Bankenes BetalingsSentral AS
Postadresse:
0045 OSLO
Besøksadresse:
Haavard Martinsens vei 54
Rommen, Oslo
Telefon: 22 89 89 89
Telefax: 22 81 64 54
Foretaksregisteret:
NO975 946 231
www.bbs.no

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep
0030 Oslo

Att:

Deres referanse:	Saksbehandler :	Oslo
200700605-KDB	Birgith Klingenberg	14. mai 2007

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

Vi viser til høringsbrev av 12. mars 2007. Bankenes Betalingssentral AS (BBS) ønsker med dette å avgi høringssvar til departementets forslag til strategi.

1. Bakgrunn

BBS leverer og drifter løsninger for utstedelse og bruk av personsertifikater på flere nivåer og virksomhetssertifikater deklarert i samsvar med selvdeklarasjons-forskriften, og kan tilby løsninger for samtrafikk. Vi drifter blant annet PKI-løsninger for norske og utenlandske virksomheter, herunder BankID.

2. Generelt

Strategien innebærer en forskyvning av bruksområder for digitale signaturer i retning av utstrakt bruk av elektroniske signaturer, fortrinnsvis uten bruk av PKI. Dette mener vi er uheldig. Forslag til strategi påvirker først og fremst sertifikater av typen Person Standard. I Norge er denne sertifikattypen godt innarbeidet og standardisert gjennom SEID/ Kravspesifikasjon for PKI. Person Standard sertifikater er etablert i markedet og er en rimelig løsning for brukerstedene. Det vil derfor representere et sikkerhetstap hvis denne sertifikattypen skulle forsvinne.

Når det gjelder innholdet i forslag til strategi mener vi at den bør fokusere på "bruk av eID", eller alternativt "strategi for utbredelse av PKI-anvendelse" . Selv om begrepene er benyttet i utkast til strategi er dette likevel ikke beskrevet i det omfang som vi forventet. Vi mener også at det eksisterer gode eID løsninger på markedet som det offentlige bør benytte fremfor å utvikle nye løsninger da vi mener at dette gir størst samfunnsøkonomisk gevinst.

Inntil det offentlige har fastsatt forpliktende planer som fokuserer på konkrete behov og anvendelse i offentlig sektor, vil befolkningens og samfunnets nytte av strategien være begrenset og vi antar at privat sektors implementeringer og de derigjennom etablerte faktiske standarder derfor vil bli toneangivende for valg av eID løsninger.

I vår høringsuttalelse har vi valgt å kommentere følgende punkter nærmere:

- Definisjon og bruk av sikkerhetsnivåene
- Roller og ansvar
- Forretningsmodell
- Forholdet til markedet

3. Definisjon og bruk av sikkerhetsnivåene

Strategiens innføring av nye begreper skaper forvirring. Dette gjelder særlig de nye sikkerhetsnivåene og forholdet til selvdeklareringsforskriften.

Det offentlige ser for seg fire sikkerhetsnivåer, der kun sikkerhetsnivå 4 har krav til bruk av PKI. Utkast til strategi sier videre at de fleste tjenester vil kunne operere på sikkerhetsnivå 3 (samme type id som brukes på MinSide i dag), altså vil det være svært få som har behov for nivå 4, men helsesektoren nevnes som et slikt område.

Forvirringen gjelder spesielt nivå 3 som favner flere sikkerhetsløsninger som ikke ligger på samme sikkerhetsnivå. Dersom strategien differensieres på anvendelse av sikkerhetsnivåene i forhold til etatenes konkrete behov vil dette gi bedre oversikt og forutberegnelighet for partene. Det må drøftes hvorvidt det er hensiktsmessig å definere ett sikkerhetsnivå pr. likestilt sikkerhetsløsning. Vi mener at Person Standard har sikkerhetsmekanismer som kvalifiserer til et høyere sikkerhetsnivå enn de øvrige. Siden Person Standard er innarbeidet i Kravspesifikasjonen for PKI i offentlig sektor, mener vi at det er viktig å beholde dette nivået som et eget sikkerhetsnivå. Videre bør det konkretiseres hvilke tjenester som skal benytte hvilke sikkerhetsnivåer.

4. Roller og ansvar

Strategien representer et lavt ambisjonsnivå for PKI i det offentlige. I samsvar med strategien legges det opp til samordningsgrep for eID på sikkerhetsnivå 3 (Altinn/Skatt) og først senere en utvikling som leder an til at sikkerhetsnivå 4 gradvis vil overta fra 2009 og utover. Dette lave ambisjonsnivået er ikke i samsvar med de planer som tidligere er publisert og som næringen har gjennomført store investeringer for å tilpasse seg.

4.1. Statens rolle

Statens rolle er blant annet å tilrettelegge for publikumstjenestene eller som det tidligere er kommunisert en døgnåpen elektronisk forvaltning. For å sikre at tjenestene kan legges ut i en elektronisk løsning på en trygg og god måte er det behov for en standardisert sikkerhetsinfrastruktur og standardiserte beskrivelser av hvilke sikkerhetsløsninger som kan benyttes i en mange til mange kommunikasjon i offentlig sektor.

For å få dette til må staten være villig til å legge ned vesentlige ressurser (tid, penger og kunnskap) for å få dette til, og være pådriver for utbredelse og bruk. Vi mener at utkast til strategi ikke gir en tilstrekkelig forsikring om at staten har en slik rolle.

Det finnes mange kvalifiserte aktører som kan dekke det offentliges behov i markedet og som kan bidra til å redusere kostnadene, såfremt det offentlige er villig til å ta de rette beslutningene, herunder være mer tydelig på sin rolle og ansvar.

Vi støtter forslaget om å opprette et samtrafikknav som forvaltes av Brønnøysundregistrene da dette vil kunne bidra positivt til den standardiseringen som det er behov for.

5. Ansvar og forretningsmodeller for Samtrafikknavet

Vi ser at fortsatt det kan være utfordringer med hensyn til spørsmål om ansvar og forretningsmodell ved videreformidling av eID.

I tillegg til Samtrafikknavet, kan det være opp til 4-5 andre parter involvert eksempelvis ID-leverandør, driftsleverandør, brukersteder, sertifikatinnehaver og betalingsløsninger.

Det legges opp til ikke-kommersielle avtaler mellom ID-leverandør og Samtrafikknavet (Brønnøysundregistrene). Det bør avklares om dette aksepteres av eID leverandørene.

Vi mener at ansvarsforholdene må tydeliggjøres og forretningsmodellene gjennomgås.

6. Forholdet til markedet

Det offentlige stiller strenge krav til teknologi og infrastruktur i kravspesifikasjon for PKI i offentlig sektor og krav om "frivillig sertifisering" etter selvdeklarerings-forskriften. Staten legger imidlertid ikke opp til en utbredelse som forsvarer den investering leverandørene har hatt ved å tilpasse seg disse absolutte kravene over en lengre periode.

Dersom staten skal lykkes med hensyn til å ta i bruk eID løsninger på en kostnadseffektiv og samfunnsøkonomisk god måte, må det offentlige være villig til påta seg volumforpliktelser ved kjøp av tjenester da dette gir større risikovilje og lavere priser fra leverandørene. Løsningene er tilgjengelige, men kravene må koordineres bedre og staten og kommunene må tilstrebe at strategien holdes noenlunde fast i en periode på 3-5 år, samt at den følges av statlige og kommunale brukersteder.

Med vennlig hilsen
for BBS/ZebSign

Sven Falcke
Director Tillitstjenester
BBS AS