Behov for sertifikattjenester for norsk offentlig sektor

OMNI/03/99

Jon Ølnes

Desember 1999

Norsk Regnesentral
ANVENDT DATAFORSKNING

NR-notat/NR Note

Tittel/Title:
Behov for sertifikattjenester for norsk offentlig sektor

Dato/Date: 10. desember
År/Year: 1999
Notat nr: OMNI/03/99
Note no:

Forfatter/Author:
Jon Ølnes

Sammendrag/Abstract:
Dette notatet ser på behov for sertifikattjenester (offentlig-nøkkel sertifikater) og tilhørende policyer internt i offentlig sektor, i tillegg til det som tilbys gjennom Forvaltningsnettsamar-beidets rammeavtaler og FSP-1 policy. Notatet diskuterer også krav til tjenester og policy på grenseflaten mellom offentlig og privat sektor (privatpersoner og bedrifter).
Konklusjonene er at FSP-1-nivå og smartkort må kreves for digitale signaturer, men at det er behov for rammepolicyer som stiller krav til enklere tjenester for sikker Web-aksess, VPN og tunnelløsninger. Slike rammepolicyer kan dekke behov både internt i offentlig sektor og mot privat sektor. Det anbefales ikke at det offentlige etablerer tjenester selv. Isteden kan en lisensiere de tjenestetilbyderne som oppfyller kravene nedfelt i rammepolicyene.
Offentlige Web-tjenester som tilbyr annet enn åpen informasjon vil trenge sertifikater. Slike kan skaffes fra dagens tjenester på Internett, eller fra norske leverandører som kan tilby dette.
Det er behov for rollesertifikater / autorisasjonssertifikater både i offentlig og privat sektor, men her er standardiseringsarbeidet kommet såpass kort at det ikke er mulig å lage noen generell løsning nå. Der det er behov for denne typen sertifikater, må problemene løses for hvert enkelt tilfelle separat. Det offentlige kan stille opp krav til kvaliteten på sertifikattjenester, og kan eventuelt også gi noen spesifikasjoner for sertifikatprofiler.
Som en siste konklusjon pekes det på behovet for løsninger som tillater digitale signaturer og bruk av smartkort med tynne klienter. Her er imidlertid FSP-1 dekkende som policy.
Notatets oppsummeringskapittel kan leses som et «executive summary» av innholdet.

Emneord/Keywords: Sertifikatpolicy, sertifikat, X.509, PKI, offentlig-nøkkel, Forvaltningsnettsamarbeidet, FNS, digital signatur, kryptering,

Tilgjengelighet/Availability: Åpen

Prosjektnr./Project no.: 88000

Satsningsfelt/Research field: Sikkerhet

Antall sider/No. of pages: 16

Norsk Regnesentral / Norwegian Computing Center
Gaustadalléen 23, Postboks 114 Blindern, 0314 Oslo, Norway
Telefon 22 85 25 00, telefax 22 69 76 60
http://www.nr.no

Innhold

1. Innledning

1.1. Krav til forkunnskaper

Dette notatet går forholdsvis rett på sak når det gjelder problemstillingene. Det forutsetter basis kunnskaper om offentlig-nøkkel infrastruktur (PKI) og annen teknologi som omtales, om Forvaltningsnettsamarbeidet (FNS)[1], og om nasjonale forhold innen PKI. FNS har utgitt en veileder[2] som kan brukes som introduksjonsmateriale.

1.2. Utgangspunkt i FNS

Forvaltningsnettsamarbeidet (FNS) har inngått rammeavtale med tre leverandører av TTP-tjenester for utstedelse av digitale sertifikater, m.a.o. PKI-tjenester. Disse tjenestene opererer under en felles sertifikatpolicy, FSP-1 (Forvaltningsnettsamarbeidets Sertifikat-Policy nr. 1)[3]. Det primære mål for avtalene er å understøtte bruk av digitale signaturer i forvaltningen. FSP-1 er derfor primært en policy for «formelle» digitale signaturer, på nivå med de krav EU stiller[4] eller vil stille i forbindelse med såkalte kvalifiserte sertifikater[5]. FSP-1 støtter også sertifikater for virksomheter, organisasjonsenheter innen virksomheter og roller innen virksomheter. FSP-1 etablerer en kopling mellom subjektet i sertifikatet og en virksomhet, og atskiller seg derfor fra prosjekter for personlig elektronisk identitetsbevis, som har vært sterkest i fokus spesielt i Sverige og Finland (se 3.2.3).
FNS-avtalene kan kun brukes av virksomheter innen offentlig sektor (med noen unntak – enkelte private virksomheter f. eks. innen helsevesenet kan få adgang til bruk). FSP-1 gjelder også i utgangspunktet kun for offentlig sektor, og for sertifikater som er utstedt i sammenheng med bruk av FNS-avtalene. Men en tilsiktet bieffekt av FNS-avtalene og FSP-1 er at disse skal ha en standardiserende effekt, slik at leverandørene forhåpentligvis vil ønske å tilby tjenester basert på dette arbeidet også for private bedrifter.

1.3. Problemområde for dette notatet

Problemstillingen for dette notatet er det offentliges egne behov for sertifikater og sertifikat-tjenester i tillegg til det som dekkes opp av FSP-1 og FNS-rammeavtalene. I tillegg gis en vurdering av hvilke krav det offentlige bør stille når det gjelder PKI-tjenester for sikring av kommunikasjon mellom privat og offentlig sektor. Privat sektor omfatter både private bedrifter og privatpersoner.
Notatet er skrevet av NR[6] på oppdrag fra AAD, som har initiert arbeid med utredning av en offentlig PKI-politikk. Notatet skal være et grunnlagsdokument for dette arbeidet. Det pågår en god del

[1] Se http://forvaltningsnett.dep.no – her er også FNS rapporter og andre dokumenter tilgjengeliggjort.

[2] «Anskaffelse og innføring av tiltrodde tredjepartstjenester og digital signatur», Forvaltningsnettsamarbeidet rapport 12/99. Også tilgjengelig fra FNS' nettsted.

[3] «Forvaltningsnettsamarbeidets SertifikatPolicy – Nr. 1 (FSP-1:1.0): Høysikkerhets sertifikatpolicy for utstedelse av X.509-baserte sertifikater for personer og virksomheter i norsk offentlig forvaltning», Forvaltningsnettsamarbeidet rapport 8/99. Også tilgjengelig fra FNS' nettsted.

[4] EU Common Position No 28/1999 – nylig vedtatt EU-direktiv om elektroniske signaturer.

[5] Et kvalifisert sertifikat er et sertifkat som understøtter en signatur som kan betraktes som ekvivalent til en håndskrevet signatur på et nærmere angitt lovområde. Det stilles særskilte krav til innholdet i et kvalifisert sertifikat, til sertifikatutstederen, og til utstyret / programvaren som skal produsere signaturene.

