Nærings- og handelsdepartementet
Postboks 8014 Dep
0030 OSLO

Vår dato
28.9.2005

Vår referanse
FOB/

Deres dato
11.7.2005

Deres referanse
200502726-2/EAB

Høring – uttalelse vedrørende forslag om frivillige selvdeklarerings-ordninger for sertifikatutstedere (tilbydere av elektroniske signaturer)

ZebSign ønsker med dette å avgi høringssvar til departementets utkast til ny forskrift om frivillige selvdeklarasjonsordninger for sertifikatutstedere. Høringssvaret må ses i sammenheng med Moderniseringsdepartementets høringsnotat om forslag til endring av forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) av 2004-06-25 nr 988. Likelydende brev er derfor sendt til Moderniseringsdepartementet.

1. Innledende

ZebSign forventer leveranse av sertifikater og tjenester til felles offentlig sikkerhetsportal (heretter kalt Sikkerhetsportalen) i henhold til "Rammeavtale om Sikkerhetsportaltjenester". Denne rammeavtalen forutsetter at PKI-tjenester som leveres til Sikkerhetsportalen skal tilfredsstille krav i "Kravspesifikasjon for PKI i offentlig sektor".

Vi må forholde oss til kravene i avtalen, samtidig som vi må ta hensyn til hvordan krav i forslag til forskrift vil påvirke PKI-leverandørenes mulighet til å etterleve kravene. Når det gjelder PKI-leverandører, må vi ta hensyn til både eksisterende og eventuelle nye leverandører som ønsker å integrere sine løsninger i Sikkerhetsportalen.

ZebSign har i dag betydelige leveranseforpliktelser, også til offentlig sektor, og må ta hensyn til at funksjonalitet levert til eksempelvis Rikstrygdeverkets bruksområder skal ivaretas på samme måte som i dag.

2. Generelt

ZebSign og våre underleverandører har behov for trygghet for at krav som stilles til leverandører og tjenester er forutsigbare og at det offentlige utviser betalingsvillighet ved krav om endringer. Dette kan også gjelde ved gjennomføring av godkjenningsprosedyrer, spesielt de nærmeste årene. Det er også behov for ro og stabilitet rundt Kravspesifikasjonen slik at man unngår usikkerhet i forbindelse med etableringen. Forskriftene må bidra til å skape denne tryggheten.

3. Kravspesifikasjon for PKI i offentlig sektor

Det fremgår av forslag til eForvaltningsforskriftens § 27-4 at koordineringsorganet kan bestemme at det ved elektronisk kommunikasjon med og i forvaltningen bare kan benyttes sertifikater som er publisert i henhold til selvdeklareringsforskriften. Ved bruk av PKI i offentlig sektor oppfattes kravspesifikasjonen og selvdeklareringsordningen dermed som obligatorisk krav. Sett fra leverandørene kan valg av ordet "frivillig" virke uheldig eller mindre dekkende.

ZebSign sier seg enig med Statskonsults uttalelse av 10.6.2005 om at det "bør det etableres rutiner for oppdatering av kravspesifikasjonen for PKI i offentlig sektor som omfatter hvilke dokumenter som skal oppdateres, hvor ofte det skal oppdateres, hvem og hvordan nye versjoner skal utarbeides, hvem som skal høres i forbindelse med nye versjoner og hvem som skal ta beslutningen om å godkjenne en ny versjon".

ZebSign mener at dette ikke er tilstrekkelig ivaretatt i de to høringsnotatene. Kravspesifikasjonen bør likestilles med forskrift fastsatt av offentlig myndighet og endringsprosedyrene bør derfor som et minimum følge krav til forskriftsendringer.

I en periode hvor forskriften ikke har vært endret på en stund, jfr. avsnitt 2 ovenfor hvor det påpekes behov for stabilitet, kan det oppstå gap mellom behov for endring og tilsynsmyndighetens tolkning av eksisterende krav. § 27 bør derfor åpne for at det i avtale mellom tilsynsmyndighet og PKI-leverandør kan gjøres unntak fra kravspesifikasjonen.

Mulighet til å gjøre unntak i avtale, må også ses i sammenheng med behov for overgangsordninger, se nærmere om dette nedenfor.

