



Nærings- og fiskeridepartementet

Postboks 8090 Dep
0032 OSLO

NATIONAL POLICE DIRECTORATE

Deres referanse:
15/4361

Vår referanse:
201504583-17

Sted, Dato
Oslo, 02.05.2016

HØRING - GJENNOMFØRING AV EUS FORORDNING OM ELEKTRONISK IDENTIFISERING (EID) OG TILLITSTJENESTER FOR ELEKTRONISKE TRANSAKSJONER I DET INDRE MARKED

Politidirektoratet viser til høringsbrev datert 30. november 2015 fra Nærings- og fiskeridepartementet om gjennomføring av EUs forordning om elektronisk identifisering (eID) og tillitstjenester for elektroniske transaksjoner i det indre marked (eIDAS). Høringsfristen var i høringsbrevet fastsatt til 1. mars 2016. Politidirektoratet er imidlertid i e-post fra Justis- og beredskapsdepartementet 15. februar 2016 underrettet om utsettelse av svarfristen.

Politidirektoratets (POD) IDeALT-program har fulgt arbeidet med eIDAS i lang tid og har deltatt både i ekspertgrupper på EU-nivå og i norske referansegrupper. eIDAS er meget relevant for IDeALT-programmet ettersom regjeringen 18. april 2016 vedtok at eID på nasjonalt ID-kort skal realiseres. Dette vil bli en løsning med eID på høyeste sikkerhetsnivå og vil inkludere kvalifisert personsertifikat, samt løsning for kvalifisert signatur. POD har også som mål at eID på nasjonalt ID-kort notifiseres i henhold til eIDAS på høyeste nivå for bruk mot utenlandske tjenester.

For politiet som tilbyder av tjenester på nett er også eIDAS relevant. POD anser at flere av politiets nåværende og fremtidige tjenester må være tilgjengelige for brukere med utenlandsk eID i henhold til eIDAS. Det er også sannsynlig at politiet vil tilby tjenester som krever avansert elektronisk signatur, og dermed må kunne akseptere tilsvarende signaturer fra borgere i andre EØS-land.

eIDAS' formål er å tilrettelegge for handel og tilgang til tjenester på tvers av landegrenser. I utgangspunktet anser politiet dette som positivt, men det er viktig for POD å poengtere at risikoen for svindel og potensial for misbruk da også øker siden forordningen åpner opp for nye og mer avanserte metoder å kommunisere enn dagens praksis.

Generelle merknader

POD støtter høringsnotatets hovedkonklusjon om innføring av eIDAS med gjennomføringsrettsakter i norsk lov og har ingen kommentarer til den foreslåtte lovteksten. POD støtter også at esignaturloven kan og bør oppheves ved innføringen av eIDAS i norsk lov.

Politidirektoratet

POD har imidlertid en rekke merknader til innholdet i høringsnotatet. Etter PODs mening er konsekvenser av innføringen av eIDAS meget svakt beskrevet. For å muliggjøre bruk av andre lands eID mot offentlige tjenester i Norge er en rekke tiltak nødvendige, spesielt i tilknytning til ID-porten og Folkeregisteret. Disse er i altfor liten grad omtalt. Økonomiske og administrative konsekvenser er i liten grad utredet, og spesielt er ikke konsekvenser for norske tjenesteeiere berørt. Vi savner også vurderinger knyttet til risiko for alle berørte parter, samt beskrivelse av mulige tiltak mot og oppfølging av svindel og misbruk.

POD mener dessuten at høringsnotatets tolkning av eIDAS på en del områder er mangelfull og til dels direkte misvisende. Merknadene gis i det følgende med henvisning til punktene i høringsnotatet. Vi håper at vårt hørings svar kan gi innspill som har verdi for det videre arbeidet.

Høringsnotatet pkt. 1 Hovedinnholdet i høringsnotatet

POD har ingen kommentarer til dette punktet.

Høringsnotatet pkt. 2 Bakgrunn

POD har ingen kommentarer til dette punktet.

Høringsnotatet pkt. 3 Gjeldende rett

I avsnitt 3.2 står det at «PKI-løsninger som benyttes i offentlig virksomhet», skal oppfylle Kravspesifikasjon for PKI i offentlig sektor. POD påpeker at det er viktigere i denne sammenhengen at dette kravet også gjelder for PKI-løsninger som benyttes for tilgang til offentlige tjenester på nett.

I avsnitt 3.3 står det at ID-kortloven åpner for å utstede ID-kort til EØS-borgere. Det korrekte er at lovens § 14 andre ledd bokstav b åpner for å gi forskrift om «utenlandske statsborgeres rett til å få nasjonalt ID-kort, blant annet om særlige vilkår om tilknytning til Norge». Dette gjelder med andre ord utenlandske statsborgere generelt og ikke bare EØS-borgere.

