Fra: Thomas Gramstad på vegne av Thomas Gramstad
Sendt: 19. mai 2007 00:19
Til: Postmottak FAD
Kopi: Thomas Finneid
Emne: Høringsuttalelse fra EFN om eID strategiforslag

Elektronisk Forpost Norge (EFN)
Pb. 2631 Solli
N-0203 Oslo

Fornyingsdepartementet (FAD) Oslo 15. mai 2007
Postboks 8004 Dep
N-0030 Oslo
(postmottak@fad.dep.no)

HØRINGSUTTALELSE FRA EFN OM FORSLAG TIL STRATEGI FOR BRUK AV EID OG E-SIGNATUR I OFFENTLIG SEKTOR

EFN leverer med dette høringsuttalelse (via epost) til FADs Forslag til strategi for bruk av eID og e-signatur i offentlig sektor.
(http://www.regjeringen.no/nb/dep/fad/dok/Horinger/Horingsdokumenter/2007/Horing--forslag-til-strategi-for-bruk-av/-4.html?id=454624)

EFN stiller seg positive til det arbeid som gjennomføres og forslaget. Forslaget leder mot et krafttak i arbeidet med å modernisere offentlig sektor i forhold til elektroniske tjenester.

EFN registrerer enkelte svakheter i strategien som bør vurderes. EFN foreslår følgende punkter der strategien bør utvides eller revurderes.

Strategien, slik den er presentert, bygger på en mangelfull forståelse for helheten av PKI-konseptet. Dette vil påvirke sikkerhets- og trussel-bildet strategien bygger på og løsningene strategien presenterer. Høringsnotatet mangler en vurdering/strategi for eID som kommer på avveier, samt en vurdering av den begrensede levetiden en sikker elektronisk ID har i et digitalt samfunn kontra det en ID har i det vanlige samfunn. Strategien diskuterer praktisk og organisatorisk håndtering av eID, men ser i stor grad bort fra enkelte sikkerhetsmessige aspekter i forbindelse med eID-håndtering som bør vurderes. Eksempler på dette er: universalnøkkel kontra tjenestespesifikk nøkkel. Bruk av sikkert medium for lagring av eID. Strategiendokumentet åpner med at eID bør være bæreruavhengig, men konkluderer senere med en sterk knytning til Nasjonalt ID. Høringsforslaget diskuterer ikke bæreruavhengige strategier eller alternativer. Løsningen har potensiell gjenbruk langt utenfor offentlig sektor. Strategien bør derfor inneholde vurderinger som tillater at gjenbruk lar seg gjennomføre med hensyn til kostnader og bruksområder. Enkelhet og brukervennlighet i løsningen og tjenestene. Markedet har ikke klart å løse problemet, derfor bør det offentlige vise vei.

HELHETSFORSTÅELSE OG KOMPLEKSITET VED PKI

Dessverre er det i dag altfor mange som misforstår PKI-konseptet i

sin helhet og derfor ser på PKI som løsningen på de fleste sikkerhetsproblemer, spesielt i forbindelse med et usikkert medium som Internett. Den største misforståelsen pleier som regel å være bygget på det teknisk-matematiske grunnlaget og dermed et løfte om garantert sikkerhet ved bruk av PKI. Dette løftet er i seg selv så lokkende at man ofte blindes for de andre tekniske og sosiale egenskapene som omgir enhver elektronisk tjeneste.

En tjeneste som skal publiseres i en elektronisk verden, og Internett spesielt, er tilgjengelig for alle verdens datamaskiner, enten direkte eller indirekte. Internett er et tett sammenkoblet nettverk av relativt ubeskyttede datamaskiner, som ofte er tilgjengelig store deler av døgnet. Siden Internett i tillegg har en kraftig anonymiserende faktor, fører disse to punktene til en senket terskel for gjennomføring av aktiviteter som i det vanlige liv ville vært lite gjennomførbare.

Enhver tjeneste består av minst tre aspekter:

1. Tjenesten
2. Kommunikasjonskanalen
3. Brukeren

PKI er en løsning for å sikre kommunikasjonen mellom brukeren og tjenesten gjennom en usikker kommmunikasjonskanal. I dette ligger det endel kraftige begrensninger. Det vil si at PKI ikke har muligheten til å sikre tjenesten eller brukeren i seg selv, men benytter bare disse for å sikre kommunikasjonen. PKI representerer derfor bare en del av løsningen. Dersom andre deler ignoreres, kan dette sammenlignes med å plassere en bankhvelvdør på et telt - man kan ikke bryte inn gjennom døren, men andre veier er ganske åpne. På tjenestesiden løses dette ved å sikre og overvåke tjenesten av profesjonelle fagfolk. På brukersiden vil ikke de samme ressurser og ekspertise være tilgjengelig. Dermed er brukeren det svake leddet i løsningen.

