NOU 2001 - 10

Uten penn og blekk

Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen

Utredning fra et utvalg oppnevnt ved kongelig resolusjon av 4. februar 2000
Avgitt til Arbeids- og administrasjonsdepartementet 2. mars 2001

Til Arbeids- og administrasjonsdepartementet

Regjeringen oppnevnte ved kongelig resolusjon av 4. februar 2000 et offentlig utvalg for å utrede bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen.

Utvalget legger med dette fram sin utredning.

2. mars 2001

Katarina de Brisis Leder

Ole-Gunnar ;Drabløs

Inger-Elisabeth Kvaase

Jens Nørve

Bjørn Erik Fjeldheim

Monica Lütken

Hilde Kristin Storvig

Johs. Hansen Hammer

Helge Lægreid

Audun P. Aanæs

Torgeir Jonvik

Brynjar Mørkved

Anne Karen Bonnevie Seip

Hovedsekretær

Amund Eriksen

Del I
Mandat og hovedkonklusjoner

1 Utvalgets sammensetning mandat og arbeid

1.1 Utvalgets sammensetning og mandat

Utvalget ble oppnevnt ved kongelig resolusjon 4. februar 2000 etter forslag fra Arbeids- og administrasjonsdepartementet.

1.1.1 Sammensetning

Utvalget har hatt følgende sammensetning:

- Seniorrådgiver Katarina de Brisis (leder) Oslo Arbeids- og administrasjonsdepartementet.
- Vara: Seniorrådgiver Rolf Borgerud Asker Arbeids- og administrasjonsdepartementet.
- Underdirektør Hilde Kristin Storvig Brønnøy Brønnøysundregistrene.
- Vara: Avdelingsdirektør Håkon Olderbakk Brønnøy Brønnøysundregistrene.
- Seksjonssjef Jørn Andreas Arnesen Oppegård Datatilsynet ut 2000.
- Vara: Rådgiver Audun P. Aanæs Oslo Datatilsynet medlem fra 2001.
- Underdirektør Torgeir Jonvik Oslo Finansdepartementet.
- Vara: Ikke oppnevnt.
- Forsker Helge Lægreid Oslo Forsvarets overkommando/Sikkerhetsstaben.
- Vara: Overingeniør Lars Venger Gunnarsson Eidsvoll Forsvarets overkommando/Sikkerhetsstaben fra 30.8.00: Forsker Øystein Hole Oslo Forsvarets overkommando/Sikkerhetsstaben.
- Avdelingsdirektør Monica Lütken Bærum Forsvarsdepartementet.
- Vara: Rådgiver Brynjel Johnsen Moss Forsvarsdepartementet.
- Spesialkonsulent Ole-Gunnar Drabløs Nittedal Kommunenes Sentralforbund.
- Vara: IT-sjef Tore Halstensen Skedsmo Kommunenes Sentralforbund til juni 2000 fra 31.8.00: Spesialkonsulent Geir Leth-Olsen Oslo Kommunenes Sentralforbund.
- Seniorrådgiver Jens Nørve Oslo Nærings- og handelsdepartementet.
- Vara: Rådgiver Vigdis Olsen Oslo Nærings- og handelsdepartementet til 5.9.2000.
- Rådgiver Barbro Onsøien Oslo Post- og teletilsynet ut 2000.
- Vara: Seniorrådgiver Brynjar Mørkved Oslo Post- og teletilsynet medlem fra 2001.
- Seksjonssjef Bjørn Erik Fjeldheim Oslo Rikstrygdeverket.
- Vara: Rådgiver Svein Burkeland Frogn Rikstrygdeverket.
- Seniorrådgiver Johs. Hansen Hammer Bærum Skattedirektoratet.
- Vara: Underdirektør Kristin Vestmo Lørenskog Skattedirektoratet.

- Seniorrådgiver Inger-Elisabeth Kvaase Oslo Sosial- og helsedepartementet.
- Vara: Rådgiver Alfred Ehrenclou Oslo Sosial- og helsedepartementet.

Justisdepartementet og eRegel-prosjektet (Kartleggingsprosjektet) ble invitert til å ha observatører i utvalgets møter. Dette ble ivaretatt av Ole Christian Hyggen Justisdepartementet prosjektleder Thomas Myhr Nærings- og handelsdepartementet og rådgiver Halvor Oseid Statskonsult.

1.1.2 Sekretariat

Sekretariatsfunksjonen for utvalget ble ivaretatt av Statskonsult ved seniorrådgiver Anne Karen Bonnevie Seip hovedsekretær og seniorrådgiver Amund Eriksen. I tillegg har seniorrådgiver Endre Grøtnes deltatt.

1.1.3 Mandat

Utvalget skal utrede innholdet i en policy for offentlig forvaltning på området bruk av digital signatur dokumentkryptering for konfidensialitetsformål og tilhørende infrastruktur (PKI Public Key Infrastructure).

Utredningen skal:

- presisere og avgrense hvilke spørsmål (jf. listen nedenfor) man mener en offentlig PKI-policy skal berøre
- foreslå innhold i policy på enkelte punkter og ev. videre utredningsarbeid på andre
- uttale seg om hva slags status en slik policy (eller dennes enkelte bestanddeler) bør ha i forvaltningen – anbefale tiltak.

Hovedspørsmål som ønskes utredet omfatter:

1. Kort oversikt over PKI-policy for offentlig sektor i andre OECD land.
2. Krav til digitale sertifikater som forvaltningen vil benytte selv eller stille krav om til andre. Et digitalt sertifikat er et bevis på at signaturen virkelig tilhører den som signerte.
   - typer digitale sertifikater – for hvem/hva innhold
   - hva slags digitale sertifikater vil forvaltningen godta fra andre evt. stille krav om
   - standardisert bruk av navn og unike identifikatorer i digitale sertifikater.
3. Behov for felles sertifikatpolicy i forvaltningen. Sertifikatpolicy angir krav til sikkerhet ved bruk av digital signatur og dokumentkryptering. Skal forvaltningen ha:
   - én eller flere policy for ulike anvendel ; ;ser (hvilke anvendelser)
   - obligatorisk eller anbefalt policy.
4. Det skal vurderes om Forvaltningsnettsamarbeidets sertifiseringspolicy FSP-1 kan bli en standard for forvaltningen.
5. Forvaltningens strategi for bruk av sertifiseringstjenester – hva bør forvaltningen sørge for selv og hva bør markedet sørge for. Oppgavefordeling mellom forvaltningen og markedet.
6. Forvaltningens krav til samtrafikk mellom leverandører av sertifiseringstjenester slik at det eksisterer valgfrihet for brukere av digital signatur når det gjelder hvem de vil få sitt digitale sertifikat fra.

7. Forslag til retningslinjer for bruk av digitale signaturer og dokumentkryptering i forvaltningen herunder spørsmålet om deponering og administrasjon av krypteringsnøkler brukt i embeds medfør.
8. Behovet for elektronisk ID-kort (som inneholder bl.a. digital signatur med mer) som vil utstedes i samband med offentlig tjenesteyting. Organisering finansiering og ansvar. Samspill med markedet.
9. Økonomiske og administrative konsekvenser bør så langt som mulig klarlegges.Det vises særlig til arbeid som utføres i et utvalg (*Myndighetsroller og TTP* eller «Torvundutvalget») oppnevnt av Nærings- og handelsdepartementet med frist 31.12.99. For øvrig vises det til følgende dokumenter:

- *Digitale signaturer og TTP gir tillit.* Rapport fra Rådet for IT-sikkerhet. Nov. 1998.
- *Elektronisk forvaltning. Handlingsplan for tverrsektoriell IT-utvikling*. Febr. 1999.
- Stortingsmelding nr. 41 (1998–99) *Om elektronisk handel og forretningsdrift*. Mai 1999
- *Forvaltningsnettsamarbeidets sertifiseringspolicy nr. 1 (FSP-1).* Aug. 1999
- *Navn og identifikatorer i sertifikater*. FNS. Rev. Sept. 1999
- FNS Avtaleverket og særlig Spesielle vilkår for TTP-tjenester.
- *Kravspesifikasjon for TTP-tjenester digital signatur og meldingskryptering*. FNS. Des. 98.
- OECD retningslinjer for kryptopolitikk
- EU direktiv *On a community framework for electronic signatures* (Common Position EC No 28/1999 adopted by the Council on 28. June 1999 OJ C 243/33) med senere tilføyelser fra Europaparlamentet (vedtatt 30.11.99).

Sekretariat

Statskonsult ivaretar sekretariatsfunksjonene for utvalget.

Frist

Punktene 2 3 4 og 5 besvares innen 1.7.2000.

Punktene 1 6 7 og 8 innen 1.10.2000.

Arbeids- og administrasjonsminister Jørgen Kosmo aksepterte at fristen for avlevering ble utsatt til 31.12.2000.

1.2 Om mandatet

Mandatet bruker uttrykket «offentlig forvaltning». Utvalget antar at det er hensiktsmessig å legge omtrent samme betydning i dette som forvaltningsloven gjør slik at ethvert organ for stat eller kommune omfattes samt private rettssubjekter i de tilfellene der de treffer det loven kaller enkeltvedtak eller utferdiger forskrifter. Forretningsdrift fra det offentlige er holdt utenfor. Det antas at det ikke er behov for en mer presis avgrensning i denne utredningssammenhengen.

Utvalget legger til grunn at mandatet ikke ber om utredning av behovet for digitale signaturer mv. men om forslag til hvordan et forutsatt behov kan dekkes gjennom hvilke konkrete løsninger.

Utvalgets oppgave er følgelig å anbefale konkrete krav og regler/retningslinjer for hvordan digitale signaturer kan benyttes på en formålstjenlig måte for forvaltningen selv og av brukere av forvaltningens elektroniske tjenester.

Utvalget har ut fra mandatet ikke funnet grunn til å behandle andre typer teknologier for autentisering. Andre måter å autentisere på kan imidlertid være nyttige på enkelte områder der digitale signaturer ikke er en egnet eller nødvendig løsning.

I henhold til mandatpunkt 6 skal det utredes forslag til retningslinjer/regler for bl.a. dokumentkryptering i forvaltningen. Problemstillingene og behovet for overordnet politikk rundt bruk og regulering av kryptografi (konfidensialitet og hemmelighold av meldingsinnhold) er tidligere behandlet i en egen arbeidsgruppe[1]i regi av Rådet for IT-sikkerhet (RITS). Det vises til rapporten den gruppen laget. Vår utredning kan til en viss grad sies å være en oppfølging av noen av forslagene fra RITS-arbeidsgruppen bl.a. forslagene om behov for å få utarbeidet og vedtatt kryptopolitikk for offentlig forvaltning og for privates samvirke med det offentlige.

Et aktuelt spørsmål er om politi- og påtalemyndighet ut fra lovlige etterforskningsformål i forbindelse med alvorlig kriminalitet skal ha mulighet for avlytting eller nøkkelregenerering (key recovery) på en eller annen måte. Dette spørsmålet er imidlertid ikke tatt med i mandatet og utvalget tar det ikke opp i denne utredningen. Her vil det handle om intern saksbehandling i forvaltningen og om grenseflaten mellom forvaltning og enkeltpersoner/næringsliv men ikke om etterforskning i forhold til alvorlige forbrytelser. Innholdskrypteringen som det i mandatpunkt 6 blir foreslått regler om må sees i et slikt lys.

Utvalget legger til grunn at sikkerhetstjenester som autentisering integritet og ikke-benekting er mandatets hovedtema. Begrepene forklares i kapittel 3. Disse viktige funksjonene kan ivaretas av teknologien innenfor området for digitale signaturer. Slike tjenester representerer etter utvalgets syn ikke problemer etterforskningsmessig ettersom de ikke forvansker eller skjuler noe av innholdsmessig karakter i opplysningene/dokumentene.

Forholdet til rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser er ikke tema i denne utredningen. Disse forholdene er nå regulert i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) vedtatt i 1998. Den trer i kraft samtidig med at et sett forskrifter er ferdige og kan tre i kraft antakelig i første halvår 2001.

Når sikkerhetsloven med forskrifter trer i kraft oppheves samtidig en rekke instrukser deriblant sikkerhetsinstruksen og datasikkerhetsdirektivet. Alle de nevnte regelverkene er gitt av hensyn til rikets sikkerhet mv. I tillegg er (deler av) datasikkerhetsdirektivet gitt anvendelse for beskyttelsesinstruksen som regulerer gradering av «andre grunner» enn dem som knytter seg til rikets sikkerhet. Når datasikkerhetsdirektivet oppheves må elektronisk behandling av opplysninger gradert etter beskyttelsesinstruksen ivaretas på en annen måte som det i skrivende stund (januar 2001) ikke er truffet beslutninger om. Denne utredningens kapittel 11 jf. mandatpunkt 6 inneholder imidlertid forslag som har sammenheng med det nevnte regelområdet.

1.3 Utvalgets arbeid

Utvalget har hatt åtte heldagsmøter og to møter som har gått over to dager. I tillegg har leder sekretariat og enkelte utvalgsmedlemmer deltatt i møter med forvaltningsvirksomheter og aktører i markedet som har interesse/behov for løsninger på området for digitale signaturer mv. for informasjonsutveksling og diskusjon. Dette omfatter bl.a. møter med Finansdepartementet Kommunal- og regionaldepartementet Sosial- og helsedepartementet Utenriksdepartementet Vegdirektoratet Riksarkivet Patentstyret Aetat

---

1

Rådet for IT-sikkerhet – *Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk* FO/S 1997-11-10. Rapporten kan fås ved henvendelse til Rådets sekretariat i Nærings- og handelsdepartementet Forskningsavdelingen.

Statens lånekasse Norges vassdrags- og energidirektorat Banknæringen Norsk Hydro Telenor Posten SDS (nå: ErgoGroup) og Strålfors.