Høringsnotatet pkt. 4 Arbeidet med regelverket i EU og Norge

POD har ingen kommentarer til dette punktet.

Høringsnotatet pkt. 5 Gjennomføring av regelverket

POD har ingen kommentarer til dette punktet.

Høringsnotatet pkt. 6 Formål og virkeområde

POD er enig i at reglene ikke bør anvendes på lukkede systemer. En kan vurdere om ikke bare virksomhetsinterne, men også sektorinterne løsninger kan sies å være «lukkede systemer», for eksempel løsninger innen helse- og omsorgssektoren eller internt i offentlig sektor.

POD antar at reglene ikke vil komme til anvendelse for systemer som er omfattet av sikkerhetsloven.

Høringsnotatet pkt. 7 Elektronisk identifisering

I avsnitt 7.1 presenteres det to alternative tolkninger for rekkevidden av anerkjennelsesplikten som gis av eIDAS artikkel 6. POD anser det som avklart og uomtvistelig at det er alternativ 2

som gjelder, det vil si at *norske myndigheter vil være pliktige til å akseptere andre EØS-lands notifikerte eID-løsninger for tilgang til offentlige tjenester uavhengig av om Norge selv velger å notifikere eller ikke*. POD stiller seg undrende til at alternativ 1 – anerkjennelse av andre lands notifikerte eID-løsninger avhenger av at en selv notifikere – i det hele tatt presenteres som et alternativ. En slik tolkning er direkte i strid med intensjonen med eIDAS og ville medføre at medlemsland kunne «melde seg ut» av eIDAS's bestemmelser om eID ved å la være å notifikere selv.

Det er kanskje mulig å tolke teksten i eIDAS artikkel 6 isolert på denne måten, men forarbeidene til eIDAS viser at tolkningen er feil. Det første utkastet til eIDAS-forordningen uttrykker eksplisitt at en må akseptere notifisert eID fra andre land uten betingelser (COM(2012) 238/2, artikkel 5, 6. juni 2012), og selv om teksten er endret, har aldri denne intensjonen blitt endret. POD, som har fulgt eIDAS-arbeidet over lang tid, kjenner ikke til noen andre aktører i Europa som forfekter at høringsutkastets alternativ 1 er en mulig tolkning.

Når en legger tolkningsalternativ 2 til grunn, kan en vurdere to forhold helt uavhengig av hverandre:

- Notifisering av et norsk eID-system for bruk mot tjenester i andre EØS-land.
- Bruk av andre EØS-lands notifikerte eID-systemer mot norske offentlige tjenester.

Problemstillinger og konsekvenser ved notifikering av norsk eID-system

Når det gjelder notifikering av norsk eID-system, mener POD at høringsnotatet burde anbefalt at Norge skal ha som intensjon å notifikere et eID-system for bruk mot offentlige (eventuelt også private) tjenester i andre EØS-land. For POD er det opplagt at en må ta sikte på å sikre norske innbyggere slik tilgang.

Et eID-system vil bestå av (se eIDAS artikkel 7) «electronic identification means», det vil si eID-er, og «authentication online», som med de tekniske løsninger som er i bruk i dag (ref. STORK-prosjektet og CEF Digital eID byggekloss), antageligvis vil være ID-porten i Norge. Selv om det ikke er særskilt nevnt i forslaget, legger POD derfor til grunn at notifikering fra Norge vil være tett knyttet til ID-porten, og at de eID-ene som støttes i ID-porten, og som det er hensiktsmessig å notifikere, vil bli notifisert. Som nevnt innledningsvis har POD som intensjon at eID på nasjonalt ID-kort skal være del av et norsk, notifisert eID-system.

En eID som notifiseres, må kunne brukes mot minst én offentlig tjeneste i Norge. Dette sikres ved støtte i ID-porten. Videre må en eID som notifiseres:

- Være utstedt av Staten (som MinID og kommende eID på nasjonalt ID-kort),
- Være utstedt under et mandat fra Staten,
- Være utstedt uavhengig av Staten, men anerkjent av Staten (eID-er i markedet som støttes i ID-porten antas å oppfylle dette kravet).

Dersom eID fra en markedsaktør skal notifiseres, må Staten (dvs. aktøren med ansvar for notifikering) forsikre seg om at eID-en oppfyller kravene til nivået den skal notifiseres på, samt inngå avtale om notifikering med eID-utstederen. I tillegg til betaling må en avtale omfatte ansvarsforhold, se artikkel 11 i eIDAS. Dersom en mot formodning ikke skulle oppnå avtaler om notifikering med eID-utstederne i markedet, vil eID på nasjonalt ID-kort garantere at det finnes en eID som kan notifiseres fra Norge på høyeste sikkerhetsnivå.