[6] Alle synspunkter i notatet står for NRs regning, og reflekterer ikke nødvendigvis det AAD eller andre offentlige virksomheter måtte mene.

annet arbeid innen dette feltet i offentlig sektor, delvis som oppfølging av RITS' (Rådet for IT-Sikkerhet) rapport om digitale signaturer[7]. Ett tiltak er en lovgjennomgang med sikte på å fjerne unødvendige hindringer for elektronisk kommunikasjon. Et annet, som er spesielt relevant for dette notatet, er «Torvund-utvalget»[8] som skal se på:

- Frivillig godkjenningsordning for TTP-virksomhet og krav til slik virksomhet,
- Anerkjennelse av sertifikater (på tvers av leverandører i Norge, og internasjonalt),
- Roller i markedet – spesielt hvilke som skal spilles av myndighetene,
- Tilhørende problemstillinger som finansiering og økonomiske / adminstrative konsekvenser.

Torvund-utvalget skal legge fram sin innstilling innen utgangen av 1999. Dette notatet er ikke koordinert med Torvund-utvalget, men notatet går bevisst ikke i dybden i problemstillinger som forventes diskutert av Torvund-utvalget.

Viktigste fokus for Torvund-utvalget og annet arbeid er digital signatur, samme område som FNS-avtalene og FSP-1 dekker. Dette notatet ser imidlertid også på andre anvendelser av offentlig-nøkkel teknologi, sertifikater og PKI-tjenester.

Dette notatet vil ikke komme inn på tiltak innen rent privat sektor, ut over å konstatere at de spesifikasjoner og valg som offentlig sektor gjør, vil ha en meget stor påvirkningskraft. En løsning som virker mellom privat og offentlig sektor, vil også virke mellom kun private aktører. En ønsket bieffekt av FNS-avtalene og FSP-1 er at dette skal sette norsk standard[9] innen området. Dette bør også være en ønsket effekt av andre offentlige initiativer innen området.

1.4. Noen observasjoner

Noen viktige observasjoner kan gjøres allerede her, siden de gir viktige premisser for resten av notatet:

1. Det offentlige er den viktigste premissgiver til arbeidet med sikring av elektronisk kommunikasjon i Norge. Offentlig sektor kan, i kraft av sin størrelse, «tvinge» leverandører til å tilby tjenester og produkter etter de ønskede spesifikasjonene. Forutsetningen er selvsagt at offentlig sektor opptrer koordinert, som gjennom FNS.
2. En løsning som tilfredsstiller behov internt i offentlig sektor, kan påregnes også å fungere i de fleste private bedrifter.
3. Det offentlige bør derfor utvikle spesifikasjoner som dekker eget behov, men som i tillegg er generelle nok til å ha bredere anvendelse. Dette kan gi en standardiseringseffekt, og vil gjøre det enkelt for leverandører å tilby (tilnærmet) samme tjenester og produkter til private kunder.
4. Arbeidet med spesifikasjoner bør gå parallelt med arbeid med akkrediterings- og sertifiseringsordninger[10] for IT-sikkerhet. Disse ordningene kan dermed forholde seg til konkrete spesifikasjoner.

[7] «Digitale signaturer gir tillit til elektronisk kommunikasjon: Forslag til tiltak for aksept og utbredelse», RITS-raport, november 1998. Tilgjengelig fra http://www.odin.dep.no/nhd/publ/esign

[8] Se http://www.odin.dep.no/nhd/publ/esign/mandat.html

[9] I denne omgang kun i betydningen «de facto» standard. Det er foreløpig ikke tatt initiativer fra FNS eller AAD for å få definert offisielle norske standarder eller profiler basert på FNS' spesifikasjoner.

[10] Se bl.a. «Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner», rapport fra RITS (Rådet for IT-Sikkerhet), november 1997.

2. Sertifikater internt i offentlig sektor

2.1. Hva dekkes av FSP-1

2.1.1. Ansattsertifikater

FSP-1, og FNS-rammeavtalene, dekker behovet for «formelle» digitale signaturer innen offentlig forvaltning gjennom personlige ansattsertifikater. Behovet for kryptering av meldinger er også dekket. FSP-1 krever tre nøkkelpar og sertifikater for hver bruker: Digital signatur, (nøkkelutveksling for) kryptering, og autentisering. Bruken av nøkkelparet for autentisering er ikke spesifisert i FNS. Tanken er at dette skal kunne brukes ved pålogging, lokalt eller over nettverk, og for autentisering ved aksess til tjenester i nettverk. FSP-1 krever smartkort (eller tilsvarende, f. eks. PCMCIA-kort) for beskyttelse av private nøkler og annen sikkerhetskritisk informasjon.

2.1.2. Virksomhetssertifikater

FSP-1 dekker i tillegg opp sikring av meldinger til / fra virksomheter, organisasjonsenheter og roller. Normalt vil dette brukes på nøyaktig samme måte som sikring av meldinger mellom personer, gjennom digitale signaturer og kryptering. Men tanken er at denne formen for sertifikater også skal dekke opp de behovene som kom fram under arbeidet med FNS-ramme-avtalene innen elektronisk datautveksling og EDI, nemlig meldinger til (og delvis også fra) en tjeneste. FSP-1 anbefaler bruk av spesialelektronikk for beskyttelse av private nøkler, eventuelt kan en bruke smartkort. Dersom systemet som tilbyr tjenesten er meget godt sikret, godtas rene programvareløsninger med private nøkler lagret i hukommelse / på disk.

2.1.3. Profesjonssertifikater

FSP-1 dekker også et behov, framsatt av helsesektoren, for profesjonssertifikater. Disse brukes på samme måte som ansattsertifikater. Personenes tilknytning er imidlertid ikke til en arbeidsgiver, men til en autoritet som godkjenner profesjonsrettigheter, f. eks. for helsepersonell. Sertifikatene har et unikt nummer som angir dette, f. eks. helsepersonell-nummer. I tillegg har sertifikatene et tittelfelt som gir en tekstlig beskrivelse av profesjonen[11]. Denne beskrivelsen egner seg ikke for maskinell behandling, men kan brukes av en menneskelig mottaker for å bestemme autorisasjoner. Autorisasjoner må ellers sjekkes ved å sammenholde informasjonen i sertifikatene med informasjon i et register (f. eks. helse-personellregisteret). FSP-1 stiller krav om bruk av smartkort i forbindelse med profesjons-sertifikater.

2.2. Er FSP-1 tilstrekkelig innen sine områder

FSP-1 er, som undertittelen indikerer, en høysikkerhets policy. Men høy sikkerhet innebærer også høye kostnader, og spørsmålet er om en i noen sammenhenger kan greie seg med enklere og billigere alternativer. Typisk vil billigere alternativer stille mindre strenge krav til PKI-tjenestene, og en vil gjerne vurdere om bruk av smartkort er nødvendig. Merk at løsninger uten bruk av smartkort er i pilotdrift i dag, både i EDNA-prosjektet[12] i Kommunal og Regionaldepartementet, og i prosjekter i regi av Rikstrygdeverket.

[11] F. eks. «Lege, spesialist indremedisin».

[12] EDNA-prosjektet er i ferd med å gå over til bruk av smartkort.