Mange virksomheter har utredet egne behov og opplegg for elektronisk signering og konfidensialitet. Noen av dem er referert i vedlegg 1.

I tillegg ble det opprettet underutvalg i to sammenhenger først som et ledd i arbeidet med mandatpunkt 6 om retningslinjer for bruk av digitale signaturer (kapittel 11) der også representanter for henholdsvis Justisdepartementets lovavdeling og Arbeids- og administrasjonsdepartementet deltok dernest som et ledd i sluttarbeidet med utredningen.

Et internasjonalt møte over to dager ble arrangert i mai av Arbeids- og administrasjonsdepartementet v/utvalgsleder Katarina de Brisis. Møtet var en oppfølging av tilsvarende møte og rapport i regi av International Council of IT in Public Administrations (ICA) om digitale signaturer/PKI. Utvalgsleder sekretariat og et utvalgsmedlem deltok sammen med representanter fra USA Canada Nederland Irland Storbritannia Finland Sverige og Japan. Politisk rådgiver Hilde Kristine Nysten Thorkildsen holdt innlednings- og velkomsttalen. Møtet er dokumentert i en egen rapport fra Arbeids- og administrasjonsdepartementet [3].

Den direkte kontakten og informasjonen fra dette møtet er hovedgrunnlaget for utvalgets besvarelse av mandatets punkt 1 kort oversikt over PKI-policy for offentlig sektor i andre OECD-land.

Utvalget har på enkelte områder innhentet delutredninger og hjelp fra:

- JB Consult v/Jens Biong (knyttet til mandatpunkt 7 elektroniske ID-kort) [46]
- Rolf Riisnæs stipendiat Institutt for rettsinformatikk Universitetet i Oslo (knyttet til mandatpunkt 6 forslag til retningslinjer for bruk av digitale signaturer og kryptering i forvaltningen) [62]
- PKI Consulting Services v/Jon Ølnes og Rune Hagen (knyttet til bl.a. mandatpunkt 5 samtrafikk mellom sertifikattjenester samt sertifikatprofiler for offentlig sektor og sluttarbeid på hele utredningen) [61] [60]
- Forvaltningsinfo AS v/Tor Nygaard (kvalitetssikring i sluttfasen av utredningen).

For å skape debatt om utvalgets forslag ble tre delutredninger lagt ut på nettsidene til Forvaltningsnettsamarbeidet (FNS) med ønske om reaksjoner som i et visst omfang kom.

Utvalget har hatt stor nytte av denne bistanden. Delutredningene er i større og mindre grad bearbeidet gjennom behandling på utvalgsmøter og ansvaret for de endelige tekstene er utvalgets.

Utvalgsleder og enkelte utvalgsmedlemmer har deltatt i skrivearbeidet.

Innholdet i noen av utvalgets anbefalinger ble presentert av utvalgsleder og diskutert på et seminar om elektroniske signaturer i regi av Statens dataforum den 30.11. og 1.12.2000 på Losby Gods i Lørenskog der også flere av utvalgets medlemmer deltok.

2 Utvalgets hovedkonklusjoner

2.1 Innledning

Samfunns- og teknologiutviklingen stiller store krav til forvaltningens omstillingsevne. Forvaltningen må kunne levere rask individtilpasset og kostnadseffektiv tjenesteyting [21]. Fornyelse av offentlig sektor står høyt på den politiske dagsorden i dag. Blant viktige tiltak for å fornye offentlig sektor framheves «døgnåpen forvaltning» som et sentralt virkemiddel. Døgnåpen forvaltning skal levere offentlige tjenester på en kostnadseffektiv måte og på brukernes premisser uavhengig av tid og sted. Internett som kommunikasjonskanal er et grunnleggende element i realiseringen av slik forvaltning. For å kunne oppnå målsettinger for døgnåpen forvaltning er det nødvendig for forvaltningen å etablere hensiktsmessige løsninger for elektronisk saksbehandling elektronisk tjenesteyting og elektroniske administrative rutiner som økonomiforvaltning og innkjøp. Løsninger bør integrere hele verdikjeden dvs. interne systemer samt systemer for eksterne tjenester og virke på tvers av sektorer og forvaltningsnivå for å gi gevinster.

Til støtte for slike løsninger trengs en sikker effektiv og pålitelig infrastruktur for elektronisk informasjonsutveksling som kan sørge for at elektronisk samhandling gis samme juridiske gyldighet som den papirbaserte. Internett er «den elektroniske motorveien» der informasjon kan utveksles mellom ulike aktører og på ulike måter. Forvaltningen kan samhandle elektronisk med enkeltpersoner bedrifter kan samhandle med forvaltningen og forvaltningen kan effektivisere sin interne samhandling.

Internett er i utgangspunktet ikke et sikkert nett. Elektronisk samhandling uten å ha vissheten for *hvem* man samhandler med og uten å vite om det som sendes er det som kommer fram eller om noen har lest det underveis er ikke en god og trygg løsning for forvaltningens kommunikasjonsbehov. Utbredelsen av sikre og standardiserte løsninger for autentisering av kommunikasjonspartnere og beskyttelse av den elektroniske informasjonen som utveksles – digitale signaturer – kan vise seg å være en god og effektiv løsning på problemet.

Digitale signaturer representerer en bestemt måte å implementere elektroniske signaturer på. I lov om elektronisk signatur vedtatt i desember 2000 omtales digitale signaturer som «avansert elektronisk signatur».

Digitale signaturer med tilhørende infrastruktur (PKI = Public Key Infrastructure) gir muligheter for å vite hvem avsenderen av en elektronisk meddelelse er (autentisering) muligheter for å sikre meddelelsen slik at alle forsøk på endringer blir oppdaget og stoppet (integritet) muligheter for å forvrenge innholdet (kryptere) slik at det er uleselig for andre enn mottakeren (konfidensialitet) og muligheter for å knytte innholdet til avsenderen slik at hun ikke kan nekte for å stå bak det (ikke-benekting).

Den store fordelen med infrastruktur for digitale signaturer er at den kan tilby en samordnet sikkerhetsløsning for elektronisk tilgang til forvaltningens tjenester og elektronisk innrapportering og annen informasjonsutveksling med og i forvaltningen. Samordnede sikkerhetsløsninger vil kunne redusere forvaltningens kostnader ved etablering og utvikling av slike tjenester og vil kunne gi forenklinger for forvaltningens brukere.

Alternative løsninger til digitale signaturer finnes på enkelte områder (særlig når det gjelder autentisering). Det er imidlertid svært få om noen standardiserte løsninger som kan støtte elektronisk signering for ikke-benekting. For anvendelser i forvaltningen som trenger god sikring mot benekting av transaksjoner er digitale signaturer en forutsetning for at tjenesten skal kunne tilbys elektronisk.

Man trenger ikke å forstå «innmaten» i ny teknologi for å ha glede og nytte av den men man må som bruker beherske anvendelsen av den. Det som fortoner seg enkelt for brukere er ofte svært komplekst og avansert «bak kulissene». Innføring og bruk av digitale signaturer med tilhørende infrastruktur medfører en rekke teknologiske juridiske organisatoriske og administrative utfordringer. Dette er et komplisert felt for forvaltningen å forholde seg til. Derfor trenger den en politikk på området der det med politikk forstås normer for bruk grunnleggende prinsipper for etablering innføring og vedlikehold av infrastrukturen samt strategier for hvordan forvaltningen skal legge forholdene til rette for å sikre at den virker etter forutsetningene.

Denne utredningen foreslår grunnleggende elementer i en slik politikk.

2.2 Anbefalinger på enkelte mandatpunkter

2.2.1 Sertifikattyper og identifisering

For å kunne bruke digitale signaturer i stor skala trengs det et digitalt sertifikat. Et slikt sertifikat er en elektronisk legitimasjon av eieren som gir sikkerhet for at den digitale signaturen virkelig tilhører henne.

Utvalget har drøftet hvem som vil trenge slike sertifikater hva sertifikatene skal inneholde av informasjon samt hvordan informasjonen skal tolkes og særlig hvordan det skal bli mulig å identifisere fysiske og juridiske personer på en pålitelig måte i et slikt sertifikat.

Utvalget vil peke på at spørsmål behandlet her i høyeste grad er et internasjonalt anliggende og anbefalinger må sees i et slikt perspektiv. Det foregår et omfattende internasjonalt og europeisk standardiseringsarbeid på området og vedtakelsen av EU-direktivet om elektroniske signaturer setter klare premisser for valgene som kan gjøres.

Utvalget søker i sine anbefalinger å legge dette til grunn så langt situasjonen på den internasjonale arena er avklart på det tidspunktet innstillingen avgis.

Utvalget har kommet fram til at det i samhandling med og i forvaltningen kan være behov for fire typer sertifikater:

- Ansattsertifikater (sertifikater for de ansatte i forvaltningen)
- Virksomhetssertifikater (sertifikater for virksomheter)
- Offentlige personsertifikater (sertifikater for privatpersoner)
- Profesjonssertifikater (personlige sertifikater som knytter en person til et bestemt yrke/utdanning og eventuelt autorisasjon/godkjenning fra en myndighet eller en organisasjon.

Utvalget anbefaler at disse sertifikatene inneholder informasjon som kodes og fortolkes i samsvar med profiler[2]basert på internasjonale og europeiske standarder. Profiler for de fire definerte sertifikattypene er vedlagt utredningen.

Utvalget anbefaler at det i sertifikater for ansatte i forvaltningen enten benyttes et ansattnummer eller en unik personlig kode for unik identifisering i den grad dette er nødvendig for å skille to ansatte i samme virksomhet fra hverandre.

Utvalget anbefaler at sertifikater for fysiske personer (offentlige personsertifikater) bør ha identifikatorer som tildeles av en sertifikatutsteder og som er unike for hver person hos sertifikatutstederen. Slike identifikatorer (tall og/eller bokstaver) bør være forskjellige fra personens fødselsnummer. Det må finnes en kopling hos utstederen mellom det unike nummeret og fødselsnummeret. De forvaltningsenhetene som har tjenstlige behov kan få tilgang til sertifikateiers fødselsnummer via sertifikatutsteder.

I anvendelser der en offentlig virksomhet har begrunnet behov for direkte bruk av fødselsnummer i sertifikatet (dette gjelder f.eks. trygdeetaten) bør dette tillates.

Utvalget ser ikke behov for å ha fullt navn iht. folkeregisteret i sertifikatet dersom sertifikatutsteder sjekker dette før utstedelse. Sertifikatet vil inneholde personens vanlig brukte navn. Gjennom oppslag i folkeregisteret skal utstederen verifisere at det er den rette personen som skal få sertifikatet.

Utvalget anbefaler at virksomhetssertifikater inneholder organisasjonsnummer fra Enhetsregisteret i Brønnøysund som unik identifikator. I profesjonssertifikater anbefaler utvalget at et nummer fra det

---

2

En profil er en presisering av en standard tilpasset et konkret anvendelsesområde.

relevante registeret over personellet i den aktuelle yrkesgruppen benyttes som unik identifisering. Eksempel på et slikt nummer kan være helsepersonellnummer. Bruk av profesjonssertifikater diskuteres i helsesektoren.

Innholdet i sertifikater kan variere etter sertifikattype og det kan variere med sertifikatutsteder. Alle steder et sertifikat skal behandles automatisk må det finnes klare regler for hvordan innholdet i hvert aktuelt informasjonselement skal kunne fortolkes og behandles. Dette vil skape utfordringer når forvaltningen mottar sertifikater utstedt av ukjente utstedere f.eks. fra utlandet. Når det gjelder håndtering av sertifikater fra utlandet viser utvalget til at utredning og tilrettelegging av dette må inngå som en av flere oppgaver for samordningsfunksjonen som er omtalt i punkt 2.2.3.

Utvalgets vurderinger angående dette mandatpunktet er å finne i kapittel 7.

2.2.2 Sikkerhetsnivåer

For å kunne signere digitalt utstyres sertifikateieren med et sett med såkalte nøkler (kryptografiske koder) bestående av en privat og en offentlig nøkkel. Den offentlige nøkkelen ligger i det digitale sertifikatet som er tilgjengelig for alle. Den private nøkkelen er hemmelig og skal oppbevares på en betryggende måte.

Hver utsteder av digitale sertifikater og nøkler må dokumentere at han tilfredsstiller sikkerhetskrav til utstedelse håndtering og vedlikehold av sertifikater og nøkler. Slik dokumentasjon kalles hhv. sertifikatpolicy og sertifikatpraksis. Sertifikatpolicyen gir et bilde av sikkerhetsnivået på sertifikatet.

Utvalget har drøftet behovet for ulike sikkerhetsnivåer for sertifikatene som forvaltningen kan bruke internt eller som brukere kan benytte mot forvaltningen. Utvalget foreslår tre grunnleggende sikkerhetsnivåer for digitale signaturer/PKI-løsninger som forvaltningen kan bruke.

Nivå 3 innebærer at sertifikater og tilhørende private nøkler lagres i smartkort og at beregningene utføres i kortet. Nivå 2 skiller seg sikkerhetsmessig fra nivå 3 ved at nøkler og sertifikater ikke trenger å være lagret i et smartkort men kan lagres f.eks. kryptert i en PC eller på en særskilt diskett.

For begge nivåer anbefaler utvalget at det benyttes sikre og pålitelige krypteringsalgoritmer og at eiere av sertifikater må møte opp personlig minst én gang for å kunne identifiseres med sikkerhet i forbindelse med utstedelse av et sertifikat for digitale signaturer. Det bør også finnes sikre rutiner for utlevering av nøkler og sertifikater til eiere.

Utvalget anbefaler at det for hver sertifikateier skal genereres tre separate sett med nøkler hvert sett til sitt bruk. De tre nøkkelsettene skal benyttes hhv. til signering autentisering og kryptering.

