KREDITTILSYNET
The Financial Supervisory Authority of Norway

Nærings - og handelsdepartementet

Postboks 8014 Dep

0030 OSLO

Saksbehandler:	Anne Karen Seip
Dir. tlf.:	22 93 98 46
Vår referanse:	05/5695
Deres referanse:	
Arkivkode:	008
Dato:	30.09.2005

HØRINGSUTTALELSE OM FORSKRIFT OM FRIVILLIGE SELVDEKLARASJONSORDNINGER FOR SERTIFIKATUTSTEDERE

Kredittilsynet viser til brev fra Nærings- og handelsdepartementet av 11.7.2005 der det er foreslått en forskrift som skal bidra til å høyne sikkerhetsnivået for sertifikattjenester og øke tilliten til og bruken av slike tjenester.

Vi har noen kommentarer til utkastet.

1. Forskriftens utkast til § 1 Formål og virkeområde

Ut fra Kredittilsynets erfaring gir ikke selvdeklarasjoner i seg selv høyere sikkerhetsnivå for sertifikattjenester, slik det beskrives i formålet for forskriften.

Departementet påpeker at en selvdeklarasjonsordning er det minst administrativt krevende som kan innføres, men det går ikke fram om det eventuelt er krevende for foretaket eller departementet. Det er rimelig å forvente at et foretak som tilbyr sertifikattjenester, har gode prosedyrer for utvikling og drift av tjenestene. Samtidig er det ikke dokumentert at samfunnsinteresser alltid er tjent med eller bør evalueres etter om de er minst administrativt krevende.

Evaluering kan defineres som prosessen med å samle bevis for at en sikkerhetstjeneste oppfyller eller ikke oppfyller gitte krav. Grunnlag for å skape tillit til sikkerhetsnivåer i tjenester av ulike slag deles ofte i tre. Man kan

1. Stole på leverandørens forsikringer
2. Utføre egne tester

Postadresse: Postboks 100 Bryn 0611 Oslo
Besøksadresse: Østensjøvelen 43 0667 Oslo
Telefon: 22 93 98 00 Telefaks: 22 63 02 26 Org. nr.: 840747972
post@kredittilsynet.no www.kredittilsynet.no

3. Få uttalelser fra en tredje part.

Selvdeklarasjon kan baseres på alle tre punktene.

Tredjeparten i punkt 3 kan være en bekjent, som bruker det samme systemet, eller et uavhengig organ som er akkreditert til å utføre evalueringer og sertifiseringer av f.eks. produkter, systemer eller administrasjon av informasjonssikkerhet. Evalueringer og sertifiseringer kan følge mer eller mindre velutviklete metoder, og si noe om en tjenestes sikkerhetsnivå, eventuelt hvilket sikkerhetsnivå det aktuelle objektet relaterer seg best til. Dette medfører at tilliten til uttalelser fra en tredjepart vil variere, og kan være avhengig av om man vet hva og hvor godt evalueringen dekker, hvem som betaler for den, om laveste pris for arbeidet er valgt osv.

IT-tilsynet i Kredittilsynet har brukt selvdeklarasjoner i tilsynsarbeidet i 4 år. Institusjoner under tilsyn skal svare på ca. 180 spørsmål[1] og i tillegg sende inn spesifisert dokumentasjon før et stedlig tilsyn. Spørsmålene er relatert til IKT-forskriften og dekker 34 prosesser knyttet til utvikling og drift av institusjonenes IT-systemer. Ca. 120 institusjoner under tilsyn har svart på slike spørsmål.

IT-tilsynet har erfart at

- Alle spørsmål ikke passer like godt for alle institusjoner
- Spørsmålene ikke alltid er godt nok formulert til å avdekke det vi ønsker å få svar på
- Det svares *Ja* steder det burde vært svart *Nei*, og omvendt.

Det gir et bedre bilde av status for tilsynsobjektet når besvarelsene følges opp med møter og personlig kontakt med nøkkelpersoner i institusjonen. Da kan svarene justeres i forhold til innsendt dokumentasjon og ved utdypende intervjuer eller samtaler.