Når det gjelder funksjonen for digital signatur («non-repudiation» angitt som formål i sertifikater), vil vi ikke anbefale at offentlig sektor går inn på avtaler som gir dårligere sikkerhet enn FSP-1. Argumentasjonen er:

1. Dersom en offentlig ansatt likevel trenger smartkort og sertifikater etter FSP-1, vil det være fordyrende og kompliserende om den samme ansatte også skal bruke andre løsninger.
2. Dersom en tilbyr svakere løsninger, er risikoen at disse vil bli valgt også der en egentlig hadde behov for tjenester på nivå med FSP-1, og dermed blir sikkerheten innen offentlig sektor svekket.

Vi legger da til grunn at tjenester på nivå med FSP-1 er nødvendig for å understøtte EU-direktivet om kvalifiserte sertifikater og tilsvarende norske lover og regelverk. Nasjonal sikkerhetsmyndighet, FO/S, har også uttalt[13] at de mener at smartkort eller tilsvarende er nødvendig for å oppnå tilstrekkelig sikkerhetsnivå for digital signatur.

Anbefalingen er altså at dersom offentlige virksomheter har behov for / ønske om å kjøpe produkter og tjenester for digital signatur og meldingskryptering, så skal PKI-tjenestene være på nivå med FSP-1, og det skal benyttes smartkort eller tilsvarende.

Bruk av autentiseringsfunksjonen i FSP-1 er ikke spesifisert innen FNS i dag, og som vi skal se nedenfor, er det her rom for alternative løsninger.

2.3. Hva dekkes ikke av FNS og FSP-1

2.3.1. Nettverkssikkerhet

Ett viktig område som ikke er dekket av nåværende spesifikasjoner for sertifikattjenester, er nettverkssikkerhet – opprettelse av en autentisert og beskyttet kommunikasjonskanal mellom to parter. Her er det flere løsninger, og eksemplene nedenfor kan faktisk allerede kjøpes over andre rammeavtaler innen FNS:

- VPN (virtuelle private nett) er etablering av en «lukket brukergruppe», der autentisering og kryptering vanligvis foregår mellom aktørenes rutere eller brannmurer.
- Tunnelløsninger brukes for en sikret kanal mot en spesifikk motpart, særlig for forbindelser fra hjemme-PC eller bærbart utstyr mot arbeidsplassen.
- Sikker Web-aksess etablerer en sikret kommunikasjonskanal mellom en nettleser og en Web-tjener.

VPN

Standardløsninger for VPN vil på sikt basere seg på IPSec-spesifikasjonene[14]. Typisk vil autentisering og nøkkelutveksling foregå ved hjelp av offentlig-nøkkel kryptografi mellom de maskinene (rutere, brannmurer mm.) som er involvert. Disse maskinene vil da trenge nøkkelpar og sertifikater. VPN-løsninger kjøpes i dag typisk fra én leverandør, og leveransen inkluderer nøkler og sertifikater ferdig installert. Det er ønskelig med en enkel policy som angir krav til sikkerhet i prosedyrene for nøkkelgenerering, beskyttelse av nøkler og sertifisering. Det trenger ikke være noen krav om at sertifikater skal utstedes fra en lisensiert sertifikattjeneste, men dersom et VPN skal kunne bygges med komponenter fra forskjellige leverandører, kan likevel dette være ønskelig.

[13] Møte med FO/S holdt under arbeidet med spesifikasjonene for FNS-rammeavtalene.

[14] «Security Architecture for the Internet Protocol», RFC2401, november 1998.

SSL

Både tunnelløsninger og sikker Web-aksess vil normalt bruke SSL[15] (Secure Sockets Layer) protokollen. Tunnelløsninger vil bruke SSL fra den programvaren som etablerer forbindelsen, og normalt vil begge maskiner autentiseres gjennom signaturer og sertifikater. Sikker Web-aksess bruker SSL mellom nettleser og Web-tjener. Vanlig praksis i dag er at kun Web-tjeneren autentiseres ved offentlig-nøkkel kryptografi, mens klienten enten ikke autentiseres i det hele tatt, eller ved brukernavn og passord som overføres over SSL-kanalen. SSL har imidlertid mulighet for bruk av klient-sertifikater, og dette anbefales som langsiktig løsning. Brukernavn og passord er et sikkerhetsmessig dårligere alternativ, og er meget vanskelig å administrere i stor skala.

Tunneler

For tunnelløsninger gis det samme anbefalinger som for VPN-løsninger: Det er ønskelig med en enkel policy som angir krav til sikkerhet i prosedyrene for nøkkelgenerering, beskyttelse av nøkler og sertifisering, men det trenger ikke være noen krav om at sertifikater skal utstedes fra en lisensiert sertifkattjeneste.

Web-tjenere

For sertifisering av Web-tjenere anbefales det å bruke en anerkjent sertifikattjeneste som har en solid nok policy for formålet. Dette kan være en norsk tjeneste, eller faktisk også en av de tjenestene som er tilgjengelig på Internett (se avsnitt 3.2.1), men da med sertifikater av «høy klasse». Autentisering av tjener krever nemlig at klientene – nettleserne – kjenner offentlig nøkkel til tjenerens sertifiseringsautoritet. De store sertifikatleverandørene på Internett har sine offentlige nøkler lagt inn i standarddistribusjonene av Microsofts og Netscapes nettlesere, mens nøkler for andre sertifikatleverandører (f. eks. en eventuell norsk leverandør) eksplisitt må legges inn av brukerne. Dersom brukerne har smartkort utstedt under FNS-rammeavtalene, og sertifikatleverandøren bruker samme nøkkelpar ved utstedelse av sertifikater til Web-tjenere som ved sertifisering etter FSP-1, vil imidlertid sertifikattjenestens offentlige nøkkel alt ligge i smartkortet.
Det burde ikke være behov for en egen sertifikatpolicy for Web-tjenester tilbudt av offentlig sektor. Merk at FSP-1 faktisk kan brukes for sertifisering av tjenere, men da med virksomhetens navn (eventuelt organisasjonsenhet eller rolle) i sertifikatene, ikke URL eller maskinnavn slik det er vanlig ved bruk av SSL.

Web-klienter

Klientautentisering for Web-aksess kan understøttes av FSP-1, ved bruk av nøkkelpar og sertifikat med formål autentisering. Her er det foreløpig et problem at nettlesere normalt ikke er satt opp til å forholde seg til smartkort, men dette vil forhåpentligvis endre seg.
Imidlertid kan det virke unødig strengt å kreve smartkort og sertifikater på FSP-1 nivå for autentisering ved Web-aksess. Brukere som allerede har FSP-1 sertifikater på plass, bør kunne bruke disse uten videre, men brukere som ikke har behov for digitale signaturer, eller er i en arbeidssituasjon (f. eks. hjemme eller på reise) der de ikke trenger digitale signaturer, bør kunne ha et enklere alternativ. Dette bør tillate nøkler lagret (kryptert) på disk eller diskett. Det bør utarbeides krav til sikkerheten i en slik løsning. Merk at dersom Web-applikasjonen faktisk skal produsere

[15] Spesifisert av Netscape, se http://home.netscape.com/eng/ssl3 SSL er videreutviklet til en Internett-standard: «The Transport Layer Security (TLS) protocol, version 1.0», RFC2246, januar 1999. Det er imidlertid fortsatt SSL som er de facto standard. TLS er ikke i bruk i særlig grad.

digitale signaturer, må det stilles krav om FSP-1. Svakere krav vil kun gjelde for klientautentisering for Web-aksess.
Web-aksess uten bruk av smartkort vil ikke nødvendigvis være akseptabelt i alle tilfeller. F. eks. er det langt fra gitt at dette vil kunne godtas for Web-basert aksess til personlig helseinformasjon eller annen personsensitiv informasjon.