Utvalget ser at det i en overgangsfase kan være nødvendig med bruk av kun to nøkkelpar på grunn av at eksisterende løsninger i markedet i begrenset grad støtter tre separate nøkkelpar. Ved slik bruk anbefaler utvalget at funksjoner som tillegges disse to nøklene fordeles slik at krypteringsfunksjonen skal ha sin egen nøkkel. Utvalget mener at det kan legges administrative begrensninger på bruk av en kombinert nøkkel for signerings- og autentiseringsfunksjon der det kan være behov for det. Slike begrensninger kan innebære at en nøkkel bare skal brukes til f.eks. signering selv om den også er merket for autentisering.

Videre anbefaler utvalget at tilgangen til private nøkler skal være sikret med en PIN-kode eller et passord med tilstrekkelig sikkerhet.

Nivå 1 dekker sertifikater som ikke tilsvarer nivå 3 og nivå 2 dvs. sertifikater som har lavere sikkerhet. På samme nivå ansees løsninger der PIN-koder og passord benyttes direkte for elektronisk samhandling/tilgang til systemer.

Utvalget ønsker ikke å gi noen anbefalinger vedrørende sikkerhet på dette nivået.

Utvalget anbefaler at det lages en felles sertifikatpolicy for utstedelse av sertifikater på nivå 3 og en tilsvarende felles policy for nivå 2. Disse policyene bør ta utgangspunkt i Forvaltningsnettsamarbeidets sertifikatpolicy nr. 1 [2] og i den europeiske standarden fra ETSI *Policy requirements for certification authorities issuing qualified certificates* [23]. Fellespolicyene som skal lages bør også tilpasses de sertifikattypene og sertifikatprofilene som utvalget anbefaler.

Forvaltningsnettsamarbeidets sertifikatpolicy FSP-1 bør tilpasses de unike identifikatorene utvalget anbefaler samordnes med ETSI-standarden samt de nye anbefalte sertifikatprofilene. Utvalget anbefaler ikke obligatorisk bruk av felles sertifikatpolicyer for forvaltningen.

Utvalgets anbefalinger på dette punktet baserer seg på dagens situasjon når det gjelder tilgjengeligheten av aktuelle teknologier og graden av standardisering av dem. Anbefalinger vil kunne endres dersom utviklingen endrer forutsetningene som ble lagt til grunn her.

Utvalgets anbefalinger angående dette mandatpunktet kan danne et utgangspunkt for offentlige virksomheters valg av sikkerhetsnivå for sine elektroniske anvendelser. Et valg må alltid baseres på individuell vurdering av hver enkelt anvendelse. Utvalget vil ikke gi anbefalinger når det gjelder hvilke sikkerhetsnivåer som kan passe for hvilke anvendelser men uttaler seg veiledende om bruk jf. anbefalinger vedrørende modeller for sertifikatutstedelse nedenfor.

Utvalgets vurderinger angående dette mandatpunktet er å finne i kapittel 8.

2.2.3 Modeller for sertifikatutstedelse samt organisering av forvaltningens samordningsbehov

Utvalget har drøftet ulike modeller for hvordan PKI kan etableres for forvaltningen og for forvaltningens brukere på en kostnadseffektiv og hensiktsmessig måte. Etablering av infrastrukturen innebærer at man avklarer hvem som skal utstede sertifikater og med hvilken sikkerhet hvem som skal sikre at sertifikater utstedes til riktige eiere (registreringsfunksjon) hva slags kostnader som kan forventes ved bruk av infrastrukturen og hvem som skal dekke dem. Avklaringer må gjøres både for forvaltningens interne bruk og for brukere av offentlige tjenester og virksomheter som forvaltningen samhandler med.

Modellene som omtales i dette kapitlet dreier seg om leveranse av sertifikater med sikkerhetsnivå 3 eller 2. Utvalget ønsker ikke å uttale seg om når sertifikater på nivå 1 skal kunne brukes. Dette er et valg som tilligger hver offentlig virksomhet som ønsker å ta i bruk sikkerhetsløsninger for elektronisk samhandling. Utvalget mener imidlertid at det ved slike valg bør vurderes grundig om «sterk» sikkerhet er nødvendig eller om man kan klare seg med løsninger på lavere nivå.

Utvalget anbefaler at forvaltningen forsynes med sertifikater for sine ansatte gjennom etablering av en ny utvidet rammeavtale om digitale signaturer og sertifikattjenester under Forvaltningsnettsamarbeidets innkjøpsordning. Rammeavtalen skal også tilby produkter og/eller tjenester som gjør det mulig for en offentlig virksomhet selv å kunne utstede sertifikater til sine ansatte. Sertifikater for offentlig forvaltning bør i hovedsak være sertifikater med sikkerhetsnivå 3 men sertifikater med sikkerhetsnivå 2 kan ikke utelukkes brukt dersom behovet tilsier det.

Utvalget anbefaler at det for forsyning av sertifikater til enkeltpersoner inngås samarbeidsavtaler med minst to aktører i markedet som utsteder eller vil utstede sertifikater til enkeltpersoner i forbindelse med egen bruk av PKI. Slike aktører kan f.eks. være bankene.

Kostnader ved bruk av slike sertifikater mot offentlig sektor bør i startfasen ikke belastes enkeltpersoner. Sertifikatene bør ha sikkerhet på minimum nivå 2 med overgang til nivå 3 når tilsvarende løsninger foreligger i markedet og er bredt tilgjengelige for enkeltpersoner.

Utvalget anbefaler at det bør høstes flere praktiske erfaringer med bruk av sertifikater i forbindelse med elektronisk samhandling mellom næringslivet og forvaltningen før man foreslår fellestiltak fra forvaltningens side.

Utvalget anbefaler at det settes av egne midler til stimulering av bruk av digitale signaturer og PKI i forvaltningen. Slike midler bør tildeles prosjekter der digitale signaturer innføres i samsvar med vedtatte fellesordninger og anbefalte felles standarder.

Utvalget anbefaler at det etableres en permanent samordningsfunksjon for bruk av PKI i samhandling med og i forvaltningen. Funksjonen bør organiseres som et fast utvalg med et sekretariat med eget driftsbudsjett. Utvalget bør bestå av sentrale samordningsmyndigheter og brukervirksomheter på alle forvaltningsnivåer. Utvalget bør ledes av et IT-samordningsdepartement – enten AAD eller NHD. Samordningsfunksjonen bør samarbeide med Post- og teletilsynet og med Datatilsynet som er tilsyn etter lov om elektronisk signatur. Utvalget mener at mandatet for samordningsutvalget samt sekretariatets oppgaver plassering og finansiering bør bli gjenstand for en drøfting mellom berørte departementer og eventuelt underliggende etater samt representanter for kommunesektoren. Utvalget mener at en slik drøfting bør komme i gang straks.

Utvalget anbefaler at det med utgangspunkt i samordningsfunksjonen etableres et eget Forum for digitale signaturer med representanter fra forvaltningen næringslivet og leverandørene for å drøfte felles standarder på området PKI.

Utvalgets vurderinger angående dette mandatpunktet er å finne i kapittel 9.

2.2.4 Samtrafikk

PKI er teknologisk juridisk og organisatorisk komplisert infrastruktur. Mange aktører deltar i infrastrukturen (jf. kapittel 3) med ulike roller og ansvar. For brukere av infrastrukturen kan dette skape en del utfordringer.

Valget av strategi for etablering av PKI (jf. punkt 2.2.3) fører med seg konsekvenser som kompliserer bruken av PKI ytterligere. Ønsket om å utnytte markedskreftene og konkurranseaspektet medfører krav til markedsaktørene om å kunne spille sammen slik at deres kunder ikke får begrenset valgfrihet når det gjelder hvem de kan kommunisere elektronisk med.

For en bruker av et sertifikat (dvs. den som mottar en signatur med sertifikat og skal kunne stole på denne) er utfordringen om dette sertifikatet kommer fra den utstederen som hun kjenner og har tillit til eller om det kommer fra en helt annen utsteder som hun ikke vet noe om. Hvordan vurdere sikkerheten ved et slikt sertifikat? Kan man stole på at signaturen likevel er ekte? Kan det hende at denne utstederen har slurvet med registreringen av sertifikateieren slik at denne nå opptrer under falsk identitet? Dette er spørsmål som sertifikatbrukere må kunne få svar på dersom de skal benytte en åpen infrastruktur der flere aktører kan utstede sertifikater til ulike målgrupper og der det kan velges fritt mellom disse utstederne.

Utfordringene kan også knytte seg til teknologier som benyttes. Selv om standardiseringen av PKI er kommet et stykke på vei finnes det fremdeles en rekke måter å implementere dette på som kan skape problemer når brukere av ulik programvare for signering og kryptering skal kommunisere og utveksle digitalt signerte meldinger eller dokumenter.

Utvalget har drøftet ulike sider ved behov for samtrafikkløsninger i en slik infrastruktur. Vurderingene knytter seg til behovet for ulike tillitsstrukturer som kan bøte på problemet med ukjente sertifikatutstedere og behovet for godt samvirke mellom programvare for digitale signaturer og kryptering fra ulike leverandører.

Utvalget anbefaler at forvaltningen bidrar til at det etableres tillitsstrukturer i markedet som kryssertifisering av utstedere eller en toppnode som sertifiserer alle utstedere innen et gitt område. Utvalget anbefaler at forvaltningen krever denne type tillitsstrukturer for utstedere forvaltningen har avtaler med.

Utvalget anbefaler at forvaltningen sammen med markedsaktørene tar initiativ til at det etableres en felles samtrafikktjeneste som brukere både i forvaltningen og i resten av samfunnet kan benytte seg av. Utvalget anbefaler at forvaltningen spiller en aktiv rolle i etableringen av en slik tjeneste i det norske markedet. Forvaltningen bør kunne bidra med eventuell delfinansiering for initiering av tjenesten. Tjenesten må ellers basere seg på kommersielle vilkår for drift.

Utvalgets vurderinger angående dette mandatpunktet er å finne i kapittel 10.

2.2.5 Regler for bruk av digitale signaturer i forvaltningen

På grunnlag av en juridisk delutredning har utvalget drøftet behov for regulering av bruken av digitale signaturer og tilhørende infrastruktur i forvaltningen og mot forvaltningens brukere. En slik bruk ble her sett i sammenheng med andre rutiner som er nødvendige ved elektronisk kommunikasjon og behandling av dokumenter.

Formålet med reglene er å beskrive hovedprinsippene for hvorledes elektronisk kommunikasjon med forvaltningen kan og skal skje med mulighet for å tilpasse løsningene til det enkelte forvaltningsorgans behov. Videre foreslås det regler for forvaltningsintern bruk av digitale signaturer og sertifikater.

Utvalget fremmer en skisse til et regelverk som gir konkrete anvisninger for elektronisk kommunikasjon mellom forvaltning og enkeltpersoner og innad i forvaltningen. Forslaget omfatter regler for både autentisering og signering samt beskyttelse av konfidensialitet. Reglene knyttes an til forvaltningslovens generelle bestemmelser om saksbehandling i forvaltningssaker.

Utvalget anbefaler at man nedfeller nødvendige regler i en ny forskrift forankret i forvaltningsloven og i lov om elektronisk signatur. En forskrift kan utformes på grunnlag av forslaget her. Utvalget mener at arbeidet med forskriften bør knyttes til gjennomføringen av eRegel-prosjektet (jf. punkt 5.2.5) og den revisjonen av forvaltningsloven som skjer som følge av dette prosjektet.

Utvalget mener at forvaltningsinterne forhold knyttet til krav til godkjenning og anskaffelse av sikkerhetstjenester og -produkter for forvaltningen samt regler om intern saksbehandling bør inntas i samme forskrift med mindre sterke hensyn taler imot.

Utvalget mener at de rettslige virkningene av at man benytter systemer valgt eller godkjent av forvaltningen eller sertifikater tilhørende forvaltningen må framgå av forskriftene eller loven som hjemler dem.

Utvalget mener at beskyttelsesinstruksens regler for behandling av graderte dokumenter ved elektronisk kommunikasjon bør kunne samordnes med regelverket som er foreslått her.

Utvalgets vurderinger angående dette mandatpunktet er å finne i kapittel 11.

2.2.6 Elektroniske identitetskort

Brukere av offentlige elektroniske tjenester vil ønske at sikkerhetsløsninger som benyttes er enkle å bruke samtidig som de er pålitelige og sikre. For å imøtekomme slike ønsker må offentlig sektor ty til kraftige samordningstiltak også når digitale signaturer med tilhørende infrastruktur benyttes. Elektroniske ID(identitets)-kort er en slik samordnet løsning som vil kunne gi brukere av offentlige elektroniske tjenester en «universalnøkkel» til forvaltningen på nett.

Et elektronisk ID-kort er et smartkort som inneholder en elektronisk identitet – EID. EID består av tre sett krypteringsnøkler med tilhørende offentlige personsertifikater til bruk for digital signering autentisering og dokumentkryptering. Kortet må ha en viss informasjon om eieren trykt utenpå men skal ikke nødvendigvis fungere som et alminnelig fysisk identitetskort. Et slikt elektronisk ID-kort skal kunne brukes til elektronisk signering og kryptering av dokumenter eller til pålogging til forvaltningens elektroniske tjenester hjemme på et offentlig servicekontor eller annet offentlig sted hvor det er lagt til rette for pålogging til Internett-tjenester med et slikt kort.

Det forutsettes her at kortet utstedes av en offentlig myndighet som kan påta seg ansvaret for riktig identifisering og verifisering av korteiere og som garanterer for sikre utleverings- og tilbaketrekkingsrutiner samt sikker infrastruktur for bruk av slike kort.

Utvalget har sett på en slik løsning som er etablert i Finland. Utvalget har merket seg at for å få en slik løsning til å fungere kreves det kraftig koordinering mellom selve ID-kort-løsningen og utviklingsarbeidet som vil pågå i de offentlige virksomheter som ønsker å legge ut elektroniske interaktive tjenester på nett. Mye tyder på at de finske myndighetene har fått problemer med slik koordinering ettersom tilfanget av offentlige tjenester der det elektroniske ID-kortet kan benyttes foreløpig er begrenset.