IT-tilsynets spørsmål er i stor grad på et overordnet nivå. De er ikke mange nok til å gi et fullstendig bilde av slike komplekse områder som regelverket vi forvalter, skal dekke. Det medfører at svarene i noen tilfeller kan være uttrykk for subjektiv synsing der det er ønskelig å få fram mer faktapreget informasjon.

Selvdeklarasjon er en subjektiv samsvarsvurdering, og gir etter Kredittilsynets oppfatning ingen garanti for at sikkerhetsnivået for sertifikattjenester blir høyere.

2. Om å følge standarder

Tekniske standarder er ikke statiske, og det varierer hvor relevante de er til en hver tid for systemene som skal benytte dem. I forhold til sikkerhetsstandarder kan spørsmål om en PKI-tjeneste følger f.eks. ETSIs tekniske standard TS 101 456[2], bli for unyansert til å skape tillit. Standarden er stor og kompleks, og noen punkter, som f.eks. nøkkelbruk (key usage), er fortsatt gjenstand for diskusjon i standardiseringsgruppa. Det vil derfor være umulig for en sertifikatutsteder å svare bare *Ja* eller *Nei* til spørsmålet om standarden følges. Selv en beskrivelse av hvordan kravene etter §§ 3, 4 og 5 i den foreslåtte forskriften er oppfylt, kan bli ufullstendig. Det hjelper at avvik skal dokumenteres, men også implementasjonen av en standard vil være gjenstand for diskusjon om hvor godt standarden følges.

Ikke alle områder har velutviklete standarder. Et eksempel er nettsentriske sertifikatløsninger. Kravspesifikasjonen for PKI i offentlig sektor har få standarder å vurdere en slik løsning, og implementasjon av løsningen i forhold til. Det er rimelig å forvente ekstra dokumentasjon for å skape tillit til at en slik løsning gir sertifikatholder kontroll med sertifikatet.

---

[1] *Basert på tilsynsmetoden CobiT, Control Objectives for Information and Related Technology*, som er en internasjonal, anerkjent standard for kontroll og revisjon av IT-organisasjoner og IT-prosesser.

[2] Jfr. Kravspesifikasjon for PKI i offentlig sektor, versjon 1.02, punkt 4.1.5 Krav til sertifikatutsteders virksomhet.

3. Samordning av krav over landegrensene

Kredittilsynet savner en utdyping av problemstillinger knyttet til rettslig anerkjennelse av kvalifiserte sertifikater over landegrensene. Nærings- og handelsdepartementet ser ut til å ha lagt seg på et lavt nivå for å deklarere et sertifikat som kvalifisert ved bare å kreve selvdeklarasjon. Kredittilsynet stiller spørsmål ved hvilke konsekvenser det får nasjonalt og internasjonalt hvis utenlandske sertifikatutstedere bare behøver å avgi en selvdeklarasjon. IT-tilsynets arbeid har vist at det er vanskelig nok for norske foretak å gi korrekte svar. Videre reises det spørsmål om utenlandske foretak vil legge det samme i sine svar som norske utstedere gjør, og hvilke problemer tilsynsmyndigheten kan få i sine vurderinger av tilmeldte sertifikattyper.

4. Tilsynsorganets oppgaver mv.

§ 9 i den foreslåtte forskriften åpner for at Post- og teletilsynet kan nekte oppføring hvis det er åpenbart for tilsynet at en selvdeklarert sertifikattype ikke oppfyller kravene. Det er viktig å være oppmerksom på behovet for ressurser og kompetanse ved innføring av den foreslåtte paragrafen, uavhengig av antallet som vil registrere sertifikater.

5. Forslag til endring av § 10 krav om tilleggsinformasjon

Kredittilsynet foreslår en utvidelse av den foreslåtte § 10. Utvidelsen er understreket.

§ 10 Krav om tilleggsinformasjon mv.

Tilsynsorganet kan kreve at sertifikatutsteder innen en angitt tidsfrist sender inn ytterligere opplysninger dersom melding etter § 7 ikke er fullstendig eller for å kontrollere at selvdeklarert sertifikattype oppfyller kravene etter §§ 3, 4 eller 5. Tilsynsorganet kan eventuelt kreve evaluering fra en uavhengig tredjepart.

Med hilsen

Kredittilsynet

Frank Robert Berg
spesialrådgiver

Anne Karen Seip
seniorrådgiver