Et vesentlig avklaringspunkt som vi ikke kan se er berørt i høringsnotatet, er om en skal kunne benytte norsk fødselsnummer/d-nummer til å identifisere norske innbyggere mot utenlandske tjenester, eventuelt om denne identifiseringen vil være begrenset til offentlige tjenester.

Dersom fødselsnummer ikke kan brukes etter dagens regelverk, må en enten endre regelverket eller etablere en annen metode for unik identifisering av norske innbyggere mot utenlandske tjenester.

Merk at eIDAS artikkel 9.1.b sier at eID-utstederne og autentiseringstjenesten skal underlegges tilsyn, men eIDAS spesifiserer ikke nærmere hva dette innebærer (se også kommentar til pkt. 8 i høringsnotatet).

Siden norsk notifikasjon antas å bli tett knyttet til ID-porten, anbefaler POD at KMD eller Difi får ansvaret for norsk notifikasjon, avhengig av om en velger å legge ansvaret på departements- eller direktoratsnivå.

Fastsettelse og bruk av sikkerhetsnivåer

POD mener at en eID på høyeste tillitsnivå må representere en unik knytning til sluttbruker ved bruk av nasjonalt unikt nummer og biometri, og at dette må hensyntas ved etablering av norsk profil for eIDAS høy.

Som nevnt over må det legges til grunn at norske offentlige tjenester på nett vil være forpliktet til å akseptere notifikerte eID-er fra andre EØS-land uavhengig av om Norge selv notifikerte. Dette medfører at en må vurdere hvilket eIDAS-nivå ulike offentlige tjenester krever. POD anbefaler sterkt at en tilpasser norske eID-nivåer slik at disse samsvarer med eIDAS-nivåene. Det vil si at norsk nivå 4 vil tilsvare eIDAS høy, norsk nivå 3 vil tilsvare eIDAS betydelig, og eventuelt (mindre viktig siden anerkjennelsesplikten etter eIDAS artikkel 6 ikke gjelder) at norsk nivå 2 vil tilsvare eIDAS lav. Sikkerhetsnivå for en tjeneste vil da være det samme i henhold til nasjonalt rammeverk og eIDAS. Godkjenning av en eID for nasjonalt nivå og eIDAS-nivå blir også det samme, men av nasjonale eID-er er det kun de som er notifisert som kan benyttes mot andre land. Som diskutert nedenfor mener POD at en i prinsippet kan velge å notifisere en eID på et lavere nivå enn den egentlig er godkjent for. Det vil si at en eID som holder nivå høy, kan notifiseres på nivå betydelig for bruk mot utenlandske tjenester dersom dette av en eller annen grunn skulle være ønskelig.

eIDAS gjennomføringsrettsakt om sikkerhetsnivåer gir flere alternative metoder for å oppnå et gitt nivå. Det er nødvendig å definere en norsk «profil» av denne gjennomføringsrettsakten for å beskrive hvilke av disse metodene som er relevante i Norge, og hvilke krav som må gjelde etter norske forhold. Eksempelvis vil det være nødvendig å spesifisere hvilke fysiske legitimasjonsdokumenter som kan være akseptable, og det kan være nødvendig å spesifisere krav til en eID som skal kunne brukes for utstedelse av andre eID-er. I denne sammenhengen gjør POD oppmerksom på at eID på nasjonalt ID-kort vil utstedes etter personlig fremmøte på passkontor med kontroll av biometri og meget sterk sikkerhet for korrekt og unik identitetsfastsettelse. eID på nasjonalt ID-kort skal kunne brukes ved utstedelse av andre eID-er. POD anbefaler at norske retningslinjer stiller krav om identitetsfastsettelse på nivå med eID på nasjonalt ID-kort for at eID-en skal kunne brukes til utstedelse av en annen eID på eIDAS nivå høy.

Av punkt 7.3 i høringsnotatet går det frem at det er rom for tolkninger av hvordan anerkjennelsesplikten skal fungere for tjenester som kun refererer til norske sikkerhetsnivåer, se eIDAS artikkel 6.1.b. I forbindelse med nasjonal eID-prosjektet har enkelte tjenesteeiere i offentlig sektor ytret et behov for å kunne stille strengere krav til eID enn dagens sikkerhetsnivå 4. POD anbefaler at det gjennomføres en nærmere kartlegging av et slikt behov i det videre arbeidet med å revidere nasjonale sikkerhetsnivåer for å sikre at en ikke skaper et

mulig hinder for fremtidige tjenester som kan ha strengere krav til sikkerhet enn dagens nivå 4.