2.3.2. Tynne klienter

Spesifikasjonene for FNS-rammeavtalene sier at smartkort skal settes i den maskinen brukeren sitter ved (PC normalt). Dette er begrunnet med at brukeren skal ha kontroll over smartkortet. Videre er det krav om at programvare for signering og kryptering skal kjøres lokalt, siden det er der smartkortet er.
Det siste kravet er ikke forenlig med bruk av tynne klienter, der all programvare kjøres på tjenermaskiner, mens brukerens maskin kun tar seg av brukergrensesnittet og tastatur / mus. Vi ser nå at tynne klienter blir tatt i bruk innen offentlig sektor, og bruken må forventes å øke. Som ett eksempel kan tynne klienter brukes for å oppfylle Datatilsynets krav til behandling av sensitive personopplysninger i en kommune[16]. Dette kan ofte være eneste praktisk brukbare metode for å hindre klipp-og-lim funksjonalitet og lokal lagring av sensitiv informasjon. Videre har bruk av tynne klienter kostnadsmessige og driftsmessige fordeler.
Det finnes i dag minst ett produkt på UNIX-plattform (fra Sun) som støtter bruk av smartkort i en tynn klient konfigurasjon. Her sitter smartkortet i klienten, men styres fra tjenermaskinen som om smartkortleseren skulle vært tilkoplet denne. Tilsvarende funksjonalitet finnes så vidt vi vet ikke i dag for PC-plattform (Wincenter og liknende), men dette kan komme. Det kan finnes måter å programmere seg rundt dette for å oppnå muligheter for å kople en smartkortleser til klienten, og det kan godt være produkter underveis.
Men den typen konfigurasjon som er presentert for å oppfylle Datatilsynets retningslinjer i en kommune (se over og fotnote), kan vanskelig støttes fullt ut. Her har brukerne en normal PC-plattform for aktiviteter som ikke er sensitive, og bytter til en Wincenter-omgivelse når de aksesserer f. eks. helse- og sosialsystemer. Det er vanskelig å tenke seg at Wincenter-omgivelsene her på noen måte skal kunne få aksess til smartkort tilkoplet PCene.
Uansett: Det vil være viktig å tilby digital signatur og meldingskryptering på tynne klienter, og fortsatt med den forutsetningen at brukeren skal ha kontroll over smartkortet, dvs. at dette skal stå i brukerens lokale maskin. En trenger å kartlegge produkter som kan støtte dette, og hvilke forutsetninger disse opererer under. En trenger også å spesifisere sikkerhetsmessige krav til bruk av digital signatur og meldingskryptering i slike omgivelser. Spesielt vil det være strenge krav til beskyttelse av informasjonen som overføres mellom klient og tjener.
FSP-1 sertifikatpolicy kan brukes også i slike omgivelser. Policy stiller ikke krav om bruksomgivelser (annet enn i generelle, rådgivende vendinger), og kan vanskelig gjøre det, siden dette er utenfor sertifikattjenestens kontroll.

2.3.3. Autorisasjonssertifikater og roller

FSP-1 dekker autorisasjoner i noen grad gjennom profesjonssertifikater. FSP-1s rollesertifi-kater dekker behovet for roller som kan innehas av flere personer, men dekker ikke behovet for sertifisering av personlige roller.

[16] Ref. presentasjon gitt av IT-sjef Tore Halstensen i Skedsmo Kommune under FNS-informasjonsmøte om «Sikker data- og dokumentutveksling», Regjeringskvartalet, 17. november 1999.

En enkel form for personlige rollesertifikater kan utstedes ved å inkludere rollenavn i Title-attributten i navnet i sertifikatet (gjøres alt for profesjonssertifikater). Det viktigste problemet her er at navn på roller ikke er standardisert. Title-attributten gir da god indikasjon for menneskelige brukere, men egner seg dårlig for maskinell bearbeiding med mindre man har klare konvensjoner for bruken. Dette er likevel en enkel utvidelse til FSP-1.

I de tilfellene der en person har én rolle internt i en virksomhet (f. eks. stillingsbetegnelse), burde en enkel bruk av Title være i orden, men i svært mange tilfeller har en person flere roller i sin virksomhet, roller i flere virksomheter, eller roller i aktiviteter som går på tvers av virksomheter. Det er svært uhensiktsmessig dersom personen da skal trenge flere sett av smartkort og ansattsertifikater – ett for hver rolle / virksomhet.

Siden roller skifter relativt raskt, er det heller ikke noen løsning å inkludere alle roller i ett sertifikat. Løsningen er heller å definere egne rollesertifikater, som må brukes sammen med et ansattsertifikat (eller profesjonssertifikat) for autentiserings- og autoriseringsformål. Et rollesertifikat må klart angi hvem som har autorisert rollen. Ett eksempel er en revisor som arbeider i et revisjonsfirma, og har sitt ansattsertifikat der, men som har rollen revisor for en rekke andre virksomheter. Her er det disse andre virksomhetene som skal autorisere revisorrollen, gjennom sertifikater som kopler revisorens navn, rollen revisor, og virksomhetens navn. Slike sertifikater kan være nøkkelløse[17], eller de kan bruke samme offentlige nøkkel som revisoren har i sitt ansattsertifikat (det med formål digital signatur). Et rollesertifikat kan realiseres i form av en signert melding fra virksomheten, men sikrere i form av et «formelt» sertifikat utstedt av en sertifiseringsautoritet. Sertifikatformat må uansett defineres.

For roller og autorisasjoner er det flere store problemer:

- X.509 sertifikater er ment for autentisering, ikke autorisasjon,
- Andre sertifikatformater er i liten grad standardisert, og i enda mindre grad tatt i bruk,
- Det finnes ingen standarder for å representere autorisasjoner og roller (utover det som alt dekkes av profesjonssertifikater),
- Anvendelser av sett av sertifikater, som skal tolkes i bestemte sammenhenger, f. eks. for å bevise autorisasjoner, er ikke standardisert eller utbredt,
- Det kan stilles spørsmålstegn ved effektiviteten av løsninger som krever prosessering av mange sertifikater.

Vi ser anvendelser der en «strekker» X.509 sertifikatformatet til å kunne angi autorisasjoner, men egentlig bør en bruke andre sertifikatformater for formålet (ofte kalt PAC – Privilege Attribute Certificate[18]).

Vi ser ingen enkel og generell løsning for sertifikater for autorisasjoner og roller. Det offentlige kan definere representasjon av de mest aktuelle roller og autorisasjoner, definere en X.509-profil for denne informasjonen og stille generelle krav til prosedyrer for utstedelse av slike sertifikater. Men bruken av dette må spesifiseres separat for hver enkelt konkret anvendelse.

