

Mandat for felles kravspesifikasjon for PKI i offentlig sektor (AFPKI). 25.8.2004.

Bakgrunn

Regjeringen ønsker å utløse potensialet for flere offentlige elektroniske tjenester som gir muligheter for en enklere hverdag for borgerne og næringsliv og en effektivisering av offentlig forvaltning. Elektronisk ID og signatur sees i økende grad som en grunnleggende forutsetning for effektiv elektronisk samhandling med borgere og næringslivet. Det er viktig å etablere elektronisk saksbehandling med elektronisk signatur som garanti for rettsikkerhet og gyldighet. Dette krever stor innsats i mange deler av forvaltningen.

Mål

For å oppnå størst mulig forenkling for offentlige virksomheter som ønsker å ta i bruk elektronisk ID og signatur, samt for å sikre samtrafikk og samhandling på tvers av ulike løsninger, har Regjeringen besluttet at det skal utarbeides en felles kravspesifikasjon for elektronisk ID og signatur for offentlig sektor. Kravspesifikasjonen skal foreligge innen den 15. november 2004, og skal baseres på spesifikasjonsarbeidet gjort bl.a. i Altinn og andre relevante prosjekter. Kravspesifikasjonen skal dekke behovet for elektronisk ID og signatur, samt konfidensialitet, der dette behovet ikke dekkes på andre måter, i statlig og kommunal forvaltning i forbindelse med:

- elektroniske tjenester, for publikum og næringsliv,
- elektronisk innrapportering til det offentlige,
- elektronisk dokumentutveksling mellom offentlige, og mellom offentlige og private virksomheter, både på virksomhet- og på ansattnivå
- tilgang til oppslag i sentrale grunndata registre (slik som folkeregisteret) og
- elektronisk saksbehandling i offentlige virksomheter.

Kravspesifikasjonen skal kunne forenkle vurderinger rundt valg av sikkerhetsmekanismer for ulike tjenester. Anvendelse av spesifikasjonen skal samtidig sikre størst mulig brukervennlighet ved at samme sikkerhetsløsning kan brukes på tvers av tjenesteytere.

Forutsetninger

- Infrastrukturen for eID og signatur skal leveres av markedet
- Det er ønskelig med virksom konkurranse i dette markedet
- Det må foretas nødvendig avveining mellom kostnaden ved å ta i bruk og bruke eID og signatur (dette omfatter investeringskostnad og tid som medgår til anskaffelsen), brukervennligheten av løsningen og sikkerhetsnivåer den representerer
- Den eID som en bruker vil anskaffe skal gi størst mulig nytte, dvs. skal kunne brukes mot flest mulig elektroniske tjenester, både offentlige, men også private, der eID eller e-signatur er påkrevet
- Det skal være enkelt for en bruker å forholde seg til de rettslige/avtalemessige forhold knyttet til bruken av en eID eller signatur
- Det skal inngås rammeavtaler til bruk i hele offentlig sektor på grunnlag av kravspesifikasjonen

Rammer for arbeidet

Arbeidet med en kravspesifikasjon skal skje innenfor følgende rammer:

1. Kravene skal i størst mulig grad dekke behovene for elektronisk ID, signatur og kryptering i Altinn og Helsenet. Øvrige behov defineres av arbeidsgruppen.
2. Kravene skal utformes slik at de åpner for bruk av ulike prismodeller og anskaffelsesmodeller.
3. Kravene bør ikke utelukke eksisterende produkter eller tjenester fra utstedere av aktuelle sertifikater, særlig der antallet sertifikater i markedet er stort
4. Kravene skal så langt mulig følge anbefalingene fra SEID-prosjektet¹ samt relevante internasjonale standarder.
5. Kravspesifikasjonen skal også dekke konfidensialitetsbehov som f. eks. kan knyttes til taushetsplikten iht forvaltningsloven og unntaksbestemmelser i offentlighetsloven, samt bestemmelser i personopplysningsloven.

Arbeidet skal **avgrenses** mot følgende punkter:

6. Kravspesifikasjonen skal ikke ta spesielt hensyn til konfidensialitetsbehov som følger av sikkerhetsloven og beskyttelsesinstruksen – delen som gjelder elektronisk dokumenthåndtering.
7. Kravspesifikasjonen skal ikke dekke andre typer sikkerhetsløsninger enn PKI.
8. Kravspesifikasjonen skal ikke spesifisere krav i forbindelse med tjenester for tidsstempling, dersom de ikke er knyttet til autentiserings- og signeringsfunksjoner.
9. Kravspesifikasjonen skal heller ikke omfatte sertifikattyper (for eksempel attributtsertifikater) som ikke pt. støttes av standard løsninger.
10. Spesifikasjonen har ikke til hensikt å berøre bruk av PKI i VPN-sammenheng, bruk av SSL, signering av programkode mv.

Deloppgaver

1. Det skal utarbeides en systematisert oversikt over behovene for elektronisk ID og signatur i offentlig forvaltning, representert ved de virksomheter som deltar i arbeidet, basert på tilgjengelig dokumentasjon fra etatene.
2. Det skal beskrives ett eller flere sikkerhetsnivåer for elektronisk ID og signatur samt konfidensialitet, som dekker behovene i offentlig forvaltning. Sikkerhetsnivåene skal spesifisere hva slags bruk nivået er tilegnet og enkel funksjonell beskrivelse av mulige løsninger for nivået. Arbeidet vil ta utgangspunkt i et utkast utarbeidet av AAD.
3. Det skal utarbeides krav til både personsertifikater og virksomhetssertifikater (se definisjoner nederst). Krav til ansattsertifikater taes med bare hvis behovet konkluderes i deloppgave 1. Kravene skal formuleres på funksjonelt nivå så langt mulig. Kravene skal ta hensyn til ulike modeller for brukeradministrasjon.