Høringsnotatet diskuterer spesielle problemstillinger som oppstår dersom det nasjonalt stilles strengere krav enn eIDAS høy. POD mener de tolkningene av eIDAS som presenteres i høringsnotatet er mangelfulle. POD er enig i at tjenester som stiller strengere krav ikke bør omfattes av anerkjennelsesplikten. Dersom en må akseptere eID på eIDAS nivå høy fra andre land mot en slik tjeneste, vil det senke sikkerheten i tjenesten. EU-kommisjonen har uformelt, i epost til oss, uttalt at de mener at anerkjennelsesplikten gjelder og at en ikke har anledning til å stille strengere krav enn eIDAS nivå høy for offentlige publikumstjenester. Dersom behovet for strengere krav enn eIDAS høy viser seg å være tilstede anbefaler POD at mulighetsrommet avklares nærmere.

Høringsnotatet sier at når en eID notifisert på et gitt eIDAS-nivå brukes nasjonalt mot en tjeneste, så har en implisitt sagt at tjenesten er på dette nivået, og at notifiserte eID-er fra andre land på samme nivå må aksepteres. Det vil si at dersom en har en nasjonal tjeneste med krav om høyere eID-nivå enn eIDAS høy, så vil en bare kunne bruke ikke-notifiserte eID-er som er dokumentert sterkere enn eIDAS nivå høy mot denne tjenesten. Dette er en mulig tolkning, men etter PODs mening er en mer sannsynlig tolkning utelatt.

POD sin tolkning tar utgangspunkt i at eIDAS kun gjelder for eID-bruk over landegrensene slik det er definert i formålet for forordningen, og at nivået en eID kan brukes på nasjonalt, og nivået eID-en er notifisert for, er «frikoplet». Med denne tolkningen kunne, som et tenkt eksempel, Norge valgt å notifisere eID på nasjonalt ID-kort på eIDAS betydelig, fordi en ikke ønsket å ta ansvar for bruk på høyere nivåer mot andre land, selv om eID-en opplagt oppfyller kravene til eIDAS høy og nasjonalt brukes på dette nivået. Notifiseringsnivået bestemmer sikkerhetsnivået for utenlandske tjenester eID-en kan brukes mot, men for nasjonale tjenester kan den samme eID-en brukes på høyere sikkerhetsnivå hvis den er godkjent for dette.

Med referanse til mulighetene for å etablere nasjonale tjenester med strengere krav enn eIDAS høy, vil en med PODs tolkning for eksempel kunne definere eID på nasjonalt ID-kort til å ha nasjonalt nivå «ekstra høy» og stille dette som krav til en nasjonal tjeneste, og dette vil være uavhengig av om eID på nasjonalt ID-kort er notifisert på eIDAS høy. Notifisering vil ikke «senke kravene», slik høringsnotatet sier. Som nevnt over, forutsetter imidlertid dette at anerkjennelsesplikten ikke gjelder for en slik tjeneste.

POD bemerker at eIDAS kun gjelder autentisering mot offentlige tjenester. Andre anvendelser, for eksempel for utstedelse av andre eID-er på nivå høy, kan Norge kreve bruk av eID på nivå med eID på nasjonalt ID-kort, noe som er høyere enn minimumskravene til eIDAS høy.

Bruk av utenlandsk notifisert eID mot norske, offentlige tjenester

Under «identifiseringsutfordringer» sier høringsnotatet at det «kun er anerkjennelsen av autentiseringen» som reguleres av forordningen. POD er uenig i denne begrensingen. PODs tolkning av eIDAS artikkel 6 er at intensjonen er at utenlandske brukere faktisk skal kunne anvende offentlige tjenester i Norge ved bruk av eID fra annet EØS-land, forutsatt at brukeren i en eller annen forstand er autorisert for tilgang til tjenesten. Offentlige tjenester i Norge bruker i stor grad fødselsnummer/d-nummer for å identifisere brukere. Høringsnotatet beskriver utfordringene ved å identifisere en person med utenlandsk eID, men beskriver i liten grad nødvendige tiltak.

Identifiseringsutfordringene kan deles i to:

1. Personen som bruker utenlandsk eID har allerede fødselsnummer/d-nummer og er registrert i Folkeregisteret.
2. Personen som bruker utenlandsk eID er ikke registrert i Folkeregisteret.

I tilfelle 1 antar POD at offentlige tjenester skal bruke personens fødselsnummer/d-nummer som vanlig. Det betyr at en i Folkeregisteret eller i et annet register må lagre koplingen mellom identifikasjon av brukeren fra utlandet og norsk fødselsnummer/d-nummer, slik at en kan slå opp basert på autentisert, utenlandsk identitet og oversette til fødselsnummer. Som høringsnotatet belyser, er dette en langt fra triviell oppgave. Kompleksiteten varierer med hvilket land brukers eID kommer fra. POD presiserer at Folkeregisteret allerede i dag kan lagre koplinger mellom fødselsnummer og tilsvarende identifikatorer fra andre nordiske land. Det er mulig at en form for registreringsprosedyre vil være nødvendig for å kople en utenlandsk eID til personens norske fødselsnummer/d-nummer.