2.4. Konklusjoner

Det offentlige bør opprettholde kravet om sertifikater på nivå med FSP-1 der det er krav om digitale signaturer. Men i tillegg er det behov for en rammepolicy for sikring av Web-aksess, dvs.

[17] Dvs. at sertifikatet ikke inneholder noen offentlig nøkkel. Det betyr at offentlig nøkkel i det autentiserings-sertifikatet som følger med meldingen, er den nøkkelen som skal brukes.

[18] Format er standardisert av ECMA (European Computer Manufacturers Association) i ECMA-219: «Authentication and Privilege Attribute Security Application with Related Key Distribution Function (Parts 1-3)», mars 1996. Så vidt vi vet arbeides det ikke med dette innen standardiseringsorganer som ISO eller IETF.

autentisering av Web-klienter og opprettelse av en sikret kommunikasjonskanal. Her kan en bruke smartkort og sertifikater (formål autentisering) utstedt under FSP-1, men for brukere som ikke har behov for digitale signaturer, bør det finnes en enklere løsning.
Dersom det offentlige skal tilby Web-tjenester til annet enn åpen informasjon, vil det oppstå behov for sertifikater for Web-tjenerne. Slike sertifikater kan en skaffe fra en av de tjenestene som er tilgjengelige på Internett, men da trengs det sertifikater av høy klasse. Eventuelt kan sertifikater kjøpes fra norske leverandører som gir dette tilbudet. Det burde ikke være behov for noen egen sertifikatpolicy for offentlig sektor her, men en må forvisse seg om at den tjenesten en velger, holder tilstrekkelig nivå.
Det bør stilles visse krav til sertifikater og nøkler for VPN og tunnelløsninger, men her trenger det ikke være noe krav om at sertifikater skal utstedes av lisensierte sertifikattjenester.
FNS-avtalene på digital signatur og meldingskryptering bør utvides med løsninger for tynne klienter. Her kan en fortsatt bruke FSP-1 sertifikatpolicy.
Autorisasjonssertifikater og sertifikater for personlige roller er det behov for både i offentlig sektor og privat sektor. Dette er et område der standardiseringarbeidet er kommet svært kort, og en nærmest henvist til å løse problemstillingene fra sak til sak. Men det offentlige kan sette opp krav til kvalitet på tjenester som skal tilby slike sertifikater, og kan gjøre en del arbeid på sertifikatformater.

3. Sertifikater for privatpersoner

3.1. Anvendelser, valgmuligheter

Det finnes det en rekke anvendelser der privatpersoner kan ha nytte av offentlig-nøkkel kryptografi, smartkort, sertifikater osv. Eksempler er elektronisk handel, betaling, aksess til Web-tjenester, sikring av elektronisk post og tjenester for mobiltelefon[19] (kan bruke SIM-kortet i en GSM-telefon f. eks.).
Det offentlige har behov for å spesifisere hvordan privatpersoner kan bruke denne typen teknologi for å sikre kommunikasjon til / fra det offentlige. Her ser vi primært to anvendelser:

- Digitale signaturer og meldingskryptering i forbindelse med «formell korrespondanse», f. eks. søknader og svar, og for andre dokumenter,
- Adgang til informasjonstjenester der autentisering / autorisering er nødvendig, og i tilknytning til dette, til Web-skjema anvendelser o.l. (dersom Web-skjema brukes til f. eks. en søknad, kan en måtte stille krav om digital signatur på nivå «formell korrespondanse»).

Det offentlige har i prinsippet tre valgmuligheter for regulering av dette området:

1. Evaluere de tjenester som er tilgjengelig i markedet, og godkjenne de som holder mål (for et gitt formål eller generelt),
2. Sette opp krav til tjenester som skal kunne godkjennes (for et gitt formål eller generelt), der kravene kan være meget detaljerte (f. eks. definere en spesifikk sertifikatpolicy som skal følges), eller mer overordnede,
3. Etablere en offentlig tjeneste for utstedelse av «elektroniske borgerkort», der selve driften av tjenesten kan settes bort til en kommersiell aktør, eventuelt noen få aktører.

Det kan tenkes kombinasjoner av disse alternativene, der ett alternativ egner seg for ett formål, mens et annet alternativ er best for andre formål. Alle alternativene vil måtte medføre en eller annen form for lisensiering av sertifikattjenestene. I de to første alternativene vil dette innebære en evaluering /

[19] Dette kan godt være tjenester for elektronisk handel og betaling mm., men også mer spesifikke tjenester.

evaluering i henhold til krav, mens en i det siste tilfelle vil måtte lisensiere en spesifikk tjeneste, evt. et begrenset antall.
Nedenfor ser vi kort på status innen området og på enkelte problemområder (forholdet til ansatt-sertifikater og bruk av unike identifikatorer) før vi gir noen konklusjoner.

3.2. Status innen området

3.2.1. Tjenester på Internett, og PGP

Det finnes flere tjenester tilgjengelig på Internett for utstedelse av personlige, digitale sertifikater. Eksempler er Verisign[20], Thawte[21] med flere. Felles for disse er:

- De er kun basert på elektronisk kontakt mellom sertifikattjeneste og bruker[22], ikke noe personlig frammøte eller egen RA-funksjon,
- Brukerne genererer nøkler selv,
- Nøkkellagring er på disk.

Nøkler og sertifikater brukes primært sammen med nettlesere, for klientautentisering i SSL (Secure Sockets Layer) og signering / kryptering av epost. De internasjonale tjeneste-leverandørene har betalt en bra sum for å få sine offentlige nøkler lagt inn i distribusjons-utgavene for Netscapes og Microsofts nettlesere. I tillegg kan brukere selv legge inn offentlige nøkler for andre sertifikatleverandører i nettleserne.
Vi kan trygt konkludere med at de tjenestene som er tilgjengelige på Internett idag, kun tilbyr begrenset tillit. Det er liten grunn til at det offentlige i Norge skal godta en signatur som understøttes av f. eks. et Verisign sertifikat (unntatt muligens dersom dette er av høyeste klasse), der det er formelle krav til signatur for (elektronisk) korrespondanse.
PGP[23] (Pretty Good Privacy) er et meget populært program for sikring av epost og kryptert lagring av informasjon. PGP bruker ikke PKI-tjenester, og har ikke noe tilfredsstillende system for tilbakekalling av sertifikater. Isteden sertifiserer PGP-brukere hverandres nøkler («Web of trust»). PGP kan derfor ikke skalere (med tilstrekkelig tillit) i den sammenhengen vi snakker om her. PGP kan være et meget godt alternativ i tilfeller der en begrenset, lukket gruppe skal samarbeide og utveksle informasjon som trenger beskyttelse. Men det vil være vanskelig for det offentlige å godta bruk av PGP generelt, og spesielt der det er krav om digital signatur.

3.2.2. Tjenester fra norske leverandører

Det er kun annonsert en tjeneste for digitale sertifikater for privatpersoner i Norge: Postens Elektroniske Id[24], i regi av Posten SDS. Denne bruker smartkort, og sertifikater og smartkort utstedes etter personlig fammøte på et postkontor (og antagelig også ved hjelp av landpostbud mm.). Det er ikke publisert noen sertifikatpolicy for tjenesten, men det har vært et meget tett samarbeid mellom postverkene i Norge, Sverige, Finland og Irland, og det er tette koplinger til SEIS. Det er derfor nærliggende å tro at SEIS S10 vil være utgangspunkt for en sertifikatpolicy.