Gitt dagens virus-situasjon er det ikke vanskelig å se for seg virus som spesialtilpasses for å gjemme seg på brukerens maskin for i det skjulte å:

1. lagre informasjon eller
2. manipulere den informasjonen som blir vist til brukeren
3. gjennomføre uautoriserte og ikke-brukerinitierte handlinger
4. stjele brukerens eID samt lese dens passord uten at brukeren oppdager dette.

Dette har vi ferske eksempler på fra DNBNor og andre banker i Skandinavia, der et spesialtilpasset virus har, i det skjulte, bedt nettbanktjenesten om å overføre penger til spesielle kontoer uten at brukeren vet om dette. Disse angrepene har bare vært en generalprøve på hva vi kan forvente oss i fremtiden. Det er ikke vanskelig å kjøpe slike tjenester fra kriminelle organisasjoner over Internett og få dem spesialtilpasset for norske offentlige Internett-tjenester. Dette kan være spesielt attraktivt i forbindelse med f.eks. industrispionasje der norske bedrifter er i sterkt konkurransepregede markeder (hvor de ansatte kan bli mål for utpressing), eller fremtidige arbeidsgivere og f.eks. bransjer som har behov for detaljert personinformasjon for å selge produktet sitt. Dermed åpner man for enkel og uautorisert tilgang til informasjonen og tjenesten gjennom brukeren eller brukerens utstyr, dvs. PC, mobil etc.

Derfor mangler høringsforslaget en strategi for å sikre at eID bare kan lagres på sikre medier, som fortrinnsvis tillater sikker handlingsvisning og handlingsgodkjenning, slik at brukerens datamaskin bare blir en kanal for å formidle beslutninger i stedet for et apparatet som gjør beslutningen.

KOMPLEKSITETEN FORBUNDET MED PKI

Ettersom en PKI-strategi er omfattende, kompleks og vanskelig å få til på første forsøk, anbefaler derfor EFN at følgende punkter vurderes i strategien:

1. utvidbarhet og gjenbrukbarhet av strategien og løsningen
2. utlysning av internasjonal strategi- og løsnings-konkurranse for bruksområdet.

Det er sannsynlig at det behøves endringer, både små og store, på kort sikt og lengre sikt i forbindelse med løsningen og strategien. Strategidokumentet bør diskutere hvordan man kan og skal håndtere dette og inkludere åpenhet, utvidbarhet og gjenbrukbarhet i strategien og løsningen. Konkret kan dette gjøres ved å bryte strategien og løsningen ned i små og selvstendige deler som henger sammen på spesifiserte måter. Dermed vil det være lettere å endre på strategien og løsningen på et senere tidspunkt. Et eksempel på dette er å si at scenarioet for hvordan brukeren konkret gjennomfører autentisering og autorisering er en selvstendig del og gjennomføres på en standardisert måte. Dermed er dette en selvstendig del av løsningen som er uavhengig av alle andre deler av løsningen og strategien.

Sikker og fungerende PKI er et komplekst tema som krever en strategi og løsning laget spesifikt for problemområdet. Det arbeidet som gjøres i Norge nå er innenfor et område som mange vil kunne gjenbruke både offentlig og privat, i inn- og utland. Siden det ikke finnes noen generell løsning med bruk av PKI, anbefaler EFN derfor at departementet utlyser en konkurranse på internasjonalt nivå som tar sikte på å designe en helhetlig løsning for bruksområdet. Poenget med konkurransen er å dra nytte av den ekspertise og kreativitet som eksisterer over hele verden for å lage en løsning og prinsipper som mange kan gjenbruke. Dette vil være etter en modell brukt av den amerikanske regjeringen, da de for få år siden hadde en slik internasjonal konkurranse for å velge en krypteringsløsning for intern uklassifisert bruk. Løsningen fikk det offisielle navnet Advanced Encryption Standard (AES), og er i dag den anerkjente og mest brukte løsningen for sitt bruksområde i verden.

eID PÅ AVVEIER OG DENS BEGRENSEDE LEVETID

Elektroniske tjenester er som kjent ganske sårbare med hensyn til levetiden til løsningens sikkerhetsnivå. Når man i tillegg vet at en slik tjeneste vil være en sentral og attraktiv tjeneste som offentlige e-tjenester og sikkerhetsløsning er, vil det være nærliggende å anta at interessen for det tjenesten tilbyr. vil være stor for uautoriserte brukere. Med bakgrunn i den ovenfornevnte virussituasjon, er det nærliggende å anta at brukere vil, over tid, bli utsatt for kriminelle aktiviteter slik som forsøk på å stjele eller kopiere brukerens eID og passord. Siden dette er realiteter i Internett og et digitalt samfunn, er det viktig at strategien inneholder punkter om hvordan forholde seg til eID som er:

- tapt
- på avveier
- brukt til identitetstyveri

Det som er viktig i denne sammenhengen er at brukeren ikke blir gjort til ufrivillig offer ved slike handlinger. Ettersom man tufter løsningen på ideen om at PKI gir uavviselighet, er det derfor viktig at strategien tar hensyn til dette slik at brukeren ikke vil lide under slike tilfeller. Det er også viktig i samme åndedrag å nevne hvordan man skal håndtere det relaterte problemet med levetid på eID. Siden takten på aktiviteter i det digitale samfunn er betydelig større enn i det analoge, kan man ikke anta at et eID kan overleve lenger enn kanskje ett år. Det er derfor viktig å ha en strategi for å på en effektiv og brukervennlig måte

tillate utbytting av eID. Dermed får vi to punkter som er viktige i strategien:

1. Foreldede eID: utbyttingstakt og praktiske rammer rundt dette.
2. eID på avveier: erstatning og tilbakekalling av disse.

Et viktig problem i forbindelse med dette er det faktum at strategien bygger på uavviselighet i forbindelse med PKI, men gitt ovennevte scenarier må strategien ta hensyn til at det ikke nødvendigvis er brukeren som har autorisert en handling eller informasjon og derfor kan man ikke legge uavviselighet til grunn for sikringen av tjenesten på en slik måte som angitt i strategien i høringsforslaget.

SIKKERHETSMESSIGE ASPEKTER

Foruten de organisatoriske og praktiske sider av eID-håndteringen tilkommer aspekter som angår det sikkerhetsmessige:

1. Universalnøkkel kontra tjenestespesifikk nøkkel.
2. Nivåsikkerhetsløsninger: PKI kontra engangspassord (PIN etc.).

Selv om disse punktene i stor grad krever en teknisk fagmessig vurdering, er det også viktig å understreke at de må forankres i en strategi for at tjenestene skal sikres i sin helhet. Strategien nevner kort universalnøkler kontra tjenestespesifikke nøkler, men legger ikke mer vekt på dette. Slik EFN ser det er dette en viktig del av strategien av to grunner:

1. Det påvirker løsningen til tjenesten direkte, ved at man må vurdere flere modeller.
2. Det påvirker sikkerheten til løsningen, og dermed brukeren, direkte ved at mekanismen brukeren må forholde seg til endres avhengig av den valgte strategien på disse områdene.

Som nevnt ovenfor, i forbindelse med virus-trusselbildet, er det sannsynlig og dermed påkrevet at strategien legger til rette for utvidet sikkerhet. EFN anbefaler at strategien legger opp til en PKI-løsning som bygger på tjenestespesifikke nøkler. Dette innebærer at dersom noen skulle få tak i brukerens tjenestenøkkel har vedkommende ingen større mulighet til å bruke andre tjenester brukeren har tilgang til eller etterligne brukeren i andre sammenhenger. Personens eID bør være begrenset i bruk til opprettelse/endring av tjenestenøkler og enkelte andre sentrale bruksområder. Personens eID vil da til vanlig ikke være eksponert og vil dermed være langt sikrere.

Når det gjelder nivåsikkerhet med hensyn til PKI kontra PIN-koder o.l. er det viktig å være klar over at engangspassord ikke gir dårligere sikkerhet enn PKI. Tvertimot gir et engangspassord bedre sikkerhet, siden passordet ikke kan gjenbrukes og dermed har det ingen verdi dersom det blir stjålet. Problemet er heller brukervennlighet. Engangspassord slik de brukes i dag er tjenestespesifikke og skrives ut i åpen tekst på et ark man ikke tar med seg til daglig. Hvis engangspassord skal benyttes i enkelte tilfeller bør det styres av navet som "single sign on" for alle tjenester. Da oppnår man noe, nemlig større brukervennlighet, samt at kostnaden ved å bruke løsningen blir mindre for hver tjeneste.

BÆRERUAVHENGIGHET

Innledningen til høringsforslaget gir en beskrivelse av et spennende scenario for bruk av eID, samt beskrivelse av noen fremtidsrettede tanker. En av disse tankene er at eID bør være multibærende slik som i Finland eller Sverige. Dette er en tanke EFN støtter. Dessverre konkluderer arbeidsgruppen med at førstevalget til strategi for eID innebærer en sterkt knytning til

Justisdepartementets forslag om Nasjonalt ID. EFN mener dette hindrer bæreruavhengighet og gjør eID ekskluderende. Det bør fokuseres på bæreruavhengiget, der bærer er en standardisert bærende enhet som kan komme i mange former avhengig av både bruken og brukerens valg.