Dersom personen ikke har norsk identifikator, må det tilordnes en identifikator før tjenester kan brukes. Høringsnotatet diskuterer hvordan personen eventuelt kan tilordnes et d-nummer og registreres i Folkeregisteret. POD mener at registrering i Folkeregisteret bør være forbeholdt personer som har rettigheter eller plikter i Norge. Folkeregistrering av en person som kun forsøker å bruke en offentlig tjeneste i Norge, bør ikke gjøres. Videre kan en få problemer med antall mulige d-nummer dersom en skal tilordne d-nummer til alle slike personer, potensielt «alle personer i EØS-området». POD foreslår at en i stedet ser på bruk av en midlertidig identifikator etter modell av «felles hjelpenummer» som brukes i helsesektoren. Med en midlertidig identifikator kan brukeren gis umiddelbar tilgang til tjenesten uten å måtte vente på tildeling av d-nummer. Også for et slikt hjelpenummer er det mange forhold som må utredes, blant annet om dette skal slettes dersom brukeren ikke oppnår noe med tilgangen til den norske tjenesten, eller lagres slik at personen får samme nummer neste gang vedkommende bruker en norsk offentlig tjeneste.

Selv med et «felles hjelpenummer» vil det være tjenester der det er behov for å endre regelverk og/eller teknisk løsning for å tillate tilgang for utlendinger uten norsk fødselsnummer/d-nummer. Som eksempel krever tjenesten «samordnet registermelding» (selskapsregistrering med mer) i Altinn at brukeren har d-nummer før tjenesten brukes. Mens selskapsregistrering fra utlandet i en rekke land nå er en meget rask og enkel prosess, må en utlending i Norge bruke et par uker på å få tildelt d-nummer i en papirbasert og manuell prosess før et selskap kan registreres. POD antar at liknende forhold kan gjelde flere tjenester.

Høringsnotatet diskuterer prosess for tildeling av d-nummer. POD ønsker å påpeke at autentisering av personen med attributter som kan overføres ved bruk av CEF Digital eID-infrastruktur, bør kunne gi både tilstrekkelig informasjon for registrering og en sterkere identitetsfastsettelse enn dagens papirprosess med oversendelse av kopi av bilsiden i personens pass. Hvis instansen som rekvirerer d-nummer kan gjøre dette elektronisk med referanse til norsk, midlertidig identifikator, kan hele prosessen med rekvirering av d-nummer gjøres elektronisk og antagelig automatisk med økt sikkerhet. Som belyst i høringsnotatet vil kompleksiteten i dette variere med hvilket land brukeren kommer fra. For noen land kan en slik automatisert prosess være umulig å få til.

POD påpeker at bruk av denne typen registreringsprosesser må koples til gradering av «sikker identitet» i Folkeregisteret. Den sikreste identitetsfastsettelsen får en ved unik identitet knyttet til biometri – både etablert i forbindelse med utstedelse av pass eller ID-kort og på utlendingsfeltet. Selv om en automatisert prosess som nevnt over bruker eID på eIDAS høy, gir dette lavere sikkerhet for korrekt identitet.

Videre mener POD det er en forutsetning for å hindre et potensielt misbruk at en identifisering med bruk av utenlandsk eID entydig kan knyttes til eksisterende nasjonale identifiseringsopplysninger/d-nummer. En utlending skal ikke kunne etablere to identiteter i Folkeregisteret ved å bruke to forskjellige eID-er fra sitt hjemland.

Som konklusjon på punktene over mener POD at det i lys av eIDAS er nødvendig med en full gjennomgang av regelverket for tildeling og bruk av fødselsnummer og d-nummer. Dette er en konsekvens som ikke er tilstrekkelig belyst i høringsnotatet.

Høringsnotatet pkt. 8 Tillitstjenester

I avsnitt 8.1.1.1 står det at "Departementet oppfatter listen [over tillitstjenester] som uttømmende". POD bemerker at listen begrenser hvilke tjenesteområder som er omfattet av eIDAS, men at det likevel fortsatt er noen uklarheter knyttet til dette. For eksempel pågår det nå diskusjoner innen standardiseringsorganene om en signeringstjeneste kan være en frittstående tillitstjeneste fra en egen tilbyder, eller om en slik tjeneste bare kan tilbys av en aktør som også tilbyr en annen kvalifisert tillitstjeneste (se eIDAS annex II punkt 3).