4. Selvdeklarasjonens innhold

ZebSign mener at selvdeklarasjonens innhold bør nyanseres noe mer enn § 3 i forslag til selvdeklarering legger opp til. Det bør være tilstrekkelig at PKI leverandør dokumenterer samsvar mellom krav i kravspesifikasjonen og de tjenester som faktisk tilbys. Som alternativ kan det vurderes om meldingen bør inneholde en oversikt over de punkter som ikke omfattes av deklarasjonen.

5. Behov for overgangsordninger

En forankring av nye krav i Kravspesifikasjonen hos alle berørte parter, samt muligheter til å enes om overgangsordninger er viktig for så vel brukerstedene som PKI-leverandørene. Dersom det stilles krav i spesifikasjonene som medfører at sertifikater ikke kan benyttes i privatmarkedet, er det en risiko for at forvaltningen kan miste tilgang til mange sertifikatbrukere med mindre forvaltningen er villig til å dekke kostnader ved drift og forvaltning av sertifikater som kun kan benyttes i offentlig forvaltning.

Det fremgår av utkast til § 8 i forskrift for selvdeklareringsordninger at tilsynsorganet skal fjerne PKI leverandører fra listen over tilbydere som har sendt melding om oppfyllelse av krav i kravspesifikasjonen for PKI i offentlig sektor, dersom det ikke er sendt ny melding innen tre måneder fra ikrafttredelse av ny versjon av kravspesifikasjonen.

Fristen på tre måneder oppfattes som den tid det forventes at PKI leverandøren skal ha til rådighet ved utarbeidelse av ny dokumentasjon til tilsynet. Siden verken utkast til eForvaltningsforskrift eller selvdeklareringsforskrift inneholder prosedyrebestemmelser mht

hvordan kravspesifikasjonen skal utarbeides og godkjennes, skaper dette utrygghet for i og med at man ikke kjenner omfanget av endringsbehovene og kan risikere at tjenesten blir fjernet fra listen inntil man kan innestå for at alle kravene er oppfylt, herunder har gjennomført nødvendige tilpasninger.

5.1 Hvilke behov må dekkes?

Avhengig av kravene kan PKI-leverandører ha behov for å gjøre endringer i sertifikatprofilene, sertifikatpolicy, teknisk løsning og/eller avtaler med underleverandører og sluttbrukere. Tre måneders tilpasningsperiode er for knapp tid til å gjøre nødvendige tilpasninger med mindre det er fastsatt overgangsordninger.

Sertifikater utstedes vanligvis med to til tre års levetid. Dersom endringskravene i kravspesifikasjonen er absolutte og dette påvirker sertifikatinnhold eller nøkkellagre, må leverandøren enten trekke tilbake sertifikater og utstede nye eller medvirke til at sertifikatene ikke lengre kan benyttes. Sistnevnte er uheldig både for leverandørene og brukerstedene.

Endringer som medfører økte kostnader, medfører behov for reforhandling av avtaler med alle berørte kunder og/eller sluttbrukere med mindre kostnaden dekkes fullt ut av det offentlige. Det må også påregnes endringer i avtaler med kunder og sluttbrukere dersom kravspesifikasjonen påvirker rutinebeskrivelser, sikkerhetskrav, driftsforutsetninger, bruksmønster eller annet som er beskrevet i avtalene.

5.2 Forslag til løsning

Dersom kravspesifikasjonen legges så nært opp til hva som ellers leveres til det private marked, vil endringskrav oftest ikke medføre store endringer og lange overgangsperioder. Tilpasningstiden bør allikevel som et minimum være 6 måneder, men det kan i enkelte tilfeller være behov for inntil 3 år.

I stedet for en eksakt frist for fornyet deklarering, kan behovet for overgangsordning løses på følgende måte:

- KOEF avklarer dette med markedet på forhånd og legger inn overgangsordninger
- Overgangsordninger avtales mellom partene
- PKI-leverandør legger i melding til tilsynet frem en plan for implementering

6. Konklusjon

- Det bør etableres nærmere spesifiserte rutiner for oppdatering av Kravspesifikasjonen for PKI i offentlig sektor, se avsnitt 3 ovenfor.
- Behovet for overgangsordninger må løses, se våre konkrete forslag i punktet ovenfor.

Hvis Nærings- og handelsdepartementet måtte ønske en nærmere utdypning, bistår vi gjerne med ytterligere detaljer.

Med vennlig hilsen
ZebSign AS

Sven Falcke
Administrerende Direktør