Fra: Randi Hestnes
Sendt: 11. mai 2007 12:49
Til: Postmottak FAD
Emne: FW: Utkast til høringsbrevet- kommentarer

Det Kongelige Fornyings- og Administrasjonsdepartementet
Avdeling for IT-politikk

Seniorrådgiver Katarina de Brisis

Innspill til "Høring- forslag til strategi for bruk av eID og e-signatur i offentlig sektor".

Nedenfor følger våre innspill i henhold til de områder dere spesielt ønsket tilbakemelding på.

Innspill om antall sikkerhetsnivåer:

Det bør være nok med fire sikkerhetsnivåer. Flere nivåer mener vi vil komplisere unødvendig.

Det er viktig å se nivåene i sammenheng med bruksområder. Sikkerhetsnivåene bør sammen med risikonivåene utdypes og spesifiseres. Enhver implementering av eID vil måtte starte med en svært viktig risikoanalyse, og det bør være enkle, klare hjelpemidler for å sørge for riktig plassering i risikobildet for implementeringen.

Det står i Vedlegg 1 kapittel 5: "Det vil bli utarbeidet en veileder med en mer grundig innføring i risikovurderinger og bruken av dette sikkerhetsrammeverket." Dette arbeidet er svært viktig, og må ikke glemmes i prosessen.

Innspill om kravene til sikkerhetsnivå 3 og 4

Kravene til disse to sikkerhetsnivåene er litt uklare. Det kan virke som om kravene er så å si det samme. Begge forteller om en eller annen form for sikring at rette vedkommende tar i bruk autentiseringen, men nivå 4 spesifiserer fysisk oppmøte med legimitering. Hva blir altså forskjellen i praksis utenom at man sier at nivå 4 er streng og skal følge offentlige krav?

På informasjonsmøtet i april ble det uttalt at kun elektronisk ID fra selvdeklarerte leverandører kan benyttes for forvaltning av offentlige tjenester. Dette er et paradoks sett opp mot at hver forvalter selv bør sette sikkerhetsnivå på sine tjenester. Mener man for eksempel at en offentlig tjeneste ikke krever mer enn sikkerhetsnivå 3 må man da også få mulighet til å benytte signaturer fra leverandører som ikke er selvdeklarerte.

Dersom man benytter selvdeklarerte leverandører virker det, ut fra definisjonene som er gitt i dokumentet, litt uforståelig at hele forskjellen på nivå 3 og 4 er at man har overlevert eID'en personlig. Ved senere bruk vil jo den tekniske sikkerheten være akkurat den samme.

Innspill om sikkerhetsnivå 2

Sikkerhetsnivå 2 er en 1-faktors autentisering hvor man ikke er sikker på at rette person har

mottat autentiseringskoden. Det er overraskende at Minside har valgt dette som autentiseringsmetode for pålogging. I praksis kan naboen din plukke opp kjente brev som kommer i posten på denne tiden, og gjøre om selvangivelsen din eller kanskje endre andre innleveringer for deg. Innenfor sikkerhetsnivå 2 må man også kunne si at det er forskjell i sikkerheten på en fast PIN som sendes i posten på folkeregistrert adresse og en passordkalkulator.

Man bør gå gjennom definisjonen av sikkerhetsnivå og vurdere om den sikkerheten som i dag beskrives i de ulike nivåene faktisk kan sammenlignes. Dersom man stoler på at brukeren selv er i stand til å vurdere hvor vanskelig passord han/hun ønsker å beskytte sin informasjon på nett med, kan det vurderes som sikrere å sette egne passord enn å få tilsendt en fast PIN i posten.

Om blanding av nivåer og flere tilganger

Det "skumle" er selvfølgelig når en autentiseringsmetode gir flere tilganger, og man må være forsiktig med hvilke nivå av sikkerhet man tilbyr. I tillegg må man være klar over at et for dårlig sikret autentiseringssystem i en offentlig enhet eller ute i markedet, kan føre til uautorisert tilgang til andre systemer som benytter samme autentiseringssystem.