Til avsnitt 8.1.1.6, omtalen av artikkel 20 nr. 4, bemerker POD at gjennomføringsrettsakt for akkreditering av samsvarsvurderingsorganer er vedtatt, og at denne henviser til standarden ETSI EN 319 403. ETSI-standard er basert på ISO/IEC 17065: Conformity assessment – Requirements for bodies certifying products, processes and services. Norsk Akkreditering har ansvaret for akkreditering etter ISO/IEC 17065. Aktører som er akkreditert etter ISO/IEC 17065, bør da kunne få en tilleggsakkreditering i henhold til ETSI EN 319 403. POD bemerker at det er gjort et bevisst valg når det gjelder å basere akkreditering på ISO/IEC 17065. Alternativet var å basere seg på ISO/IEC 17021: Conformity assessment – Requirements for bodies providing audit and certification of management systems, som blant annet ligger til grunn for sertifisering av styringssystemer for informasjonssikkerhet etter ISO/IEC 27001. Dette betyr at en aktør som akkreditert for sertifisering av styringssystemer for informasjonssikkerhet, ikke kan få utvidet denne akkrediteringen til å gjelde for samsvarsrevisjon av tillitstjenester.

Det er sannsynlig at politiet kommer til å tilby tjenester som krever avansert elektronisk signatur. Disse tjenestene må kunne motta og akseptere tilsvarende signaturer fra hele EØS-området. POD anbefaler at det som del av ID-porten etableres en sentral valideringstjeneste for utenlandske sertifikater/signaturer. Økonomiske og administrative konsekvenser av dette må vurderes. POD antar imidlertid at disse konsekvensene er langt mindre enn konsekvensene av at alle aktuelle tjenester selv blir nødt til å gjøre all signaturvalidering lokalt.

I punkt 8.2.2.4 ber NFD om syn på videreføring av særhjemmel om esignatur i offentlig sektor. PODs vurdering er at forskriftshjemmelen i forvaltningsloven § 15a er tilstrekkelig, og at innholdet i denne paragrafen ikke er i konflikt med bestemmelsene i eIDAS-forordningen.

Til avsnitt 8.3 om tilsynsorganets oppgaver har POD flere merknader.

Når det gjelder oppnevning av tilsynsorgan, er det etter PODs oppfatning to aktuelle kandidater: Nkom og Nasjonal Sikkerhetsmyndighet (NSM). Difi bør etter PODs mening ikke ha denne rollen siden Difi er avtalepart med de samme tilbyderne for bruk i ID-porten, og også fordi Difi i dag i liten grad har kompetanse som tilsynsorgan. Tillitstjenester er et område som kan sies å ligge nærmere NSMs kjerneområder enn Nkoms. NSMs tilsynsoppgaver er imidlertid i dag knyttet til sikkerhetsloven, og dersom NSM skal ha tilsyn med tilbydere av tillitstjenester,

medfører dette en prinsipiell utvidelse av NSMs virkeområde. POD bemerker også at europeisk standardiseringsarbeid innen området i stor grad foregår i ETSI, der Nkom har ansvaret for Norge.

POD bemerker at eIDAS medfører at kravene til tilsynsorganets kompetanse og omfang blir vesentlig mer omfattende enn i dag. Nkom har i dag kompetanse innen området sertifikatutstedelse. Med innføringen av eIDAS må tilsynsorganet også være forberedt på å føre et mer aktivt tilsyn med tilbydere av tillitstjenester, blant annet tidsstemplingstjenester, elektroniske leveringstjenester og elektroniske arkivtjenester, samt bidra dersom andre lands tilsynsmyndigheter ber om bistand. Dersom Nkom alene skal bygge opp og vedlikeholde tilstrekkelig kompetanse, vil dette kreve betydelige ressurser. POD ønsker i denne sammenhengen å peke på eIDAS artikkel 18 om tilsynsorganenes samarbeid over landegrenser. Et forslag kan være at en etablerer et nordisk samarbeid der spisskompetanse på tilsyn av en type tillitstjeneste i ett land kan utnyttes i de andre landene. På denne måten kan en unngå at hvert enkelt lands tilsyn må etablere kompetanse på alle mulige tillitstjenester også i de tilfellene det ikke er noen, eller et svært lite antall, tjenestetilbydere i landet. Samarbeid mellom forskjellige tilsynsorganer i Norge bør også vurderes, for eksempel med NSM som nevnt over.