Utvalget har merket seg at det ennå ikke finnes et bredt tilbud i markedet på PC-utstyr med leser for ID-kort integrert som standardutrustning og at utbredelsen av slikt utstyr i norske husholdninger er nesten lik null. Denne situasjonen kan endre seg når private aktører som tilbyr elektroniske tjenester med sikkerhet basert på slike kort går bredt ut til befolkningen. En første prøvestein i så måte ser ut til å bli Norsk Tipping med elektroniske tippekort som prøves ut i 2001.

Utvalget tror at etablering av en slik ordning vil kunne kreve store investeringer og en større prosess for å få den på plass. Utvalget mener at man ut fra hensynet til markedet må være forsiktig med etablering av offentlige tilbud på et område der det vil finnes løsninger i markedet.

På grunnlag av disse foreløpige vurderingene anbefaler ikke utvalget at forvaltningen skal gå i gang med egen etablering av en offentlig ordning for utstedelse av elektroniske ID-kort nå. Utvalget mener at ut fra samfunnsmessige og økonomiske betraktninger og for å unngå dobbeltarbeid bør forvaltningen løpende vurdere å ta i bruk ID-kort som kommersielle aktører i markedet tilbyr. Dette er også konsistent med strategien for forsyning av enkeltpersoner med sertifikater som anbefales i punkt 2.2.3 når slike sertifikater tilbys på smartkort.

Utvalget anbefaler at situasjonen i markedet observeres (både i Norge og i utlandet) og at erfaringer høstes før en eventuell videre utredning av saken.

Utvalgets vurderinger angående dette mandatpunktet er å finne i kapittel 12.

2.2.7 Økonomiske og administrative konsekvenser av utvalgets anbefalinger

Utvalgets anbefalinger innebærer etablering av et nytt fast samordningsutvalg som skal dekke hele forvaltningen inklusive regional og lokal forvaltning. Videre kan behovet for et sekretariat for utvalget føre til etablering av et eget organ eller plassering av en funksjon i en eksisterende virksomhet.

Utvalgets anbefalinger innebærer etablering av et forum for utveksling av erfaringer mellom forvaltningen næringslivet og leverandørene av løsninger for digitale signaturer. Forvaltningen skal være initiativtaker men ellers delta på like vilkår med de andre partene.

Utvalgets anbefalinger medfører etablering av en ny rammeavtale for forvaltningen med løsninger for digitale signaturer og PKI. Rammeavtalen bør tre i kraft innen rimelig kort tid etter at gjeldende rammeavtale under Forvaltningsnettsamarbeidet har utløpt (1.6.2001).

Utvalgets anbefalinger medfører forhandlinger mellom forvaltningen representert ved samordningsfunksjonen og aktører i markedet med sikte på etablering av en avtale om utstedelse av sertifikater til enkeltpersoner.

Kostnader ved sekretariatet for samordningsfunksjonen estimeres årlig til ca. kr 6 5 mill. (1–2 årsverk samt driftsbudsjett). Driftsmidlene tenkes benyttet til utredninger utarbeidelse av grunnlaget for rammeavtaler utvikling av felles sikkerhetskrav og evaluering av løsninger i markedet. Videre skal driftsmidlene benyttes til å finansiere forvaltningens deltakelse i det felles erfaringsforumet og ev. bidrag til etablering av en felles samtrafikktjeneste.

Offentlige virksomheter som vil utpeke deltakere til det faste samordningsutvalget skal finansiere denne deltakelsen selv. Det estimeres ressursbruk tilsvarende 2 månedsverk pr. år for hver deltaker og 4 månedsverk for leder.

Det forutsettes at det felles erfaringsforumets virksomhet finansieres av deltakerne.

Utvalget anbefaler at det avsettes stimuleringsmidler for bruk av digitale signaturer i offentlige virksomheter i størrelsen 9 mill. kr i 2002. Midlene bør kunne tildeles prosjekter der digitale signaturer blir tatt i bruk for å understøtte elektroniske tjenester til enkeltpersoner og til næringslivet både på statlig og på kommunalt nivå. Utvalget mener at ett av kriteriene for tildeling av midler bør være at prosjektene benytter seg av felles løsninger som foreslås etablert. Utvalget viser til tilsvarende satsing i Danmark i 1998–1999 der evalueringsrapporten framlagt høsten 2000 konkluderte med at satsingen var til god nytte for den danske forvaltning.

Utvalgets vurderinger

angående dette mandatpunktet er å finne i kapittel 13.

2.3 Forslag til videre utredningsarbeid

Utvalget mener at håndtering av utenlandske sertifikater bør utredes nærmere særlig i lys av implementeringen av EU-direktiv 1999/93/EC i EØS-området og løsninger i land utenom EØS.

Videre mener utvalget at det bør utredes hvordan en eventuell utstedelse av profesjonssertifikater skal foregå. Dette bør skje i samarbeid med myndigheter og organisasjoner som har ansvaret for føring av relevante registre over yrker/utdanninger som gir rettigheter.

I forbindelse med utvalgets anbefaling om at forvaltningen bidrar til etablering av en felles samtrafikktjeneste for sertifikater i det norske markedet bør forvaltningen utrede sine krav til en slik samtrafikktjeneste. Videre bør forvaltningen utrede hvilke felles krav man bør stille til verifikasjonsinformasjon som framkommer ved behandling av sertifikater.

Et annet spørsmål som utvalget mener bør utredes nærmere er om det i forvaltningsloven bør åpnes for helt automatiske beslutningsprosesser og hvilke krav dette vil stille til systemer dokumentasjon med mer samt hva slags sårbarhet en slik åpning kan skape.

Utvalget mener det er naturlig at ovennevnte utredninger bør initieres og gjennomføres i regi av den foreslåtte samordningsfunksjonen.

Utenom disse utredningene vil det være behov for avklaringer av en rekke spørsmål knyttet til konkret innføring av digitale signaturer og PKI innen enkelte sektorer virksomheter eller på bestemte anvendelsesområder. Bl.a. bør spørsmål knyttet til interne rutiner for arkiv og postmottak ved behandling av digitalt signerte dokumenter utredes. Utvalget ser behov for utvikling av rutiner og prosedyrer ved bruk av digitale signaturer innen elektronisk saksbehandling elektronisk økonomistyring elektroniske offentlige innkjøp med mer. Dette arbeidet bør skje i regi av relevante departementer og etater. Utvalget mener at den foreslåtte samordningsfunksjonen bør kunne trekkes inn også i dette arbeidet.

Del II
Beskrivelse av problemstillingen og status for digitale signaturer og PKI

3 Hva er digitale signaturer og PKI?

3.1 Behovet for sikring av elektronisk samhandling

For å kunne ta ut gevinster knyttet til overgangen til døgnåpen elektronisk forvaltning har forvaltningen behov for å gjøre elektronisk dokumentbehandling og kommunikasjon seg imellom med publikum og med bedrifter like sikker som samhandling ved hjelp av papirdokumenter. Til denne samhandlingen trengs det en effektiv og pålitelig infrastruktur for elektronisk informasjonsutveksling som kan medvirke til at elektronisk samhandling gis samme juridiske gyldighet som den papirbaserte. Infrastrukturen må være tilrettelagt slik at det er mulig å skape tillit mellom parter som ikke kjenner hverandre fra før og slik at det eksisterer mekanismer for beskyttelse av informasjonen mot ulike former for forfalskning og andre angrep.

Internett er «den elektroniske motorveien» der informasjon kan utveksles mellom ulike aktører og på ulike måter. Men Internett er i utgangspunktet ikke et sikkert nett. Elektronisk samhandling uten å ha vissheten for *hvem* man samhandler med uten å vite om det som sendes er det som kommer fram eller om noen har lest det underveis er ikke en god og trygg løsning for forvaltningens kommunikasjonsbehov. Utbredelsen av sikre og standardiserte løsninger for autentisering av kommunikasjonspartnere og beskyttelse av den elektroniske informasjonen kan bidra til at Internetts potensial for å kunne utnyttes i forvaltningens elektroniske samhandling kan realiseres fullt ut.

Elektronisk signatur er et upresist og overordnet fellesbegrep som kan dekke flere metoder eller teknikker for å knytte en person sammen med et dokument. Én mulig teknikk kan være å tegne navnetrekket sitt nederst på dokumentet ved hjelp av mus spesialpenn eller liknende. Men slike signaturer kan lett klippes bort og erstattes med andres hvis man ikke bruker spesielle teknikker for å holde navn og dokument sammen. Lov om elektronisk signatur definerer begrepet elektronisk signatur som *data i elektronisk form som er knyttet til andre elektroniske data og som brukes til å kontrollere at disse stammer fra den som fremstår som undertegner* [52]**.**Det finnes (biometriske) teknikker der man kan vise at en visuell underskrift er knyttet til dokumentet [3]men det er få som er basert på åpne tilgjengelige standarder.

Den mest lovende og stadig mer brukte løsningen for elektroniske signaturer i dag er digitale signaturer med tilhørende infrastruktur såkalt PKI (Public Key Infrastructure). Navnet på infrastrukturen henspiller på den teknologien som ligger til grunn nemlig offentlignøkkel-kryptografi. Denne teknologien gir muligheter for å vite hvem avsenderen av en elektronisk meddelelse er (*autentisering*) muligheter for å sikre meddelelsen slik at alle forsøk på endringer blir oppdaget (*integritet*) muligheter for å forvrenge innholdet (*kryptere*) slik at det blir uleselig for andre enn mottakeren (*konfidensialitet*) og muligheter for å knytte innholdet til avsenderen slik at hun ikke kan nekte for å stå bak det (*ikke-benekting*).

De fire egenskapene:

- Autentisering
- Integritetsbeskyttelse
- Konfidensialitetsbeskyttelse og
- Sikring av ikke-benekting

er vesentlige å ivareta når man skal innføre elektronisk samhandling over nett i stor skala.

3

Fordelen med en infrastruktur for digitale signaturer er at den kan tilby en samordnet sikkerhetsløsning for elektronisk tilgang til forvaltningens tjenester elektronisk innrapportering og annen informasjonsutveksling med og i forvaltningen. Samordnede sikkerhetsløsninger vil kunne redusere forvaltningens kostnader ved etablering og utvikling av slike tjenester og de vil kunne gi forenklinger for forvaltningens brukere. For anvendelser i forvaltningen som trenger god sikring mot benekting av transaksjoner er digitale signaturer en forutsetning for at tjenesten skal kunne tilbys elektronisk.

3.2 Teknologien som digitale signaturer bygger på

3.2.1 Kryptografi

Kryptografi er en tusen år gammel metode for å skjule innhold i en skriftlig meddelelse. De første krypteringsmetodene benyttet f.eks. enkle algoritmer (beregningsmetoder) som gikk ut på å forskyve bokstavene i alfabetet et visst antall plasser.

For å kunne lese (*dekryptere*) et skjult innhold trengte mottakeren en nøkkel. Nøkkelen fortalte hva som måtte gjøres for å få fram den opprinnelige teksten. En nøkkel for tekst kryptert etter algoritmen nevnt over kunne være 3H som betydde at forskyvingen av alfabetet var 3 bokstaver mot høyre.

Moderne kryptografi benytter avanserte matematiske funksjoner for å forvrenge innhold i dokumenter og meldinger. Moderne kryptografi er avhengig av datamaskiner for å fungere.

Det finnes to hovedtyper kryptografiske metoder som benyttes i dag:

- Symmetrisk kryptografi
- Asymmetrisk kryptografi.

Navnene på disse metodene henspiller på hvordan nøklene brukes i hver av dem.

Symmetrisk kryptografi baserer seg på samme grunnleggende metode som for tusen år siden. Avsenderen og mottakeren av en kryptert meddelelse må ha den samme nøkkelen for å kryptere og dekryptere teksten.

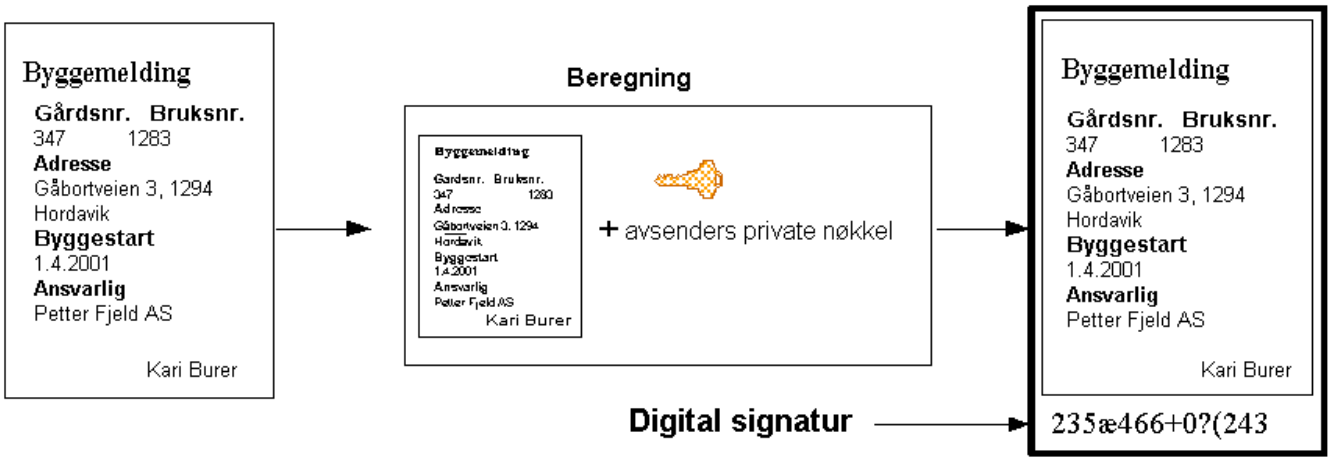
Dette skaper problemer mht. å distribuere nøkkelen til alle som behøver å ha den for å kunne dekryptere hemmelige meddelelser. Faller nøkkelen i hendene på uvedkommende kan den hemmelige meldingen leses av dem. De som samhandler må bl.a. skaffe seg en ny felles nøkkel for fortsatt å kunne sende hemmelige meldinger til hverandre. Fordelen med symmetrisk kryptering er at de matematiske metodene som benyttes gjør at kryptering av store tekstmengder kan utføres raskt.

