dette er et sikkerhetsnivå som vi ikke har noen erfaring med og vi er dermed usikre på konsekvensen av denne reguleringen.

Artikkel 28
Til nr 3 og 4 har vi samme kommentar som til artikkel 20 nr 3 og 4, se over.

Med vennlig hilsen
for FNO

Gunnar Harstad
fagdirektør