POD bemerker i denne sammenhengen at det er meget viktig at tilsynets kostnader holdes lave slik at gebyrer som belastes tjenestetilbyderne, ikke blir for høye. Modell for gebyrberegning må utarbeides. For eksempel må det avgjøres om alle tillitstjenester skal underlegges samme gebyr eller om det skal differensieres på forskjellige typer tillitstjenester. Dette er ikke berørt i høringsnotatet, men modell for gebyrberegning kan potensielt ha store konsekvenser for tilbydere av tillitstjenester og dermed for muligheten til å etablere et fungerende marked for slike tjenester.

POD ønsker ikke å konkludere på valg av tilsynsorgan, men ber om at det tas med i vurderingen hvordan NSMs kompetanse kan utnyttes for oppgaver knyttet til tilsyn i lys av det økte omfanget.

For øvrig gjør POD oppmerksom på at eIDAS artikkel 9.1.b sier at utstedere av eID-er som er med i et notifisert eID-system, og aktøren som er ansvarlig for autentiseringstjenesten som er en del av eID-systemet, skal underlegges et «applicable supervisory regime». Dette betyr at ID-porten som autentiseringstjeneste og notifiserte eID-er som ikke er underlagt annet tilsyn (for eksempel MinID dersom denne skal notifiseres), skal være under tilsyn. eIDAS stiller imidlertid ikke krav til form på dette tilsynet.

Høringsnotatet pkt. 9 Bør selvdeklarasjonsordningen beholdes?

Siden implikasjonene ved å fjerne selvdeklarasjonsordningen ikke er avklart, støtter POD høringsnotatets konklusjon om at en hjemmel til å etablere slike ordninger kan beholdes.

POD mener imidlertid at en bør ha som mål å fjerne selvdeklarasjonsordningen. Blant annet medfører ordningen to registreringer hos Nkom for utstedere av kvalifiserte sertifikater med tilhørende to gebyrer, noe som bør være unødvendig.

Selvdeklarasjon refererer til «Kravspesifikasjon for PKI i offentlig sektor». POD mener at kravspesifikasjonen må revideres slik at en i størst mulig grad henviser til eIDAS med gjennomføringsrettsakter og til europeiske og internasjonale standarder. Dette kan for eksempel gjøres gjennom fastsettelse av forvaltningsstandarder. Det vil likevel være

nødvendig med noen få særnorske tilpasninger av standardene, for eksempel hvordan en skal kode fødselsnummer i et sertifikat eller avlede fødselsnummeret fra sertifikatet.

Høringsnotatet pkt. 10 Avsluttende bestemmelser, ikrafttredelse og overgangsperiode

POD bemerker at eIDAS-forordningen trer i kraft i EU 1. juli 2016, og da tilbakekalles esignaturdirektivet. Av høringsnotatet pkt. 10.2 fremgår det at departementet legger opp til ikrafttredelse av loven 1. januar 2017. Dette kan, i hvert fall teoretisk, skape en uklar juridisk situasjon siste halvår av 2016 når det gjelder forholdet mellom Norge og EU-landene. For eksempel vil EUs system for tillitslister da være hjemlet i eIDAS, som ikke er innført i Norge. I praksis antar POD at det ikke vil oppstå noen problemer, men for sikkerhets skyld nevner vi likevel forholdet.

Høringsnotatet pkt. 11 Endringer i annet regelverk

Dette avsnittet i høringsnotatet fremstår som mangelfullt. Det omfatter kun forskrifter med henvisning til esignaturloven og eventuelt til Kravspesifikasjon for PKI i offentlig sektor. eIDAS-forordningen kan imidlertid ha langt mer vidtrekkende konsekvenser, og dette må utredes nærmere.

POD har ikke gjort noen nærmere analyse av mulige endringer, men med henvisning til tidligere kommentarer til høringsnotatet kan vi slå fast at konsekvenser for folkeregisterloven med forskrifter må utredes. Videre må en se på lover og forskrifter som stiller krav om at brukeren er tildelt fødselsnummer eller d-nummer. Ett eksempel er enhetsregisterloven § 7 som medfører at en utenlandsk bruker må få tildelt d-nummer før tjeneste «samordnet registermelding» i Altinn kan brukes.

Utredning av endringer i annet regelverk er derfor antagelig en langt mer omfattende oppgave enn det høringsnotatet gir inntrykk av.

Høringsnotatet pkt. 12 Om lovens anvendelse på Svalbard

POD har ingen kommentarer til dette punktet.

Høringsnotatet pkt. 13 Økonomiske og administrative konsekvenser

Høringsnotatet gir en svært kortfattet og begrenset vurdering av økonomiske og administrative konsekvenser. POD har en rekke kommentarer.

Høringsnotatet sier om offentlige tjenester på nett at «det er ønskelig at offentlige myndigheter ... kan tilby slike tjenester til brukere som har utenlandske eID-er». POD påpeker at det ikke kan være et «ønske» om å tilby offentlige tjenester. Dette er faktisk et krav for mange tjenester i henhold til eIDAS artikkel 6.