Ved å samle autentiseringsmetoder vil man altså forenkle, men samtidig utsettes for høyere risiko. Dette må man ta høyde for når man vurderer konsekvens, for deretter å finne riktig sikkerhetsnivå. Dersom hver offentlig virksomhet selv skal vurdere hva som er akseptabelt sikkerhetsnivå og hvilke sikkerhetsløsninger som gir forholdsmessig akseptabel sikkerhet for virksomheten, må disse være klar over disse forholdene.

Dette vil også si at risiko og trusselbildet hele tiden vil forandres i forhold til hvilke systemer som benytter autentiseringsmetodene.

Innspill om nasjonalt ID-kort som primær strategi

Dette vil være en bra strategi dersom man sikrer rask utbredelse og stort volum på utbredelse og mulig bruk. Dette kan kun skje dersom ID-kortet har en positiv verdi for den enkelte kunde. Dvs at ID-kortet kan erstatte et større antall andre dokumenter (sertifikat, bankkort, helsekort og lignende). For å få dette til er det kritisk å involvere det private næringsliv slik at også private tjenester kan tilbys ved bruk av dette kortet.

Det ble sagt på informasjonsmøtet at man ikke ønsket å benytte et allerede eksisterende register/database. Dette må det argumenteres for. Vi har allerede flere databaser som det vil være naturlig å bygge en slik oversikt på og det virker lite formålstjenelig å lage en ytterligere base som må vedlikeholdes og sikres ved siden av de allerede eksisterende.

Innspill om offentlig utstedelse av virksomhetssertifikater

Det er lite vesentlig hvem som utsteder og det kan gjerne være det offentlige, så lenge det etableres visse garantier for hvor raskt man skal kunne få utstedt sertifikat og at kapasiteten er tilstrekkelig. Her må det også legges til rette for gruppeutstedelser.

Innspill om behov for samtrafikknav

Det vil være et stort behov for et felles supportapparat for bruk av eID og eSignatur. Et slikt felles supportapparat vil kunne ta ut synergier på tvers av offentlige virksomheter og redusere behovet for egne støtteordninger.

Hvis man her også kunne fått til support mot de offentlige virksomhetene som benytter felles eID og Signatur om hvordan disse benyttes i integrasjon mot standard programvare benyttet i offentlig sektor vil dette være kostnadsbesparende for enhetene. (Eksempelvis vil de fleste av

bedriftene som benytter de felles eID-standardene ha behov for de samme webservice tjenstene eller lignende). Dette vil også videre forenkle kommunikasjon til sluttbruker i felles portaler og lignende).

Innspill om plan for realisering

Dette er et godt initiativ, men det er allerede gått for lang tid til at man kan ta ut målet som var satt i strategien om rask utvikling. Flere av de berørte offentlige virksomheter har allerede tatt i bruk ulike former for eID og signatur og vil således måtte gjøre deler av dette arbeidet på nytt når en ny felles strategi kommer. Dette har vi vært klar over og det er derfor uproblematisk å håndtere, men det understreker viktigheten av å klare å ta ut de endre effektene som er enklere tilgang for bruker og kostnadssynergi.

Iom at mange virksomheter allerede har tatt i bruk eID og signatur med god erfaring er det også viktig å ta hensyn til dette ved at man setter en overgangsperiode etter at ny standard er implementert og utbredt og det forventes at den offentlige virksomheten tilbyr sine tjenester ved ny eID og signatur standard. I denne perioden bør det kjøres i pilot som sikrer at standarden fungerer og at tilgangen på tjenestene ikke blir dårligere enn den var før felles standard ble tatt i bruk.

Med vennlig hilsen

Randi Hestnes

Randi Hestnes
Direktør

Innovasjon Norge

Akersgt. 13 Postboks 448 Sentrum N-0104 Oslo
mob. +47 90 56 91 69
dir.tel. +47 22 00 26 28