Arbeidsmåte

Arbeidsgruppen møtes jevnlig til dagslange workshop-møter der kravspesifikasjonsdokumentet gjennomgås og revideres. Ansvarlig redaktør implementerer endringene i etterkant av møtet og ny versjon sendes ut forut for neste møte. Det skal benyttes endringsmarkering og versjonsstyring av dokumenter. Alle krav skal være nummerert og tilordnet prioritet. Gruppens medlemmer skal ha lest gjennom foreliggende utkast til møter og være i stand til kort å redegjøre for egne forslag til endringer på møtene.

¹ Se <http://www.pki-forum/seid>

Dokumentet skal kvalitetssikres gjennom høring i referansegruppen og ved at en ekspert på området gjennomgår utkastet før høringen.

Organisering og fremdriftsplan

Arbeidet organiseres i et prosjekt. Eieren av prosjektet er Koordineringsorganet for PKI i offentlig sektor. Prosjektet består av en arbeidsgruppe (se vedlegg) som ledes av Katarina de Brisis, NHD/MOD. Lise Arneberg, AAD/MOD er gruppens sekretær og ansvarlig redaktør for kravspesifikasjonsdokumentet. Prosjektet har også en referansegruppe, som i hovedsak utgjøres av Samordningsgruppen under Koordineringsorganet for PKI, supplert med noen observatører. I tillegg hyrer prosjektet inn en ekstern konsulent for kvalitetssikring av kravspesifikasjonsdokumentet.

18. august 2004 kl. 10-15 holdes oppstartsmøte i arbeidsgruppen.

Det planlegges deretter å holde 1 møte i uken, som hovedregel. Møtene holdes på onsdager, kl. 10-15, i regjeringskvartalet i Oslo. Endelig møteplan fastsettes på oppstartsmøtet.

20. september 2004 Utkast til anbefalte sikkerhetsnivåer

20. september - 10. oktober 2004 Høring/kvalitetssikring av sikkerhetsnivåer

15. oktober 2004 Kravspesifikasjonen foreligger i et høringsutkast.

15. oktober – 1. november 2004 Høring/kvalitetssikring av utkastet.

1. november – 15. november 2004 Endelig utkast til kravspesifikasjon utarbeides.

15. november 2004 Kravspesifikasjonen foreligger for godkjenning og behandling i Koordineringsorganet for PKI.

Budsjett

Prosjektet disponerer et eget budsjett på kr. 200.000. Budsjettet skal benyttes til dekning av møteutgifter, innleie av konsulent og dekning av reiseutgifter til deltakere i Arbeidsgruppen utenfra Oslo, etter nærmere avtale med gruppelederen.

Definisjoner

Personsertifikat er et sertifikat hvor sertifikatinnehaber er en fysisk person.

Virksomhetssertifikat har som oppgave å identifisere en juridisk person, dvs en virksomhet som er registrert i det norske enhetsregisteret. Bruker av den private nøkkel assosiert med sertifikatet kan være en fysisk person autorisert av virksomheten eller en automatisert prosess under foretakets kontroll, for eksempel en server.

Ansatt-sertifikat er et personsertifikat, som attesterer at det finnes en relasjon mellom en identifisert virksomhet og en entydig identifisert person innenfor denne virksomheten. Relasjonen vil typisk være et ansettelsesforhold, men dette er ikke et krav.

Grunnlagsdokumenter

Følgende dokumentasjon danner grunnlaget for arbeidet med kravspesifikasjonen:

- Altinn generelle kravspesifikasjon
- Helsenetts spesifisering
- Forvaltningsnettets utkast til kravspesifikasjon fra høsten 2002.
- Lånkassens tilpasningsspesifisering for Altinn (forbehold om godkjenning fra Lånkassen).

I tillegg, som bakgrunnsdokumentasjon, kommer aktuelle internasjonale standarder eller utkast til standarder, internasjonale felles krav til PKI-løsninger og andre relevante dokumenter. All dokumentasjon er lagret på web-arbeidsplassen under www.kunnskapsnettverk.no.

AFPKI medlemsliste

Leder NHD/MOD: Katarina de Brisis

Sekretær AAD/MOD: Lise Arneberg

Nærings- og handelsdepartementet: Thomas Myhr

Brønnøysundregistrene: Hilde Storvig/ Dørthe Korner (Alternerer)

Altinn forvaltningsorganisasjon: Pål Kristoffersen

Skattedirektoratet: Jan Henrik Stubberud og Arne Thorstensen (Alternerer)

Statens lånekasse for utdanning: Hans Petter Nyberg og Ingrid Holen (Alternerer)

Senter for statlig økonomistyring: Jan-Bjørn Mortensen

Statistisk sentralbyrå: Magne Hopland

Sosial- og helsedirektoratet: Arnstein Vestad (KITH)

Domstolsadministrasjonen: Ole Martin Hole

Undervisnings- og forskningsdepartementet v/FEIDE: Jon Strømme

Trondheim kommune: Anne Hofstad

Politidirektoratet: Eric Gonçalves og xxx (Alternerer)

AAD/MOD: Kristian Bergem