Asymmetrisk kryptografi håndterer problemet med distribusjon av nøkler. Hver deltaker har i utveksling av hemmelige dokumenter to ulike nøkler – et nøkkelpar. En av nøklene er hemmelig og bare kjent for eieren. Denne kalles den *private nøkkelen*. Den andre nøkkelen vil være offentlig kjent og tilgjengelig for alle andre deltakere. Denne nøkkelen kalles den *offentlige nøkkelen*. Den matematiske metoden som ligger til grunn gjør det mulig å benytte den offentlige nøkkelen til å kryptere en meddelelse slik at bare den private nøkkelen kan dekryptere den. Ulempen med denne måten å kryptere på er at den er tidkrevende ved kryptering av store tekstmengder.

Asymmetrisk kryptografi har flere muligheter enn bare kryptering av dokumenter. Dersom man krypterer en meddelelse med den private nøkkelen er det bare den offentlige nøkkelen som kan dekryptere den. Dette ga opphavet til digitale signaturer.

3.2.2 Digitale signaturer

Digitale signaturer er en måte å benytte asymmetrisk kryptografi på som gir sikkerhet for at det er den rette personen som har sendt meddelelsen. Metoden som benyttes gir også sikkerhet for at meddelelsen ikke er blitt forfalsket av uvedkommende underveis fra avsender til mottaker (integritet).



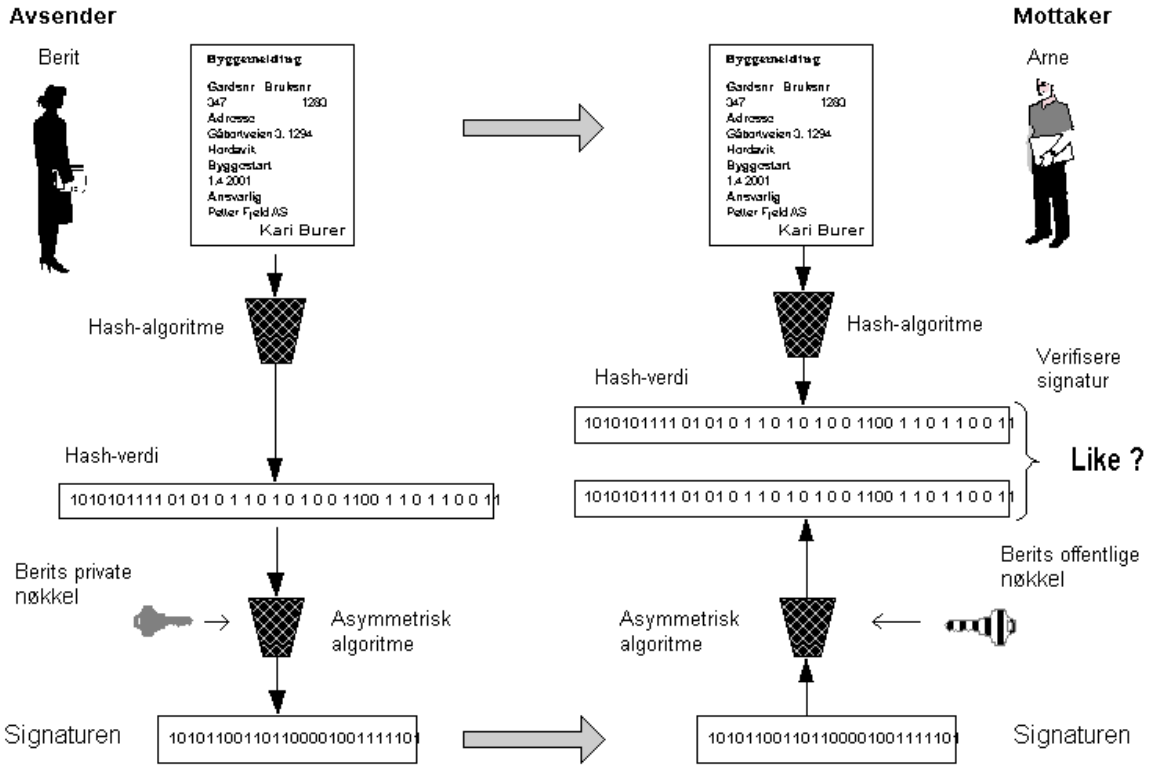
Figur 3.1 Digital signatur

En *digital signatur* er et dataelement som følger en elektronisk melding eller et dokument og som binder dokumentet til et individ en maskin eller et datasystem. Bindingen er slik at signaturen er praktisk umulig å forfalske. Den kan verifiseres av en mottaker eller av en uavhengig tredjepart. Hvis en bokstav i dokumentet endres vil den digitale signaturen ikke bli godkjent [12].

Som nevnt vil kryptering av store tekstmengder med den private nøkkelen ta for lang tid. Derfor tok man i bruk en beregningsmåte kalt *hash-algoritme* når man skulle lage en digital signatur på et dokument. Ut fra dokumentet produserer hash-algoritmen et unikt tall (en *hash-verdi*). Den matematiske funksjonen som benyttes er slik at man ikke kan gjenskape dokumentet ut fra tallet og to ulike dokumenter skal ikke lage samme tall. Man kan si at hash-verdien representerer et dokument på en i praksis unik måte. Hvis så mye som en bokstav blir endret i dokumentet vil hash-verdien bli en annen. Det er hash-verdien av dokumentet som krypteres med den private nøkkelen. *Den krypterte hash-verdien er den digitale signaturen.*

Man kan derfor si at en digital signatur er en unik kombinasjon av den private nøkkelen som ble benyttet og dokumentets innhold slik det representeres av hash-verdien. To ulike personer med to ulike private nøkler vil lage to ulike digitale signaturer på det samme dokumentet. Hvis dokumentet blir endret underveis til mottakeren vil signaturen ikke lenger la seg verifisere. Lov om elektronisk signatur [52] bruker begrepet *signaturframstillingsdata* om koder eller private nøkler som undertegneren benytter for å framstille en elektronisk (i dette tilfellet digital) signatur. Loven bruker begrepet *signaturframstillingssystem* om programvare eller maskinvare som benyttes til å framstille signaturene. Begrepet *signaturverifiseringsdata* benyttes om offentlige nøkler. Signaturer kan beregnes i en PC eller på et smartkort.

Verifisering av en digital signatur skjer ved at mottakeren av et digitalt signert dokument beregner hash-verdi av dette dokumentet. Deretter dekrypterer hun den krypterte hash-verdien som ble tilsendt med dokumentet (den digitale signaturen). Hun dekrypterer den med den offentlige nøkkelen til avsenderen. Denne nøkkelen kan enten sendes med dokumentet eller hentes fra en offentlig tilgjengelig katalog. Så sammenlikner hun de to hash-verdiene (tallene) mot hverandre. Er de helt like er signaturen i orden. Er de ulike så er noe galt dvs. noen har prøvd å endre dokumentet underveis.

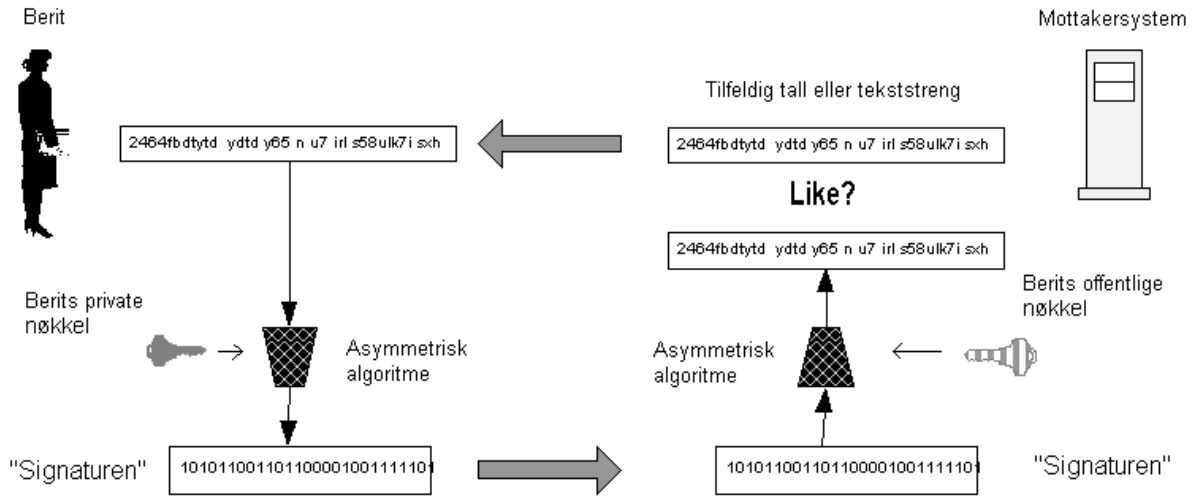


Figur 3.2 Å signere og verifisere et dokument

Dersom mottakeren ikke klarer å dekryptere hash-verdien med den offentlige nøkkelen til avsenderen betyr det at det var en annen privat nøkkel som ble benyttet. Noen har prøvd å utgi seg for eieren av den offentlige nøkkelen men hadde ikke den passende private nøkkelen. Figur 3.2 illustrerer hvordan digital signatur lages og sjekkes (verifiseres).

3.2.3 Autentisering

Digitale signaturer kan brukes på elektroniske dokumenter men ikke bare til det. Man oppdaget at denne metoden som i grunnen gir sikkerhet for hvem som brukte sin private nøkkel også kan benyttes for å verifisere hvem man kommuniserer med over nett. Autentisering kan brukes til å verifisere en påstått identitet eller en mottaker. Man kan med andre ord benytte digitale signaturer for å erstatte passord ved pålogging til datasystemer og tjenester i nettverk. Dette illustreres i figur 3.3.



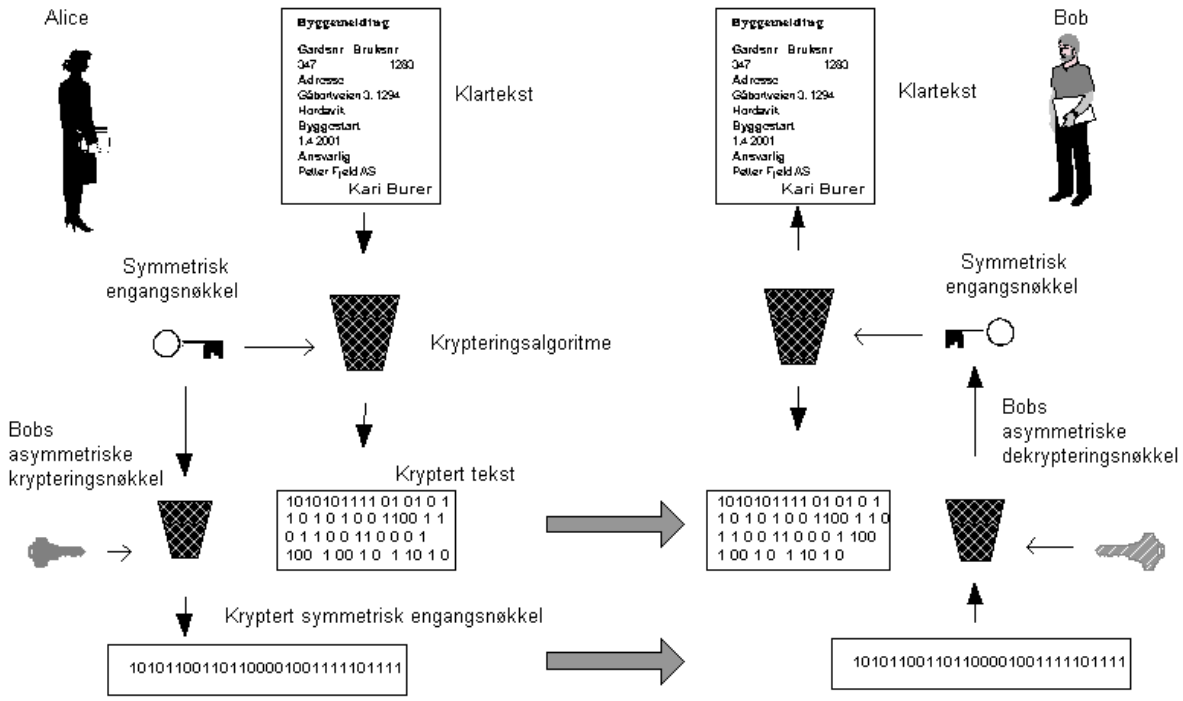
Figur 3.3 Å autentisere en bruker

Mottakersystemet sender et tilfeldig tall eller en tekststreng til den som vil logge seg på. Brukeren krypterer dette tallet med sin private nøkkel. Mottakersystemet verifiserer «signaturen» med brukerens offentlige nøkkel som enten er lagret i systemet eller hentes fra en offentlig katalog. Dersom verifiseringen av brukerens «signatur» har gått bra kan brukeren komme inn i systemet og benytte tjenester i det. Fordelen med å benytte digitale signaturer til autentisering er at de bygger på en standardisert metode som mange datasystemer kan ta i bruk. Brukeren behøver ikke å huske mange ulike passord eller koder som trengs for tilgang til de ulike systemene. Brukeren trenger bare sin private nøkkel og systemene trenger brukerens offentlige nøkkel.

