Nasjonal sikkerhetsmyndighet

Vår saksbehandler
Plan og administrasjonsstab

Vår dato
2016-02-16

Deres dato
2015-11-30

Antall vedlegg

Vår referanse
A03 - S:15/04460-7

Deres referanse
15/4361

Til
Nærings- og fiskeridepartementet
Postboks 8090 Dep
0032 OSLO
Norge

EUs forordning om elektronisk identifisering (eID) og tillitstjenester - elektroniske transaksjoner i det indre marked

Det vises til Nærings- og fiskeridepartementets brev av 30.11.15 hvor overstående ble sendt på høring.

Nasjonal sikkerhetsmyndighet (NSM) har følgende merknader.

Til kapitlene 7.1 - 7.3:

Sikkerhetsnivåene i både den norske løsningen og eIDAS er beskrevet på et overordnet nivå, og Departementet antar at det er samsvar mellom de to høyeste sikkerhetsnivåene i begge løsningene.

Tidligere har det virket som det har vært sterkere, konkrete krav til nivå EU High, noe som ville gjort at dette nivået ville være over norsk nivå 4. Det ser ikke ut til at de konkrete kravene er tatt inn i den foreliggende forordningen. Det kan således se ut til at de to øverste nivåene sammenfaller mellom EU og Norge, men det er vanskelig å gi et klart svar på det punktet, da vi ikke har hatt anledning til å undersøke om kravene for eIDAS er operasjonalisert gjennom mer tekniske kravprofiler. I tillegg bør det også bemerkes at det i forbindelse med operasjonalisering av kravene, også kan oppstå spørsmål eller uenighet om hvordan de overordnede kravene skal fortolkes. I praksis vil det være et stykke arbeid som må nedlegges for å spesifisere kravene, og først når disse profilene er utformet, vil det være mulig å foreta en reell sammenligning.

I høringsnotatet side 16 heter det at:

«Dersom norske eID-er skal benyttes for innlogging i utenlandske tjenester, vil Norge måtte tilby en tilsvarende gratis valideringstjeneste i ID-porten.»

NSM mener det bør avklares hvorvidt denne valideringstjenesten skal evalueres og sertifiseres, og eventuelt etter hvilke krav. NSM anbefaler at departementet tar i bruk

Postadresse
Postboks 814
1306 SANDVIKA

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09
Internetadresse (URL)
www.nsm.stat.no

anerkjente mekanismer for å skaffe nødvendig grad av tillit til valideringstjenesten, noe som etter direktoratets syn kan skje gjennom sertifisering på bakgrunn av tekniske profiler i henhold til Common Criteria (ISO/IEC 15408).

Til kapittel 8.1:

Kapittel 8.1.1.2:

I høringsnotatet heter det at:

«Sertifiseringen av kvalifiserte elektroniske signaturfremstillingssystemer skal etter artikkel 30 punkt 3 basere seg på refererte standarder fastsatt ved gjennomføringsrettsakt fra Kommisjonen. Fortalens punkt 55 uttaler at IT-sikkerhetssertifiseringen bør baseres på internasjonale standarder, som for eksempel ISO 15408, og dertil tilknyttede evaluerings-metoder og gjensidige anerkjennelsesordninger. Alternative evalueringsprosesser skal kun benyttes for evaluering av teknologiske løsninger hvor det ennå ikke er utarbeidet eller fastsatt en standard som disse systemene kan evalueres etter. Alternative evalueringsprosesser skal så langt som mulig være sammenlignbare med allerede fastsatte standarder for IT-sikkerhets-sertifisering.»

NSM forutsetter at evaluering- og sertifisering av elektroniske segl- og signaturfremstillingssystemer skal utføres etter godkjente tekniske profiler (Protection Profiles, collaborative Protection Profiles), alternativt tekniske løsningsspesifikasjoner (Security Target) i henhold til Common Criteria (ISO/IEC 15408). NSM kan ikke se at det per i dag finnes gode alternative evalueringsprosesser til Common Criteria (ISO/IEC 15408) som er lett sammenliknbare med allerede fastsatte standarder for IT-sikkerhetssertifisering.

Kapittel 8.1.2.1:

NSM har ingen innvendinger til at NSM v/Sertifiseringsmyndigheten for IT-sikkerhet (SERTIT) utpekes som sertifiseringsorgan ettersom direktoratet er avtalepart under det internasjonale arrangementet CCRA og den europeiske avtalen SOGIS MRA.

NSM anser ikke at lovforslaget om gjennomføring av EUs forordning om eIDAS innebærer noen utvidelse av det ansvar NSM/SERTIT allerede innehar. Det er oppdragsmengden som avgjør bemanningsbehovet i SERTIT. Ekstra ressurspådrag i forbindelse med eventuell større oppdragsmengde vil også treffe de kvalifiserte evalueringslaboratoriene innen ordningen. For deres del vil markedet regulere dette.

Det for tiden fire kvalifiserte og autoriserte evalueringslaboratorier underlagt SERTIT, slik at evalueringskapasiteten og de konkurransemessige forholdene ansees å være tilstrekkelig ivaretatt. Det kan imidlertid være at noen av evalueringsfirmaene vil kunne ha behov for å opparbeide ny kompetanse i teknikker, metoder og verktøy i samband med evaluering av sikre segl- og signaturfremstillingssystemer. Det kan da tenkes at myndighetene bør vurdere å tilby støtteordninger for evalueringsfirmaene for å kunne tilpasse seg nye markedssituasjoner, slik at sertifiseringsordningen kan opprettholde tilstrekkelig konkurranse i markedet.

Til kapittel 8.3:

NSM støtter departementets vurderinger og forslag i høringsnotatet om Tilsynsorganets oppgaver.

Dette begrunnes i at Nasjonal kommunikasjonsmyndighet (NKOM) allerede har et ansvar for å føre tilsyn med aktørene på post- og teleområdet, og synes å være den myndigheten som har bredest erfaring og ekspertise på teleområdet generelt. NKOM har vært tilsynsmyndighet etter e-signaturloven siden loven ble innført i 2001 og besitter kompetanse både på det tekniske, økonomiske og juridiske området. I tillegg har NKOM etablert et godt samarbeid med aktørene i bransjen, som det vil være nyttig å bygge videre på.

Til kapittel 9:

NSM mener sertifisering gjennom et uhildet tredjepartsorgan innebærer at man kan ha høyere tillit til tjenester enn det man oppnår ved en selvdeklarasjon. Selvdeklarasjon bør etter NSMs syn derfor ikke beholdes. NSMs erfaring er at selvdeklarasjon er et lite pålitelig redskap som ikke resulterer i tilstrekkelig tillit til tjenester.

Med hilsen

Morten Hatlem
avdelingsdirektør

for Christian R. Reusch
seksjonssjef