



Vår saksbehandler
Jan Tobiassen
+47 67 86 40 25
jan@nsm.stat.no

Vår dato
2007-05-14
Tidligere dato
2007-03-12

Vår referanse
2007/00341-2/NSM
Tidligere referanse
200700605-KDB

Til
FAD

Internt

Kopi til
FD

Intern kopi

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

Nasjonal sikkerhetsmyndighet (NSM) viser til deres brev av 12.03.07 der det bes om kommentarer til forslag til strategi for eID og e-signatur i offentlig sektor.

NSM har gått igjennom utkastet til strategi og har først og fremst kommentarer i forbindelse med tillit til løsningen, og håndtering ved kompromittering. Det er en suksessfaktor at sikkerhetsaspekter får tilstrekkelig fokus i tilblivelsen av produkter og løsninger som skal sørge for autentisering.

Videre har NSM kommentarer til kapittel 6 om samtrafikknavn i forhold til Forsvarets etablering av PKI i forsvaret.

Tillit til løsningen avhenger av tilstrekkelig sikkerhet

NSM er positiv til initiativer som forenkler dialogen mellom borgere og det offentlige Norge. Det må være i alles interesse å utnytte teknologien på en optimal måte, noe som videre vil effektivisere prosesser og medføre raskere håndtering av enkeltsaker. Strategien er et positivt bidrag for å finne fremt til nye og mer effektive løsninger.

Et suksesskriterium for at borgere skal ta i bruk nye løsninger som tilbys er at de kan ha full tillit til at opplysninger blir håndtert på en tilstrekkelig forsvarlig måte. Eventuelle kompromitteringer vil kunne medføre at enkeltindivider blir utsatt for ikke-akseptable hendelser, og i verste fall kan det være snakk om tap av liv og helse. Resultatet kan bli at man sitter med løsninger som har kostet mange millioner å etablere, men som ingen ønsker å benytte. For å sikre seg mot dette må det sørges for at beslutningstakerne har en tilstrekkelig sikkerhetsforståelse. Det må velges velprøvde og veldokumenterte tekniske løsninger, og de som avgjør hvilke løsninger som skal benyttes må ha tilstrekkelige kunnskaper om løsningenes egenskaper.

Videre må det vurderes hvordan løsningen skal følges opp med eventuelt tilsyn, testing for å identifisere sikkerhetshull og ikke minst håndtering ved kompromittering.

Interoperabilitet mellom løsninger

Forsvaret er i ferd med å etablere PKI for bruk i forsvaret. Behovet er særlig knyttet til graderte systemer, men det er sannsynlig at forsvaret også vil få sertifikater for bruk i ugraderte løsninger. NSM anbefaler at det sikres tilstrekkelig interoperabilitet slik at brukere som har slik forsvars-ID kan benytte samme elektroniske tjenester som de som har den offentlige eID. Ref. bl.a. kapittel 6 om samtrafikknæv.

Ved etablering av ny offentlig PKI infrastruktur er NSMs råd at man vurderer å ta i bruk de tekniske kravene i veiledningene (NSM Cryptographic Requirements version 2.0 + Digital Certificates and PKI v2.0) utarbeidet av NSM (se www.nsm.stat.no).

NSM har stor kompetanse innen sikkerhet, både teknisk og administrativt. Dette er kompetanse som vil kunne gjenbrukes også på områder utenfor sikkerhetslovens nedslagsfelt. Ved behov og om ønskelig vil NSM, på forespørsel, kunne bistå med råd og veiledning for å få frem en så optimal løsning som mulig med tanke på sikkerhet. Dette gjelder også råd og veiledning i forhold til oppfølging av løsningen med tanke på tilsyn, eventuell penetrasjonstesting og håndtering ved kompromittering.

Med hilsen

Kjetil Storaas Hansen
Direktør