3.2.4 Kryptering

Bruk av nøkkelparet direkte på dokumentets innhold slik at kryptering skjer med den offentlige nøkkelen til mottakeren (som alle kjenner til) og dekryptering med den private nøkkelen til mottakeren (som bare denne kjenner til) var en svært oppfinnsom løsning. Men siden symmetriske algoritmer er raskere enn de asymmetriske førte dette til ideen om å kombinere disse to.

Når et dokument skal krypteres ved bruk av symmetrisk kryptografi skjer dette i to trinn. Det første trinnet er at det genereres en symmetrisk engangsnøkkel en sesjonsnøkkel. Denne brukes så til å kryptere symmetrisk dokumentets innhold. Deretter krypteres denne engangsnøkkelen med den asymmetriske offentlige nøkkelen til mottakeren. Det krypterte dokumentet sendes deretter sammen med den krypterte symmetriske engangsnøkkelen. Mottakeren må først dekryptere den symmetriske engangsnøkkelen med sin private asymmetriske dekrypteringsnøkkel. Deretter dekrypterer han selve dokumentet med den symmetriske nøkkelen. Denne prosessen illustreres i figur 3.4.

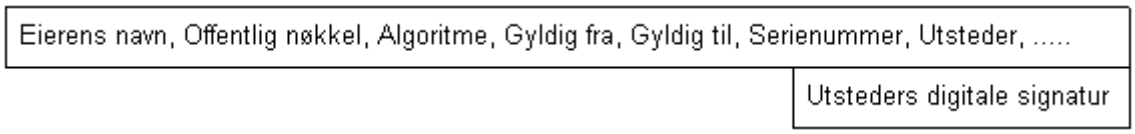


Figur 3.4 Å kryptere og sende en melding

3.2.5 Sertifikater og sertifikatutstedere

Offentlige nøkler gir i seg selv ingen informasjon om eierens identitet. Det må finnes en mekanisme som bekrefter på en tillitvekkende måte at en offentlig nøkkel hører til en bestemt person. Mekanismen kalles digitalt sertifikat eller bare *sertifikat*.

Det fundamentale prinsippet som gjør at digitale signaturer og PKI kan brukes i stor skala er at de offentlige nøklene kan distribueres fritt. Men deltakere i elektronisk samhandling over nett trenger en garanti for at de offentlige nøklene de benytter tilhører den riktige eieren og at de ikke er endret av utenforstående. Det kan tenkes at en eier av et nøkkelpar vil kunne legge ut sin offentlige nøkkel i en katalog eller sende den til mottakeren via e-post. Men hvordan skal mottakeren stole på at nøkkelen virkelig tilhører denne personen? Dette er spesielt kritisk når disse to ikke kjenner hverandre fra før. Løsningen på problemet er at begge stoler på en tredje part som kan ta på seg å bekrefte sammenhengen mellom den offentlige nøkkelen og eieren av nøkkelparet. En slik virksomhet kalles ofte for TTP (tiltrodd tredjepart). En TTP kan utføre mange oppgaver men i denne sammenheng vil han utstede sertifikater som kopler nøkkeleierens identitet (navn og andre opplysninger om eieren) med dennes offentlige nøkkel. Da kaller man TTP-en for *sertifikatutsteder*. Denne betegnelsen benyttes også i lov om elektronisk signatur som regulerer virksomheten til utstedere av såkalte kvalifiserte sertifikater. Disse omtales seinere i utredningen.



Figur 3.5 Eksempel på et digitalt sertifikat

Sertifikatutsteder signerer sertifikatet med sin digitale signatur. Utstederens signatur borger for at sertifikatet er ekte.

Et sertifikat fungerer som et legitimasjonsbevis (når det gjelder å verifisere at det er korrekt person som har signert) og sertifikatutsteder tilsvarer en legitimasjonsutsteder.

Iht. lov om elektronisk signatur er sertifikatutstederen en juridisk person som utsteder sertifikater og tilbyr andre tjenester relatert til elektronisk signatur [52]. Kundene til en sertifikatutsteder må ha tillit til at denne utfører sin oppgave på en tilfredsstillende måte. Grunnlaget for tillit kan variere. Elementer som kan komme med i vurderingen av hvor tillitvekkende en sertifikatutsteder er kan f.eks. være habilitet objektivitet og erfaringer med denne virksomheten over tid.

Sertifikatutstedere utsteder et sertifikat i henhold til en *sertifikatpolicy*. Det er et dokument som inneholder regler for hvordan sertifikater utstedes og behandles og dermed definerer bl.a. hvilken tillit man kan ha til sertifikatene. Innehaveren av et sertifikat kalles *sertifikateier* i denne utredningen. Den som mottar et digitalt signert dokument med et tilhørende sertifikat og som skal verifisere det mottatte materialet kalles *sertifikatbruker.*

Den som ønsker å skaffe seg et sertifikat må henvende seg til en *registreringsenhet* og gi opplysninger om seg selv som enheten kan sjekke. Deretter sender registreringsenheten de verifiserte opplysningene til sertifikatutsteder og ber om at sertifikatet utstedes.

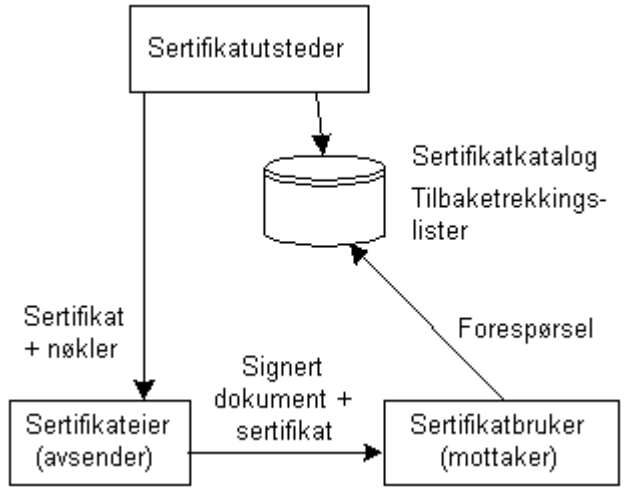
Sertifikater utstedes for begrensete tidsperioder ofte 2 år om gangen. Sertifikatutsteder lagrer kopier av dem i en katalog slik at de er tilgjengelige for sertifikateierens samhandlingspartnere. Sertifikater kan trekkes tilbake dvs. gjøres ugyldige. Det kan skje dersom opplysninger i sertifikatet må endres (på grunn av at eieren f.eks. skifter jobb) eller f.eks. dersom den tilhørende private nøkkelen går tapt eller blir kompromittert på annen måte. Tilbaketrukne sertifikater kunngjøres i en egen liste såkalt tilbaketrekkingsliste. Denne listen tidsstemples og signeres av den sertifikatutstederen som har trukket sertifikatet tilbake.

Det er som regel sertifikatutsteder som genererer nøkkelparet som sertifikateieren skal benytte. I noen tilfeller kan sertifikateieren selv generere sitt nøkkelpar for så å sende sin offentlige nøkkel til sertifikatutstederen og få et sertifikat i retur.

De private nøklene må oppbevares på en betryggende måte. Dette kan gjøres ved f.eks. å lagre dem i et smartkort på en diskett eller kryptert på harddisken i en PC.

3.3 Hvorfor trenger man en infrastruktur for å bruke digitale signaturer?

For å kunne benytte digitale signaturer i stor skala dvs. mellom mange ukjente deltakere i elektronisk samhandling over nett må de ulike oppgavene knyttet til utstedelse av nøkler og sertifikater og til sikker bruk av sertifikater organiseres på en hensiktsmessig måte. Dette gjøres gjennom PKI (Public Key Infrastructure). I sin grunnleggende versjon består denne infrastrukturen av avsenders og mottakers systemer for signering og kryptering samt av en sertifikatutsteder som registrerer sertifikateiere og utsteder og trekker tilbake sertifikater jf. figur 3.6.



Figur 3.6 Elementer i en PKI

3.3.1 Hvordan fungerer en PKI?

Elementer i en PKI kan grupperes som aktører sikkerhetskomponenter sikkerhetstjenester og regulatører.

Aktører

Følgende aktører deltar i en PKI:

- Sertifikatutstedere
- Registreringsenheter (som kan være en del av sertifikatutsteders virksomhet eller være selvstendige virksomheter som har avtale med den)
- Sertifikateiere (avsendere)
- Sertifikatbrukere (mottakere).

I mer komplekse PKI-er kan flere aktører som smartkortprodusenter driftssentraler for sertifikatkataloger samtrafikktjenester og tilsynsmyndigheter også delta.

Sikkerhetskomponenter

Sertifikateiere og sertifikatbrukere trenger spesiell programvare for signering og kryptering av dokumenter/meldinger. Dette innbefatter også behandling av sertifikater. Dersom de private nøklene lagres på et smartkort trengs i tillegg en kortleser.

Sikkerhetstjenester

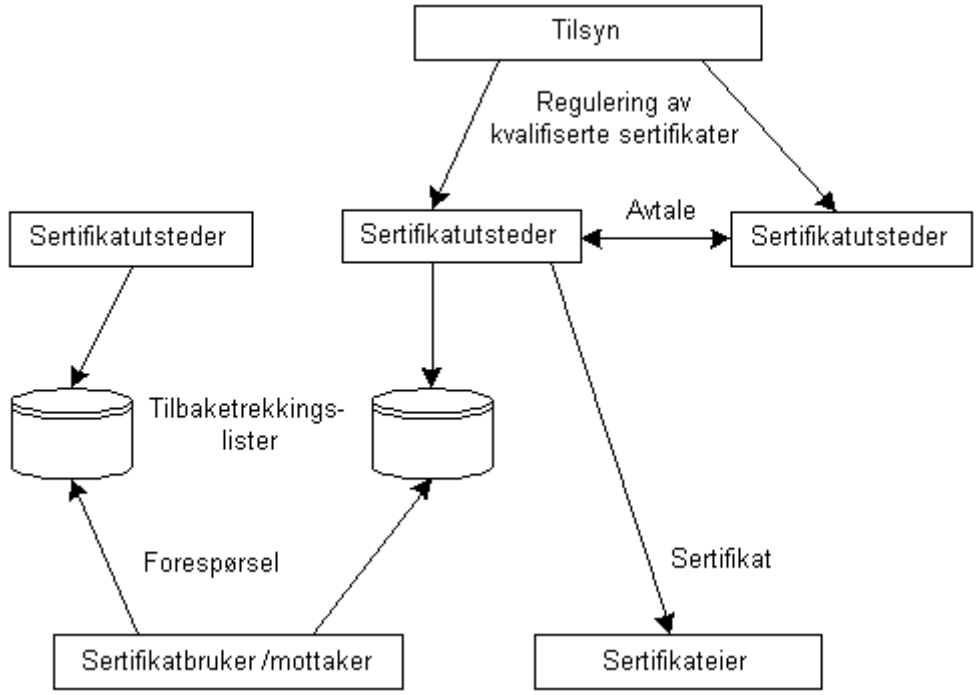
De tjenestene som er tilgjengelige i en PKI kan grupperes slik:

- Identifisering og registrering av sertifikateiere
- Utstedelse av sertifikater
- Generering av nøkkelpar
- Drift av sertifikatkataloger
- Tilbaketrekking av sertifikater og utstedelse av tilbaketrekkingslister
- Drift av en samtrafikktjeneste som kan sjekke sertifikater mot mange utstederes kataloger og deres tilbaketrekkingslister.

Tjenestene kan utføres av en aktør eller flere aktører i samarbeid.

Regulering av infrastrukturen

For at brukere av en PKI skal kunne være sikre på at den fungerer på en tilfredsstillende måte særlig når PKI-ens tjenester kjøpes i et marked er det nødvendig med tilsyn og hensiktsmessig regulering av slik virksomhet. Lov om elektronisk signatur regulerer utstedere av kvalifiserte sertifikater i Norge. Tilsynet skal påse at lovens bestemmelser mht. hvordan en utsteder av kvalifiserte sertifikater skal fungere følges. Regelverket forvaltes av Post- og teletilsynet og av Datatilsynet. I det norske markedet for PKI-er vil det trolig finnes utstedere av kvalifiserte sertifikater som loven omfatter og utstedere av andre sertifikater som ikke er definert i loven. Enkelte sertifikatutstedere vil kunne inngå avtaler om å stole på hverandres sertifikater (*krysssertifisering*) mens andre ikke vil gjøre det. Eksempel på markedet for PKI med regulatører vises i figur 3.7.



Figur 3.7 Markedet for PKI med tilsyn

Teknisk samvirke er et viktig spørsmål som må løses for å få en PKI til å fungere på hensiktsmessig måte. Teknisk samvirke innebærer at sertifikater fra ulike utstedere kan behandles uten problemer av programvare for signering og kryptering som leveres av ulike leverandører. Videre er tilgangen til ulike utstederes kataloger og tilbaketrekkingslister en del av det tekniske samvirket.

Men teknisk samvirke er ikke nok. Dersom den som mottar et digitalt signert dokument med sertifikat ikke har et kundeforhold til avsenderens sertifikatutsteder bør det finnes tjenester som muliggjør sjekking av sertifikatet på en brukervennlig måte. En løsning er kryssertifisering. Det består i at to eller flere sertifikatutstedere inngår gjensidige avtaler for å stadfeste at de kan innestå for sertifikater som den andre parten utsteder til sine kunder. Sertifikatutstedere utsteder gjensidige sertifikater for hverandres offentlige nøkler kryssertifikater. Kravet til innhold er noe forskjellig fra sertifikater utstedt til vanlige sertifikateiere. Problemstillingen er utdypet i kapittel 10 om samtrafikk.