Et svært interessant forslag er et smartkort eller en liten USB-enhet som er uavhengig av datamaskinen, som gir brukeren muligheten til å lese hva handlingen gjelder og så godkjenne eller avvise den. Denne enheten skal ha som eneste funksjon å ta i mot en kryptert og signert beskrivelse som vises på en egen liten skjerm for godkjenning. Brukeren godkjenner eller avviser handlingsforespørselen ved at enheten krypterer og signerer et svar som sendes tilbake til tjenesten. Hvis denne enheten lages på riktig måte vil dette redusere sjansen for uautorisert bruk betraktelig og datamaskinen/mobilen/etc. blir redusert til å være en formidler istedet for en godkjenner. Dersom man sammen med dette legger opp til at enheten kan lagre mange tjenestespesifikke nøkler har man en bæreruavhengig enhet med egnet sikkerhet, som også er enkel for brukeren og transportabel. En lignende type enhet er allerede spesifisert av EU og heter Secure Signature Creation Device.

En slik enhet kan også gjenbrukes til private tjenester, og dermed kan brukeren gå med en bærerenhet som lagrer alle tjeneste-nøkler, både til offentlig og privat bruk, og vil kunne gjenbruke enheten overalt. Dette er en av fordelene med å ha en fleksibel og utvidbar løsning. Dette vil også sikre at løsningen har lang levetid og enkelt kan oppgraderes, i takt med nye sikkerhetstrusler.

Videre mener EFN at selv om Nasjonalt ID ikke skulle bli gjennomført, er dette ingen grunn til at politiet ikke skal kunne ha oppgaven med å utdele digitale identifikasjonspapirer på lik linje med pass. Det bør også være en grunnpillar at man ikke krever avgifter for å kommunisere med det offentlige. I motsatt fall vil resultatet kunne bli at ressurssvake vil oppsøke det offentlige direkte eller per telefon og dermed undergrave fordelene med elektroniske offentlige tjenester.

ENKELHET OG BRUKERVENNLIGHET I LØSNINGEN

I høringsforslaget er det gjort en vurdering om at "tungtvint håndtering av eID vil skremme potensielle brukere". Dette vil EFN si seg enig i, dette understreker derfor behovet for at strategien tar hensyn til utvidbarhet og gjenbrukbarhet i løsningen og strategien, samt eID-bæreruavhengighet.

EFN vil imidlertid påpeke at det er flere faktorer som kan skremme bort potensielle brukere av slike tjenester. Først og fremst dårlig brukervennlighet på tjenesten og dårlig organisert og lite tilgjengelig informasjon.

MARKEDSALTERNATIVET

EFN vil advare mot markedsalternativene som beskrives i høringsforslaget. Grunnen til dette er at markedet selv har prøvd å lage og innføre løsninger i over 10 år allerede og ikke klart å få det til i en slik skala som herværende strategi legger opp til. Markedsaktørene har vært for opptatt av å lage noe bare for seg selv, og ikke tenkt på gjenbrukbar arkitektur som alle lett kan koble seg til. Det er derfor bedre at det offentlige nå benytter anledningen til å lage en strategi og løsning som kan utvides og gjenbrukes. Når løsningen uansett skal ut til hele befolkningen, er det ingenting galt i at dens arkitektur og løsningskomponenter kan gjenbrukes av både private, resten av samfunnet og eventuelt i andre lands institusjoner.

I arbeidsgruppens rapport er det påpekt en fare for at staten trer inn som en konkurrerende virksomhet. Men det markedet som eksisterer i dag opererer stort sett mot bedrifter og utgjør dermed ikke konkurrerende virksomhet i seg selv. Ved siden av dette har markedet som nevnt ikke klart å levere løsninger som fungerer godt nok, og dette er grunn god nok til at staten lager en egen løsning for å ivareta sine egne og borgernes interesser.

EFNs høringsuttalelse om eID er utarbeidet av EFNs arbeidsgruppe for digitale signaturer og kryptografi, koordinert og redigert av Thomas Finneid.

EFN er en elektronisk rettighetsorganisasjon som jobber med medborgerskap og juridiske rettigheter i IT-samfunnet.
www.efn.no

Med vennlig hilsen på vegne av EFN,

Thomas Finneid og Thomas Gramstad

Dette dokumentets nettadresse er:
http://efn.no/eid-hoering2007.txt