[20] http://www.verisign.com

[21] http://www.thawte.com

[22] En del leverandører, f. eks. Verisign, tilbyr forskjellige klasser av sertifikater, der klasser for høy tillit krever prosedyrer som gir en forholdsvis solid autentisering av brukeren. I praksis brukes ikke disse klassene for privatpersoner.

[23] Se http://www.pgpi.org

[24] Se http://www.sds.no/elektr_the/el_id.html

Den Internasjonale Postunionen planlegger et verdensomspennende system for sertifikat-utstedelse, i stor grad basert på det arbeidet som er gjort i Norden og Irland.
Andre sertifikatleverandører i Norge retter seg mot bedriftsmarkedet, men i hvert fall Fellesdatas tjeneste ser ut til å kunne benyttes også av privatpersoner.

3.2.3. Sverige og Finland

I Sverige har Statskontoret gjennomført en anbudsprosess og inngått rammeavtaler for bruk i den svenske statsforvaltningen med to leverandører av «elektroniske ID-kort», digital signatur og sertifiseringstjenester – Posten AB og Telia. De svenske rammeavtaler baserte seg på de samme standarder som ble valgt i FNS. Avtalene ble undertegnet i februar 1999.
I Finland ble det finske folkeregisteret gitt i oppgave å etablere et sertifikatsystem for finske borgere, basert på bruk av elektroniske ID-kort (smartkort med digital signatur og visuelle identifikasjonsopplysninger). Finnene har også gjennomført anbud på denne type tjenester, basert på samme standarder som i Sverige og Norge. Den finske tjenesten skal begynne å utstede elektroniske ID-kort i desember 1999.
FNS har under arbeidet med rammeavtaler om digital signatur hatt et godt samarbeid med prosjektene i Sverige og Finland.

3.3. Noen problemområder

3.3.1. Forholdet til ansattsertifikater

Det er nærliggende å tro at personer som har fått utstedt sertifikater i tilknytning til sin jobb, også vil ønske å kunne bruke disse til privat korrespondanse. Dette tilsvarer dagens situasjon for epost, der et stort flertall bruker epostadressen knyttet til jobben også for privat epost.
Selv om anbefalingene fra bl.a. FNS går ut på at en bør skaffe seg to sett med sertifikater – ett for privat bruk og et annet for jobbrelatert bruk – skulle det ikke være noe prinsipielt i veien for å akseptere bruk av ansattsertifikater (eller profesjonssertifikater) for privat korrespondanse mot det offentlige. Forutsetningene er:

- Sertifikatene må være av tilstrekkelig kvalitet, f. eks. utstedt etter FSP-1 eller tilsvarende,
- Sertifikatene må i tilstrekkelig grad autentisere brukeren som privatperson.

Det er ikke opplagt at det siste alltid er oppfylt. Som et eksempel: Dersom Jon Ølnes som privatperson sender en digitalt signert søknad til Plan- og Bygningsetaten i Oslo angående en gitt eiendom, og signaturen er støttet av et sertifikat som gir en unik identifikasjon av Jon Ølnes som ansatt ved Norsk Regnesentral, er dette tilstrekkelig? Hva dersom personen i eksemplet har et meget vanlig navn?
Konklusjonen skulle bli at det prinsipielt ikke er noe galt i å bruke ansattsertifikater for privat korrespondanse, men at akseptansen av slike sertifikater for korrespondanse mot offentlig sektor må vurderes for hver konkrete anvendelse. Merk at ansattsertifikater normalt ikke vil ha fødselsnummer eller annen unik identifikator, og derfor ikke kan brukes der dette er et krav.

3.3.2. Bruk av unik identifikator

Som regel er det et ubetinget krav at navnet som brukes i et sertifikat for en privatperson, unikt må identifisere personen. Dette krever i praksis at sertifikatet inneholder en attributt – en identifikator – som er unik for hver enkelt bruker. Videre er det i noen tilfeller krav om at fødselsnummer skal oppgis ved korrespondanse, f. eks. for ligningsmyndighetene og innen helsevesenet.
Det mest nærliggende er derfor å bruke fødselsnummeret som identifikator i sertifikater. Dette har den store ulempen at fødselsnummer da vil kunne spres i svært stor grad, spesielt dersom

sertifikatene skal ligge i en katalog. Mange mennesker ser på fødselsnummeret sitt som sensitiv informasjon. Problemstillingene ble berørt av ei arbeidsgruppe som så på navn og identifikatorer[25] i forbindelse med FNS-rammeavtalene og FSP-1.

Datatilsynets har gitt uttrykk for[26] at bruk av fødselsnummer er i orden i de sammenhenger der en kan godtgjøre at det er nødvendig. Konsekvensen er at sertifikater med fødselsnummer muligens bare kan brukes i visse sammenhenger, mens det i andre sammenhenger, der behovet for bruk av fødselsnummer ikke er dokumentert, ikke vil være hjemmel for å bruke disse sertifikatene. Det vil være problematisk å få konsesjon for lagring av sertifikater med fødselsnummer i en allment tilgjengelig katalog.

I Sverige løses dette ved at sertifikater som inneholder fødselsnummer, ikke publiseres i noen katalog. Men disse sertifikatene vil likevel spres i stort omfang, siden de normalt brukes der eieren signerer digitalt, og spredningen kan fort bli omtrent den samme som om de lå i en katalog.

Et alternativ, som er tatt i bruk i Finland i forbindelse med elektronisk borgerkort, og som er foreslått i Danmark, er å ta i bruk en ny «nummerserie» for å tildele unike identifikatorer til mennesker for bruk i sertifikater. Kopling til fødselsnummer kan da gjøres indirekte gjennom et register som inneholder begge numrene, og som er tilgjengelig on-line for autoriserte parter. Problemet her er at det er nokså tungvint å innføre en ny identifikator. I tillegg risikerer man at den nye identifikatoren etterhvert blir brukt i såpass stor utstrekning at den også kan bli regnet som sensitiv informasjon.

Merk at en lignende løsning brukes i ELEKTRA-prosjektet i Skattedirektoratet. Posten SDS utsteder sertifikater med en unik identifikator, og har et register som oversetter denne til fødselsnummer, før de innrapporterte opplysningene sendes fra Posten SDS' formidlingssentral til Skattedirektoratet.

ELEKTRA er ett eksempel på at den viktigste bruken av fødelsnummer for elektronisk kommunikasjon er for maskinell behandling f. eks. gjennom oppslag i databaser. Her har en unik, standard identifikator stor verdi. Ved slike løsninger trenger ikke fødselsnummeret å eksponeres for mennesker.

Det kan finnes løsninger basert på at fødselsnummer og en del annen informasjon kjøres gjennom en enveisfunksjon, som genererer en ny, unik identifikator[27]. Brukere som har adgang til fødselsnummeret og annen nødvendig informasjon, kan da bruke enveisfunksjonen for å fastslå samsvar. Det er ikke utredet hvilke krav som må stilles til en slik funksjon, eller om det finnes noen eksisterende matematisk teori som vil gi en tilfredsstillende løsning, men det er ikke helt usannsynlig at en løsning kan finnes.