3.4 Anvendelser som kan sikres med PKI

3.4.1 Bruk av nøkler og sertifikater

Digitale signaturer og PKI kan brukes i mange sammenhenger i den elektroniske samhandlingen i forvaltningen internt og med forvaltningens brukere. De vanligste bruksområdene vil være:

- E-post som skal signeres og krypteres
- E-post med vedlagte dokumenter som signeres og krypteres
- Web-baserte systemer der publikum skal identifisere seg overfor forvaltningens fagsystem og omvendt samt signere og kryptere utfylte Web-skjemaer
- Elektronisk innrapportering av data mellom systemer basert på EDI eller andre teknologier (f.eks. XML) der meldinger signeres og krypteres av avsender.

3.4.2 Utvikling av PKI-bruk

En PKI kan etableres innenfor en virksomhet for intern bruk. Den kan også etableres for et ekstranett dersom virksomheten f.eks. har et stort regionalt apparat eller til og med et internasjonalt apparat som flere store konserner har. Man kan også tenke seg en PKI for en sektor eller for hele forvaltningen. Hvordan dette kan realiseres er et av temaene for denne utredningen.

Etablering av en PKI i stor skala behøver ikke å skje ved at alle komponenter etableres overalt til samme tid. Det er mer sannsynlig at etablering og bruk av PKI vil vokse fram gradvis. PKI-er etablert for avgrensede formål vil på sikt kunne koples sammen til en større PKI og på denne måten betjene et større antall brukere som ønsker å kommunisere sammen. Enkelte forvaltningsinstitusjoner vil starte med å ha sin egen PKI. Noen institusjoner vil samarbeide seg imellom og ha en PKI som sørger for samhandling internt og med privatpersoner og bedrifter som faller inn under deres saksområder.

En del private bedrifter og grupper innen enkelte næringer etablerer for tiden egne PKI-er. En slik privat PKI vil utstede sertifikater til egne ansatte og kanskje til egne kunder og handelspartnere. Kundene og handelspartnerne vil på forhånd ha etablert et tillitsforhold til bedriften og vil derigjennom stole på sertifikatene fra bedriftens sertifikatutsteder. Kunder som har sertifikater fra andre sertifikatutstedere og starter samhandling med bedriften vil ikke automatisk ha samme tillitsforhold.

4 Anvendelsesområder for PKI i samhandling med og i forvaltningen

Dette kapitlet gir et kort overblikk over forvaltningens behov for sikker elektronisk kommunikasjon og informasjonsutveksling knyttet til arbeidet med effektivisering av interne oppgaver og til arbeidet med realisering av døgnåpen forvaltning med tilbud av elektroniske tjenester og elektronisk samhandling over nett.

4.1 Hva er behovene i forvaltningen?

Offentlig forvaltning er allerede i stor grad avhengig av elektronisk informasjonsutveksling. Denne utviklingen vil akselerere i tiden framover bl.a. som følge av politiske målsettinger om overgang til døgnåpen elektronisk forvaltning i løpet av 2003.

Behov for elektronisk utveksling av informasjon kan fordeles på to hovedgrupper: intern utveksling i forvaltningen og utveksling med forvaltningens brukere som følge av elektronisk tjenesteyting – både til enkeltpersoner og til næringslivet.

Innenfor forvaltningen vil viktige anvendelser med behov for sikker elektronisk informasjonsutveksling være:

- Elektronisk saksbehandling
- Elektronisk økonomiforvaltning
- Elektronisk offentlig innkjøp
- Elektronisk innrapportering mellom etater og forvaltningsnivåer (kommune–stat).

Mot *forvaltningens brukere* vil det hovedsakelig være anvendelser knyttet til

- Offentlige tjenester på Internett og
- Elektronisk innrapportering fra næringslivet

som vil ha behov for sikker elektronisk kommunikasjon.

PKI vil kunne brukes som sikkerhetsløsning på mange måter innenfor disse anvendelsesområdene:

- Som løsning for intern sikkerhet (tilgang til systemer autorisasjon av transaksjoner mv.)
- For meldingssikkerhet (sikker e-post)
- For dokumentsikkerhet (forsendelse via e-post eller på andre måter også sikker lagring)
- For sikker tilgang til forvaltningens tjenester (autentisering)
- For juridisk sikring av transaksjoner (signatur).

Anvendelsesområdene gjennomgås nedenfor for å konkretisere de ulike sikkerhetsbehovene som PKI vil kunne oppfylle.

4.2 Elektronisk saksbehandling

Elektronisk saksbehandling innebærer full overgang til papirløs behandling av saker i forvaltningen. Dette innebærer at dokumenter også må kunne utveksles elektronisk. I den forbindelse er det viktig å beskytte dokumentene mot utilsiktet endring mens de er underveis samtidig som mottakende virksomhet trenger pålitelig informasjon om dokumentets avsender/opphav. Dokumenter må kunne signeres der det eksisterer formkrav som krever underskrift.

4.3 Elektronisk økonomiforvaltning

Statens økonomireglement er et omfattende regelverk som stiller strenge krav til rutiner og framgangsmåter ved håndtering av betalingskrav tilskuddsforvaltning med mer. Elektronisk økonomiforvaltning vil innebære at fakturaer interne regninger og andre bilag vil kunne håndteres elektronisk både med hensyn til lagring og forsendelse. Reglementet stiller strenge krav til sikkerhet ved utbetalinger fra statskassen. Disse strenge kravene må også gjelde når rutinene for økonomiforvaltning blir gjennomført elektronisk.

Behovene her kan deles i to: behovet for sikring av utbetalinger og behovet for sikker håndtering av fakturaer/andre regnskapsbilag. Behovene i forbindelse med tilskuddsforvaltning ligger i skjæringspunktet mellom elektronisk saksbehandling og økonomiforvaltning og vil trolig dekkes av generelle løsninger for disse områdene.

I forbindelse med utbetalinger er det behov for å sikre seg mot endring av innholdet i et betalingsoppdrag. Videre er det behov for sikker autentisering av oppdraget dvs. hvor det kommer fra og hvem som har autorisert utbetalingen. Det kan være behov for flere slike autorisasjoner i forbindelse med et utbetalingsoppdrag.

Sikker håndtering av fakturaer og interne regninger innebærer at attestasjoner og anvisninger løses på en betryggende måte. Dette kan gjøres ved hjelp av elektroniske signaturer eller på andre måter men det er behov for sikre «spor» etter disse handlingene. Som følge av regnskapslovgivningen med forskrifter er det behov for å kunne verifisere slike spor aktivt i om lag 3 5 år. Etter dette overføres dokumentene til et (elektronisk) fjernlager der de skal oppbevares i ytterligere 6 5 år av hensyn til muligheter for revisjon.

Det er i den forbindelse viktig at økonomisystemer som er godkjent for bruk i staten støtter den type sikkerhetsløsning som blir valgt for sikring av spor i fakturahåndteringen. Løsningene må derfor være standardiserte nok samtidig som de er sikre nok.

4.4 Elektronisk offentlig innkjøp

Effektivisering av offentlig innkjøpsvirksomhet kan gi svært store besparelser for offentlig sektor. Besparelsene kan komme som følge av lavere priser som kan oppnås ved bedre samordning av innkjøpene innenfor etatene og på tvers av etatene. Den største innsparingen vil kunne oppnås ved å effektivisere selve innkjøpsprosessen. Elektroniske innkjøpsprosesser kan implementeres på flere ulike måter. En måte er å etablere en elektronisk markedsplass for offentlige innkjøpere der man får tilgang til relevant leverandør- og produktinformasjon og mulighet for bestilling av varer og tjenester. Et slikt konsept fordrer at det er inngått rammeavtaler med leverandørene i forkant. Kommunikasjon mot slik offentlig elektronisk markedsplass vil kreve autentisering av brukere dersom de skal foreta bestillinger eller legge inn ny informasjon til markedsplassen selv. Videre er det behov for autentisering av leverandørenes informasjon slik at brukere vet at de forholder seg til riktige opplysninger. (Dette er aktuelt dersom slik informasjon er desentralisert til leverandørenes servere.) Dersom formkravene i regelverket tilsier det kan det bli behov for elektronisk signatur eller andre former for sporing av bestillinger.

Dersom hele innkjøpsprosessen skal være elektronisk må det implementeres sikker kommunikasjon mellom leverandør og offentlig bruker for oversendelse av ordrebekreftelse faktura og betaling. Dette krever at den offentlige etaten selv har et elektronisk innkjøpssystem.

Elektronisk innkjøp der et innkjøpssystem hos en offentlig etat samhandler elektronisk direkte med leverandørenes systemer krever mer avanserte løsninger når det gjelder sikring av kommunikasjon. Autentisering på ulike nivåer og integritetsbeskyttelse av transaksjoner vil være sentrale. Løsningene må kunne samspille med næringslivets sikkerhetsløsninger for e-handel.

4.5 Elektronisk innrapportering mellom etater og forvaltningsnivåer (kommune-stat)

Som følge av bl.a. samordningen av oppgaver f.eks. Enhetsregisteret er det oppstått behov for utstrakt utveksling av elektronisk informasjon mellom offentlige etater. Denne utvekslingen må kunne sikres på en hensiktsmessig måte. Innrapportering til registre bør være autentisert og sikret mot utilsiktet endring. Dersom det er sensitive data som innrapporteres må det finnes løsninger som beskytter slike data mot uønsket innsyn.

Kommunene er pålagt omfattende rapporteringsplikt til statlig nivå. Tjenesteproduksjonsdata og ulike typer statistikker skal innrapporteres jevnlig til ulike mottakere bl.a. Statistisk sentralbyrå. Elektronisk innrapportering er en svært effektiv måte å løse dette på. Elektronisk innrapportering av slike data krever at kommunikasjon er sikret mot innsyn ettersom det ofte er sensitiv informasjon som overføres. Kommunikasjonen bør også være sikret mot utilsiktet endring.

4.6 Offentlige tjenester på Internett

Elektroniske tjenester til forvaltningens brukere vil spenne over et bredt spekter fra henvendelser pr. e-post via generell saksbehandling innsending av søknader meldinger (f.eks. flyttemeldinger) utveksling av informasjon til innberetninger og innbetalinger av avgifter m.m.

Elektroniske tjenester til enkeltpersoner kan differensieres etter graden av interaksjon og juridisk binding. En mulig inndeling er som følger:

- Web-tjenester som inneholder informasjon om etaten og dens tjenester. Kommunikasjon kun via e-post (trinn 1)
- Tjenester med interaktive funksjoner for eksempel bestillinger beregningsmuligheter søk i databaser. Interaktiv kommunikasjon direkte til saksbehandler eller fagansvarlig (trinn 2)
- Web-tjeneste som tilbyr brukeren å legge inn og hente informasjon tilrettelagt ut fra personlige kriterier. Tjenesten er knyttet til interne produksjonssystemer (trinn 3)
- Web-tjeneste med funksjonalitet for online samarbeid med andre myndigheter og samfunnsaktører (trinn 4).

Tjenester på trinn 1 krever ingen spesiell sikring av kommunikasjon utenom behovet for autentisering av den serveren informasjonen befinner seg på slik at «hackere» ikke kan sette opp vevtjenester som utgir seg for å være offentlige informasjonstjenester med påfølgende fare for feilinformasjon til enkeltpersoner.

Tjenester på trinn 2 innebærer at det kan være behov for autentisering integritetssikring av ev. beskyttelse mot innsyn i den direkte kommunikasjonen mot saksbehandler/fagansvarlig. Slik kommunikasjon vil mest sannsynlig foregå via e-post. Man trenger sikker e-post for å støtte opp om slike tjenester. Også her er behovet beskrevet for trinn 1 aktuelt.

Tjenester på trinn 3 vil i tillegg til behov beskrevet for trinn 1 og 2 kreve sterk autentisering av brukeren samt beskyttelse mot innsyn i de tilfellene der informasjonen som hentes/legges inn er sensitiv. Videre kan det oppstå behov for elektronisk signatur i de tilfellene der formkrav i regelverket krever underskrift på opplysninger som leveres.

Tjenester på trinn 4 vil i tillegg til kravene beskrevet for trinnene 1–3 kreve at det implementeres en sikker kommunikasjon mot flere servere samtidig. Autentisering av brukeren bør kunne foregå ett sted men slik at brukeren samtidig blir autentisert mot flere tjenester («single sign-on»).

4.7 Elektronisk innrapportering fra næringslivet

Elektronisk innrapportering fra næringslivet har allerede vært implementert i en del år ved hjelp av lukkede løsninger. Overgang til innrapportering på Internett krever sikring av informasjonen mot utilsiktet endring og mot uønsket innsyn. Videre vil det kreves sterk autentisering av innsenderen og trolig også elektronisk signatur av hensyn til ikke-benektingsbehovet hos myndighetene. Innsenderen vil ha behov for å autentisere den offentlige serveren som informasjonen sendes til og å motta en tidsstemplet kvittering for mottak av informasjonen av hensyn til krav i lovgivningen som pålegger rapporteringsplikt med gitte frister.

Elektronisk innrapportering fra næringslivet vil spesifikt ha den utfordringen at løsninger for sikring av innrapporteringer til ulike myndigheter bør være samordnet for ikke å legge for store byrder på næringslivet med hensyn til teknisk utstyr programvare og opplæringsbehov.

4.8 Prosjekter der bruk av PKI inngår

Nedenfor nevnes et knippe tiltak/prosjekter i forvaltningen der bruk av digital signatur inngår eller er planlagt. Listen er ikke uttømmende og er ment som en illustrasjon for at det pågår utviklingsarbeid på området mange steder i forvaltningen.

Brønnøysundregistrene planlegger å tilby nettbasert direkte registrering i Enhetsregisteret og Foretaksregisteret i løpet av 2001. Digitalt signerte elektroniske registreringsskjemaer vil kunne leveres over nett til registrene.