Politiet vil ha en rekke tjenester som faller inn under bestemmelsene i eIDAS artikkel 6. Det vil si at politiet er forpliktet til å gi tilgang til disse tjenestene basert på autentisering med en utenlandsk eID på nivå betydelig eller høyt. Tjenestene er i mange tilfeller relevante for utlendinger, for eksempel en utlending som ønsker å anmelde et forhold i Norge, som skal søke om norsk politiattest osv. Høringsnotatet gir ingen informasjon om antatte økonomiske og administrative konsekvenser for tjenesteeiere som politiet.

Høringsnotatet nevner at rettsakten «kan få administrative og økonomiske konsekvenser i forbindelse med utstedelse av egne identifikasjonsnumre» for utlendinger. Dette er svært lite konkret og antyder en mulighet for at slik utstedelse av identifikasjonsnummer ikke vil bli etablert. POD vil påpeke at en hensiktsmessig, sentral infrastruktur for identifisering av utenlandske brukere må etableres. Dette må minimum bestå i å oversette brukerens utenlandske identitet til et norsk identitetsnummer som kan brukes for tilgang til norske tjenester der det i dag brukes fødselsnummer/d-nummer. En bør også etablere en løsning slik at tjenester som normalt slår opp personinformasjon i Folkeregisteret, kan få utlevert tilsvarende informasjon om utlendinger. I Folkeregisteret eller i et annet register må det lagres koblinger mellom utenlandsk identifikasjon og norsk identifikator som utenlandske personer er tildelt. Et system for identitetsnummer krever sannsynligvis endringer i lover og forskrifter som i dag regulerer tildeling av norske identitetsnummer, og etablering og vedlikehold av systemet vil kreve betydelige ressurser. Et nærliggende alternativ er å etablere infrastrukturen i et samspill mellom ID-porten og Folkeregisteret.

Hvis en slik sentral infrastruktur ikke etableres, må hver enkelt tjeneste tilrettelegges separat for å kunne gi tilgang for utenlandske brukere. Dette vil kreve endringer i samtlige relevante tjenester som i dag bruker fødselsnummer/D-nummer for tilgang. Politiet har ikke analysert konsekvensene ved å gjennomføre slike endringer i sine tjenester, men det er sannsynlig at det vil være meget komplisert og dyrt.

I ID-porten må det tilrettelegges for autentisering av brukere med utenlandsk eID og for autentisering av norske brukere mot utenlandske tjenester. Etter de opplysninger POD har, er dette arbeidet i gang. POD mener at det er behov for et langt tettere samspill mellom ID-porten og Folkeregisteret enn det som er tilfelle i dag. ID-porten må også tilby en valideringstjeneste for utenlandske signaturer og sertifikater. De administrative og økonomiske konsekvensene for ID-porten kan derfor være betydelige.

I henhold til eIDAS artikkel 7.f skal ikke andre land betale for bruk av norsk, notifisert eID mot sine offentlige tjenester. Det betyr at utgifter til bruk av notifisert eID mot offentlige tjenester i utlandet må dekkes av Norge. Hvor store disse utgiftene blir avhenger av volum av bruk og av forretningsmodell for eID-ene som er notifisert.

Som nevnt tidligere vil det være nødvendig med styrket tilsyn med tilbydere av tillitstjenester. Dersom Nkom skal ha kompetanse på alle former for tillitstjenester, tror POD at ett ekstra årsverk vil være for lite. POD foreslår å etablere et nordisk samarbeid om tilsyn, og dette kan redusere behovet for ekstra ressurser hos Nkom.

Tilbydere av tillitstjenester vil få økt sine kostnader til tredjepartsrevisjoner som følge av kravene i eIDAS, og som følge av økte kostnader for tilsyn, kan de bli belastet med høyere gebyrer for tilsyn. Dette kan ha betydning for tilbydernes økonomiske situasjon, for prisen på tjenestene til brukerne og på mulighetene til å etablere og opprettholde et fungerende marked for forskjellige typer tillitstjenester.

eIDAS tilrettelegger for tilgang til tjenester på tvers av landegrenser. Det er viktig for POD å poengtere at risikoen for svindel og potensial for misbruk da også øker. Vurderinger knyttet til dette mangler. For å sikre at politiet har nødvendig ekspertkompetanse som kreves for etterforskning av denne type kriminalitet, kan det være behov for økte ressurser.

Med hilsen

Annar Bohlin-Hansen

politiinspektør/leder IDeALT-programmet

Unni Norum

seniorrådgiver

Dokumentet er elektronisk godkjent uten signatur.

Kopi til

Justis- og beredskapsdepartementet