Det er også mulig å overlate dette til leverandørene, som da må ha egne nummerserier, som sammen med andre navneattributter garanterer unike navn. Problemet her, sett fra det offentliges side, er at dokumenterte behov for bruk av fødselsnummer ikke oppfylles med mindre leverandørene tilgjengeliggjør (for autoriserte brukere) et register som kopler identifikator og fødselsnummer.

Tilordning av unike identifikatorer for bruk i sertifikater for privatpersoner er et område som må utredes ytterligere av det offentlige.

[25] «Navn og identifikatorer i sertifikater for Forvaltningsnettsamarbeidet, anbefalinger fra arbeidsgruppe», Forvaltningsnettsamarbeidet rapport 6/99, august 1999. Også tilgjengelig fra FNS' nettsted.

[26] Ref. Datatilsynets Jørn Arnesen, deltaker i arbeidsgruppa for navn og identifikatorer i FNS.

[27] En er ikke garantert at en identifikator er unik, men sannsynligheten for at to mennesker med samme navn også vil få samme identifikator er neglisjerbar.

3.4. Konklusjoner

I innledningen satte vi opp tre alternativer for offentlig regulering av utstedelse av sertifikater for privatpersoner for kommunikasjon mellom privatpersoner og det offentlige selv.

En konklusjon er at en regulering i henhold til det offentliges behov på dette området må forventes å få en standardiseringseffekt i Norge, avhengig av hvor tidlig det offentliges regulering / krav kommer fram i forhold til leverandørenes planlegging. For leverandørene vil det være en motivasjon å kunne oppfylle det offentliges krav, og det vil være enkelt for dem å anbefale samme type sertifikater brukt til andre formål.

Alle alternativer for offentlig regulering vil innebære en form for lisensiering av godkjente sertifikatleverandører. Lisensieringsordninger utredes, som nevnt, av Torvund-utvalget, som vil komme med sin innstilling innen utløpet av 1999. Alternativene er:

1. Evaluere tjenester tilgjengelig i markedet med tanke på godkjenning,
2. Sette opp krav til tjenester som skal kunne godkjennes,
3. Etablere en offentlig tjeneste for utstedelse av «elektroniske borgerkort».

Her vil vi anbefale at en arbeider videre med alternativ 2.

For alternativ 1 konkluderer vi at de tjenestene som er tilgjengelig på Internett, gir for dårlig kvalitet. Den eneste tjenesten som er annonsert i Norge for privatpersoner, er Postens Elektroniske Id. En kan gjøre en evaluering av denne med tanke på godkjennelse, men ikke minst av konkurransemessige årsaker er det en bedre tilnærming å samarbeide med Posten SDS og andre potensielle leverandører ved utarbeidelse av mer generelle krav til slike tjenester. I en situasjon der det hadde vært to eller flere leverandører på markedet, kunne en evaluering av tilgjengelige tjenester vært et alternativ.

Alternativ 3 anbefales ikke generelt. Lisensiering av leverandører bør knyttes til kvaliteten på tjenestene og sikkerheten i driften av disse, og ikke til at leverandørene også må ha oppnådd en avtale med det offentlige. Avtaler med et fåtall leverandører (eventuelt bare en) for utstedelse av godkjente sertifikater for privatpersoner vil kunne medføre en urimelig konkurransevridning. Ett spesialtilfelle kan tenkes her: Utstedelse av elektroniske pass, som nok vil være i form av vanlige pass med smartkortfunksjonalitet i tillegg, vil kunne kreve at det offentlige selv oppretter en sertifikattjeneste for dette formålet.

Det er rimelig at sertifikattjenester for privatpersoner bør oppfylle omtrent samme krav som tjenester som er godkjent for bruk internt i offentlig sektor, dvs. på nivå omtrent som FSP-1 der bruken er digitale signaturer og meldingskryptering. Dette er konsistent med arbeidet i Sverige og Finland, der SEIS S10 policy legges til grunn (denne var også utgangspunktet for spesifikasjonen av FSP-1). Det anbefales å kreve bruk av smartkort.

De kravene det offentlige stiller, kan formuleres gjennom spesifikasjon av en rammepolicy for sertifikater, der det er naturlig å ta utgangspunkt i SEIS S10. Rammepolicyen vil inneholde krav på de områder der det offentlige har behov for å stille krav, og ellers være åpen. Det betyr at leverandørene i sine policyer kan fylle inn de områdene der det ikke er stilt krav. I Norge ser det generelt ikke ut til å være behov for å kople elektronisk id. i smartkort med trykking / preging av kortet som et fysisk identitetskort. Dette kan derfor være en opsjon.

Det offentlige må spesifisere hvordan unike identifikatorer (fødselsnummer eller annet) skal brukes i sertifikater. Dersom fødselsnummer skal brukes, må betingelsene for dette avklares, spesielt med tanke på kataloger.

4. Sertifikater for private bedrifter

4.1. Status og tilgjengelige tjenester

Private virksomheter som har, eller planlegger, sertifikater for sine ansatte, vil i dag ha to alternative løsninger:

- Kjøpe sertifikater fra en ekstern sertifikattjeneste, slik som FNS legger opp til,
- Opprette en egen sertifikattjeneste for virksomheten, enten driftet internt, eller satt bort til en ekstern leverandør.

Ved det siste alternativet vil sertifikatutsteder være virksomheten selv. Dette er et marked som spesielt. Entrust[28], men også andre, har siktet seg inn på. Bedriftens interne sertifikattjeneste kan i sin tur ha et sertifikat, som i dag vil være utstedt av en eller annen tjeneste på Internett (f. eks. Verisign), eller den kan være helt intern, til bruk for intranett, gruppevareløsninger osv. En del produkter, f. eks. Lotus Notes, har sitt eget system for sertifikatutstedelse.

Flere leverandører i det norske markedet sikter seg inn på bedriftsmarkedet med samme type løsninger som FNS har valgt, og vi må forvente at en del bedrifter nå vil begynne å velge dette. Vi ser særlig at ekstranett og informasjonsnett[29] bruker en ekstern sertifikatleverandør, men en del virksomheter bruker bedriftsinterne sertifikattjenester for ekstranett.

4.2. Anvendelser

For offentlig sektor er det spesielt tre interessante anvendelser av digitale signaturer og sertifikater mot private bedrifter:

- Innrapportering fra bedriftene, f. eks. til Skattedirektoratet,
- Elektronisk handel spesielt i forbindelse med offentlige innkjøp,
- Generell elektronisk samhandling, som korrespondanse og elektronisk foretningsdrift.

Dette kan også innebære bruk av autentiserte Web-tjenester, som diskutert tidligere.

4.3. Konklusjoner

For å holde konsistente krav til sikkerhet av digitale signaturer, bør det offentlige kreve at signaturer fra personer i private bedrifter skal være produsert ved hjelp av smartkort eller liknende, og støttes av sertifikater på nivå med FSP-1. Siden en privat virksomhet ikke er vesensforskjellig fra en offentlig virksomhet, kan en faktisk stille krav om FSP-1. Antagelig er dette å gå litt langt med hensyn på å styre leverandørenes tjenester, og en bedre tilnærming kan være å utforme en rammepolicy, basert på FSP-1, der en angir de viktigste kravene som skal være oppfylt.

