



Vår saksbehandler
Britt Jøsok
67 86 41 21
bjosok@nsm.stat.no

Vår dato
2005-09-21
Tidligere dato
2005-07-11

Vår referanse
2005/01021-002/NSM/008
Tidligere referanse
200502726-2/EAB

Til
Nærings- og handelsdepartementet

Kopi til
Forsvarsdepartementet

Internt

Intern kopi
S3-4

Høring - forslag til forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere (tilbydere av elektroniske signaturer)

Nasjonal sikkerhetsmyndighet (NSM) viser til Deres brev av 11.07.05 der det bes om kommentarer til forslag til forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere.

NSM har gått igjennom utkast til forskrift og har først og fremst kommentarer knyttet til selvdeklarasjonsordningen generelt, sett i sammenheng med formuleringene i formålsbestemmelsen. Videre har NSM en liten kommentar knyttet til utkastet § 7 om krav til meldingens innhold.

Generelt om selvdeklarasjon

NSM merker seg at formålet med forskriften er å høyne sikkerhetsnivået for sertifikattjenester og å øke tilliten til og bruken av slike tjenester. NSM vil i den sammenheng påpeke at det er vanskelig å se at en selvdeklarasjonsordning kan være med på å høyne tilliten til systemet. Etter NSMs oppfatning vil det være vanskelig å etablere full tillit til systemet uten å kreve at en uavhengig tredjepart gjør de nødvendige evalueringer. NSM presiserer at denne vurderingen gjelder uavhengig av om systemet skal inneholde gradert informasjon (iht sikkerhetsloven) eller ikke, og for så vidt uavhengig av hvilken sertifikatklasse man snakker om. Etter NSMs synspunkt er det imidlertid spesielt viktig å unngå selvdeklarasjonsordninger i forhold til sertifikatklasse Person-Høyt, der juridisk bindende kvalifiserte signaturer vil være en del av systemet, og kravene til sikkerhet dermed må være best mulig.

Krav til meldingens innhold

NSM minner om at kommersielle leverandører ikke vil kunne levere PKI for beskyttelse av gradert informasjon iht sikkerhetsloven, og at kravene til slik PKI er uavhengig av denne forskriften. Derimot kan en PKI for beskyttelse av gradert informasjon også brukes i og med offentlig forvaltning. Det kan altså tenkes tilfeller der en ordning som tilfredstiller gradert PKI også ønsker selvdeklarasjon i forhold til denne forskriften. I slike sammenhenger vil det

Postadresse
Postboks 14
1306 BÆRUM
POSTTERMINAL

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

Vedlegg
0

Vår dato
2005-09-21


Vår referanse
2005/01021-002/NSM/008

kunne være vanskelig å oppfylle kravene i § 7 litra c), da sertifikatpraksis er svært sensitiv informasjon. I forbindelse med gradert PKI vil denne sertifikatpraksisen kunne være sikkerhetsgradert etter sikkerhetslovens bestemmelser og vil ikke uten videre kunne utleveres.

For å avhjelpe denne problemstillingen ber NSM om at det vurderes en alternativ ordning i forhold til § 7 litra c). Dersom selve sertifikatpraksisen kan erstattes av en tredjepartserklæring, vil dette problemet kunne løses. NSM ser for seg en form for revisjonsrapport som fastslår at praksisen er i henhold til en viss standard. NSM foreslår derfor en tilføyelse i litra c) : "*...sertifikatpolicy og sertifikatpraksis og/eller en tredjepartserklæring knyttet til disse, samt...*"

Utover dette har NSM ingen merknader til forslaget.

Med hilsen



Jon Enkerud
fungerende Direktør