Tilsvarende kan en utarbeide en rammepolicy for autentisisering av klienter ved Web-aksess, eller antagelig heller bruke samme policy som for Web-aksess fra privatpersoner.

Som nevnt vil en del bedrifter ha interne sertifikattjenester, der bedriften selv står som utsteder av sertifikatene. Det er ikke noe prinsipielt i veien for at offentlig sektor skal kunne godkjenne sertifikater utstedt av slike tjenester, forutsatt at sikkerheten ved tjenestene oppfyller kravene. Det er nok i utgangspunktet små sjanser for at interne tjenester vil oppfylle krav på nivå FSP-1 for digitale signaturer, men kravene til sikker Web-aksess kan godt være oppfylt. Verifisering av at en bedriftsintern sertifikattjeneste oppfyller gitte krav kan være vanskelig, og krever som minimum at tjenesten følger en definert sertifikatpolicy, som kan være spesifikk for bedriften.

---

[28] http://www.entrust.com – leverer installasjoner av utstyr og programvare for sertifikattjenester.

[29] Se f. eks. http://www.fellesdata.no/bransjenett/index.htm

5. Oppsummering

Dette notatet er skrevet av Norsk Regnesentral (NR) på oppdrag av Arbeids- og Administrasjonsdepartementet (AAD). Det understrekes at innholdet i dette notatet står for NRs regning, og ikke nødvendigvis representerer det syn AAD eller andre offentlige virksomheter måtte ha på problemstillingene.

Notatet diskuterer tre problemområder:

- Behov for sertifikattjenester og tilhørende sertifikatpolicyer internt i offentlig sektor, i tillegg til det som er omfattet av FNS-rammeavtaler, og FSP-1 policy,
- Behov for sertifikattjenesterer og –policy på grensesnittet mellom offentlig sektor og privatpersoner,
- Behov for sertifikattjenester og –policy på grensesnittet mellom offentlig sektor og private bedrifter.

For offentlig sektors interne behov er den første konklusjonen at det bør stilles krav om bruk av tjenester basert på FSP-1 (eller av tilsvarende styrke) der det er behov for digitale signaturer. En bør ikke tillate andre, svakere alternativer. FNS-avtalene trenger å utvides med spesifikasjoner som dekker tynne klienter, men FSP-1 policy skal kunne brukes også i dette tilfellet.

FNS-rammeavtalene dekker ikke sikring av Web-aksess, noe som kommer til å bli et behov i løpet av kort tid. Dette gjelder autentisering ved adgang til informasjon som ikke er åpen, og etablering av sikret kommunikasjonskanal for overføring av slik informasjon. Her kan en bruke FSP-1 sertifikater og smartkort dersom brukerne har dette, men for brukere som ikke har behov for digitale signaturer, bør det finnes enklere og billigere alternativer. Det kan utarbeides en rammepolicy (sertifikatpolicy med de mest vesentlige krav) for dette.

Det er behov for å stille overordnede krav til sertifikater og nøkler for VPN-løsninger og løsninger for sikring av hjemmekontor og mobilt arbeid o.l. (tunnelløsninger). Her trenger en ikke å stille krav om at utsteder skal være en lisensiert sertifikattjeneste.

For privatpersoner anbefales det at offentlig sektor stiller spesifikke krav til tjenester som skal utstede sertifikater for å understøtte digitale signaturer for privatpersoner. Disse kravene må være oppfylt for at offentlig sektor skal kunne godkjenne slike signaturer. Kravene kan stilles i form av elementer som skal inngå i sertifikatpolicyer, f. eks. ved at en utarbeider en rammepolicy som leverandører kan ta som utgangspunkt. Det er naturlig at kravene legges på nivå med FSP-1 for digitale signaturer, og at en krever bruk av smartkort for dette. Det kan være behov for å spesifisere enklere krav til sertifikater som privatpersoner skal kunne bruke for autentisering i forbindelse med Web-aksess mot offentlige tjenester (f . eks. aksess til personalisert materiale). Det offentlige bør fastsette regler for bruk av unike identifikatorer (som fødselsnummer) i sertifikater, og forhold rundt bruk av ansattsertifikater til private formål bør også avklares.

Overfor private bedrifter vil igjen krav om sertifikater på nivå med FSP-1 være naturlig for å understøtte bruk av digitale signaturer som skal kunne godkjennes av det offentlige, f. eks. i forbindelse med innrapportering av (signert) informasjon fra bedrifter. Her er det faktisk mulig å stille krav om at FSP-1 skal brukes, men antagelig er det bedre å være mindre spesifikk i kravene, og heller utarbeide en rammepolicy som for privatpersoner. Offentlig sektor vil være interessert i sikker elektronisk handel med private bedrifter. Vi antar at der dette innebærer krav om signatur, vil det settes krav om FSP-1 eller tilsvarende nivå. Der det er krav om autentisering, men ikke signatur (f. eks. handel gjennom Web-aksess), kan en bruke en eventuell rammepolicy for Web-aksess som

diskutert over. Sertifikattjenestene for de private virksomhetene (fra leverandør av sertifikattjenester, eller fra intern tjeneste med sertifikater utstedt av virksomheten selv) må da oppfylle minimumskravene i rammepolicyen.

Sertifikater for Web-baserte tjenester (tjenerdelen) kan en få utstedt av tjenester som i dag er tilgjengelig på Internett. Det kreves f. eks. et Verisign-sertifikat av høy klasse. En bedre løsning er å la godkjente sertifikatautoriteter utstede Web-tjener sertifikater, men dette betyr at alle brukere eksplisitt må legge sertfikatautoritetens offentlige nøkkel inn i sin nettleser (med mindre den ligger i brukerens smartkort allerede).

Rollesertifikater kan det være behov for internt i offentlig sektor (f. eks. helsesektoren) og på grenseflaten mot private bedrifter (f. eks. mot Skattedirektoratet). Standardiseringsarbeidet rundt rollesertifikater er ikke særlig utviklet, og dette er i dag et område som nærmest må løses fra prosjekt til prosjekt, med mindre det offentlige velger å sette igang et spesifikasjons-arbeid av betydelig omfang. Det kan stilles generelle krav til sikkerhetsnivå i forbindelse med rollesertifikater, men både innhold i sertifikatene og bruksmåte for dem vil antagelig måtte variere for forskjellige anvendelser.

Det er foreløpig ikke identifisert noe behov for regulering av sertifikattjenester for rent privat sektor, ut over framtidige krav til evaluering av sikkerehten rundt drift av TTP-tjenester, og eventuelt lisensiering for å kunne tilby tjenester. Her henviser vi til kommende rapport fra Torvund-utvalget. Imidlertid er det offentlige den viktigste premissgiveren i utformingen av sertifikattjenester i Norge. Leverandørene bør oppmuntres til gjenbruk av de spesifikasjonene som offentlig sektor krever, for tjenester som tilbys i det private markedet.