Patentstyret (Styret for det industrielle rettsvern) utvikler innenfor sitt SANT-prosjekt elektroniske løsninger for patentsøknader over nett. Prosjektet omfatter et nytt elektronisk saksbehandlingssystem som gjør det mulig for brukere å sende inn elektroniske digitalt signerte søknader og å kommunisere elektronisk om sin sak med Patentstyret. Løsningen skal være tilgjengelig i 2. kvartal 2002.

Rikstrygdeverket har benyttet en PKI-løsning ved beregning av økonomiske oppgjør til legene siden 1996 og i forbindelse med oppgjør fra sykehusenes poliklinikker siden 1998. Sistnevnte er innført i stor skala fra februar 2000. Dette er oppgjør basert på digitale signaturer både smartkort- og softwarebaserte løsninger kryptering og TTP-tjenester. Det planlegges/er i pilotdrift nettbaserte løsninger for arbeidsgivere (innrapportering til arbeidsgiver/arbeidstaker-registeret) for helsesektoren (elektroniske sykmeldinger) og for publikum valg av fast lege innsending av søknadsblanketter og selvbetjening (f.eks. E-111 pensjonsberegning m.m.).

Utlendingsdirektoratet planlegger en tjeneste der en søker selv kan sjekke status for egen sak (saker etter statsborgerrettsloven og utlendingsloven).

Sosial- og helsedepartementet arbeider med utvikling av nasjonalt helsenett og elektronisk samhandling i helse- og sosialsektoren. I denne sammenhengen må det utvikles policyer for TTP-tjenester og bruk av elektroniske signaturer. I SESAM-prosjektet som finansieres i samarbeid mellom SHD og AAD og som drives av KITH (Kompetansesenter for IT i helsesektoren) gjennomføres det utprøving av sikker e-post mellom Aker sykehus og Bjerke bydel i Oslo. Det utveksles digitalt signerte og krypterte dokumenter knyttet til overføring av pasienter fra sykehus til bydel. I et annet delprosjekt av SESAM benyttes PKI til sikker e-post for å sende data fra fødestuer til Medisinsk Fødselsregister i Bergen. Løsningen er prøvd ut ved tre fødestuer ved årsskiftet 2000/2001 og det planlegges videre utprøving. I Midt-Norsk Helsenett (MNH) planlegges det bruk av PKI for sikring av elektroniske EDI-baserte meldinger om laboratoriesvar bestilling av prøver bestilling av røntgen mv. De første meldingene (epikrise) er i gang og flere vil komme i gang i løpet av første halvår 2001.

Etter initiativ fra *Miljøverndepartementet* og*Kommunal- og regionaldepartementet* har Statens kartverk og Statens bygningstekniske etat i samarbeid med bygge- og anleggsbransjen og kommunene satt i gang et prosjekt for elektronisk plan- og byggesaksbehandling. Dette er kalt «Prosjekt Byggsøk». Prosjektet har som målsetting å utvikle et system for elektronisk plan- og byggesøknad med forenklet behandling og dermed kortere behandlingstid. Innen tre år skal hele byggesaken kunne gjennomføres online:

- Søker skal kunne hente all nødvendig informasjon for å lage en komplett søknad på Internett
- Søknader skal kunne lages sendes og gebyrer betales elektronisk
- Søker skal kunne følge utviklingen av saken via Internett
- Tillatelser skal kunne mottas elektronisk.

Direktoratet for arbeidstilsynet skal gjøre alle sine skjemaer nedlastbare over Internett og gi mulighet til å fylle ut på skjerm. Mangel på løsninger rundt elektroniske signaturer og elektronisk mottak betyr imidlertid at skjemaer som skal returneres etaten inntil videre må skrives ut signeres for hånd og sendes pr. ordinær post. En rekke skjemaer er tilgjengelige nå. Byggemelding etter § 19 – dokumentasjonsplan for HMS er under utarbeidelse i samarbeid med Byggteknisk etat. Det foregår også et prøveprosjekt ved Arbeidstilsynets distriktskontor i Telemark der man tester ut full elektronisk rapportering over Internett. Prosjektet har løpt siden høsten 2000.

Statens lånekassefor utdanning har satt i gang et forsøksprosjekt om elektronisk søknadsbehandling (søknad om studielån) på Internett. Prosjektet innebærer også forsøk med digitale signaturer basert på bruk av smartkort. Prosjektets overordnete mål er å effektivisere Lånekassens interne arbeid og tilby bedre tilgjengelighet for kundene.

Kystverket arbeider med innføring av elektronisk saksbehandling ved å innføre et elektronisk dokumentstyringssystem. Videre ønsker man å innarbeide elektronisk signatur for intern og ekstern saksbehandling. Det er essensielt for etaten at arbeidet samkjøres med andre etater for å legge bedre til rette for implementasjon.

Skattedirektoratet arbeider med flere prosjekter og løsninger for elektronisk innrapportering fra næringslivet og fra enkeltpersoner. For levering av merverdiavgiftsoppgaven over Internett ble det fra 1.5.2000 satt i gang en prøveordning for avgiftspliktige i Akershus. Fra 1.1.2001 er denne ordningen utvidet til også å omfatte Buskerud og den skal gjøres landsdekkende fra 1.3.2001. Det benyttes digitale signaturer basert på smartkort.

Elektronisk innlevering av selvangivelse med tilleggsskjema blir gjort tilgjengelig som en prøveordning med en EDI-løsning med digitale signaturer våren 2001 for næringsdrivende i Asker Skedsmo Askøy Os og Bodø. I tillegg til å være en løsning for skatteetatens skjema er det et samarbeid med Statistisk sentralbyrå og Brønnøysundregistrene som skal gi de næringsdrivende en enhetlig løsning for rapportering til de tre etatene (SLN-prosjektet).

Etaten planlegger å tilby løsninger for PKI-sikret elektronisk innlevering av selvangivelse over Internett i 2001. Det skal også tilbys tjenester for bestilling av ny selvangivelse og bestilling av skattekort over Internett.

Statistisk sentralbyrå har drevet prosjektet KOSTRA (Kommune-Stat – Rapportering) i samarbeid med Kommunenes Sentralforbund og Kommunal- og regionaldepartementet siden 1997. Fra februar 2002 skal løsningen gå over i en driftsfase. Hver kommune rapporterer sine tjenesteproduksjonsdata elektronisk til SSB. Rapporteringen er konfidensialitetssikret med en PKI-løsning.

Vegdirektoratet gjennomfører et internt prosjekt under navnet EBASUS. Prosjektet omhandler elektronisk fakturahåndtering og -betaling. Digital signatur skal brukes ved anvisning av faktura. Etaten planlegger utvikling og testing av en pilotløsning for vegkontorene i hele Østfold fylke i løpet av 2001.

I januar 2002 planlegger Vegdirektoratet å ha tilgjengelig en tjeneste for registrering av bil og utstedelse av vognkort. Tjenesten vil i første omgang bli tilgjengelig for bilimportørene og bilforhandlerne. Den vil kreve digital signatur fra den som registrerer.

I vedlegg 1 er det beskrevet noen konkrete prosjekter som er gjennomført eller gjennomføres og planer for implementering av ulike former for sikker elektronisk informasjonsutveksling med og i forvaltningen. I disse beskrivelsene er behovene for sikring av kommunikasjonen forsøkt konkretisert i forhold til hver enkelt anvendelse som beskrives.

5 Bakgrunn og rammebetingelser

I dette kapitlet omtales ulike føringer fra inn- og utland. Det er naturlig å starte med EU og OECD dels fordi de har vært tidlig ute dels fordi de har lagt premisser for norske arbeider knyttet til digitale signaturer mv. De norske arbeidene utgjør dels politiske utgangspunkter fra regjeringen med målformuleringer som forutsetter bruk av teknologi for sikker autentisering mv. Dels omtales utredninger som mer konkret har forsøkt å finne ut hvordan man i praksis kan gjøre dette med forslag til tiltak for å nå de politiske målsettingene. I tillegg presenteres den nye loven om elektronisk signatur og den nye personopplysningsloven som begge gir rettslige rammebetingelser for noen av de spørsmålene denne utredningen tar opp. Det er skrevet et eget underkapittel om personvernspørsmål knyttet til digitale signaturer mv. Til slutt gis det en kort oversikt over noen viktige leverandører og brukere på det private markedet som også har betydning for de forslagene vi fremmer for forvaltningen og for kommunikasjon med forvaltningen.

5.1 Utgangspunkter i EU og OECD

Både EU og OECD har engasjert seg i spørsmålet om autentisering og sikkerhet ved Internett-baserte transaksjoner men med ulik tilnærming. Mens det i EU er blitt fremmet regulatoriske tiltak arbeider OECD først og fremst med å dokumentere og sammenlikne ulike tilnærminger til elektronisk signatur-anvendelse i ulike land. OECD har imidlertid også initiert arbeid med sikte på å legge fram retningslinjer for bruk av autentiseringsteknologier herunder elektroniske signaturer for å fremme global elektronisk handel og globalt elektronisk samkvem mellom nasjoner. OECD har også utarbeidet retningslinjer for kryptopolitikk publisert i mars 1997 som gir en generell ramme for bruk av kryptoteknologier.

5.1.1 EU

I 1997 fremmet Europakommisjonen en meddelelse til Ministerrådet som omhandlet autentisering av elektroniske transaksjoner og bruk av elektroniske signaturer og krypteringsteknologi. På grunnlag av Rådets behandling av denne meddelelsen ble det utarbeidet et forslag til direktiv. Det ble lagt fram den 13. mai 1998 og endelig vedtatt den 13. desember 1999.

Andre relevante EU-tiltak er eEurope-handlingsplanen og det flerårige IDA-programmet (Interchange of Data between Administrations).

EU-direktiv om rammeverk for elektroniske signaturer

Direktiv-forslaget ble fremmet med utgangspunkt i EF-traktatens artikkel 47(2) 55 og 95. Forslaget hadde dobbel målsetting. På den ene siden ønsket man å fremme utviklingen av et europeisk indre marked for elektroniske signatur-produkter og -tjenester. På den andre siden ønsket man å legge til rette for rettslig aksept av elektroniske signaturer på tvers av de ulike landenes legale systemer og ulike prinsipper for bevisføring.

Direktivet omhandler krav til og tilsyn med tilbydere av sertifikattjenester og særlig tilbydere av såkalte kvalifiserte sertifikater. Konseptet kvalifisert sertifikat er tett knyttet til direktivets artikkel om rettslig likestilling av en håndskreven og en elektronisk signatur.

I direktivet er det gitt adgang for medlemslandenes forvaltninger til å stille tilleggskrav til elektroniske signaturer som ønskes brukt i forvaltningen.

Nærings- og handelsdepartementet la fram Ot.prp. nr. 82 (1999–2000) om lov om elektronisk signatur for Stortinget i oktober 2000. Loven ble vedtatt i desember 2000 og skal etter planen tre i kraft 1.7.2001 sammen med ny forskrift. Loven peker ut en tilsynsmyndighet for tilbydere av kvalifiserte sertifikater. Det er Post- og teletilsynet som skal ivareta denne oppgaven. Loven er omtalt nedenfor.

Selv om direktivet er ment som en teknologinøytral regulering så omhandler det i hovedsak digitale signaturer. Direktivet krever imidlertid at elektroniske signaturer ikke nektes bevisverdi bare på det grunnlaget at de er elektroniske. Dette er en stadfesting av det norske prinsippet om fri bevisføring og fri bevisvurdering.

Direktivet slår ellers fast at det ikke er adgang for myndigheter til å forhåndsgodkjenne tilbydere av sertifikattjenester. Men det kan etableres frivillige godkjenningsordninger.

Videre krever direktivet at det utpekes nasjonale organer som skal godkjenne såkalte sikre signaturframstillingssystemer. Godkjenning gitt av ett medlemsland skal respekteres i de andre landene.

EESSI – European Electronic Signature Standardization Initiative

Europakommisjonen satte i gang EESSI-arbeidet i forbindelse med vedtakelsen av det europeiske direktivet om rammeverk for elektroniske signaturer (1999/93/EC) i desember 1999.

Initiativet er finansiert av Kommisjonen og gjennomføres som et fellestiltak i samarbeid mellom to europeiske standardiseringsorganisasjoner – ETSI (European Telecommunication Standards Institute) og CEN (det europeiske standardiseringsorganet). EESSI styres av en egen styringsgruppe bestående av representanter for industrien og brukere. EESSI rapporterer jevnlig framdriften i arbeidet sitt til EU-komiteen som er etablert i medhold av direktivets artikkel 9.

Formålet med EESSI er å utvikle europeiske standarder som skal kunne støtte gjennomføringen av direktivet. Standardene er ment som en konkretisering av direktivets fire vedlegg med hhv. krav til kvalifiserte sertifikater krav til utstedere av kvalifiserte sertifikater krav til sikre signaturframstillingssystemer og anbefalinger for sikker signaturverifisering.

De to organisasjonene utarbeider standardene med tanke på å få dem på plass innen sommeren 2001 som er fristen for implementering av direktivet i medlemslandene.

EESSI har utviklet eller skal fullføre utviklingen av følgende standarder:

- Standard sertifikatpolicy(er) for utstedere av kvalifiserte sertifikater (ETSI standard TS 101 456) [23]
- Standardkrav for sikre systemer for utstedelse av sertifikater (CEN/ISSS-utkast forventes godkjent 1. kv. 2001)
- Standard profil for kvalifiserte sertifikater basert på Internett-standarden RFC 2459 (ETSI standard TS 101 862) [24]
- Standardkrav for sikre signaturframstillingssystemer (CEN/ISSS-utkast forventes godkjent 1. kv. 2001)
- Standard for elektronisk signatur – format (ETSI TS 101 733)
- Standardkrav til signaturframstillingsprosess og -miljø (CEN/ISSS-utkast forventes godkjent 1. kv. 2001)
- Standardkrav til signaturverifiseringsprosess og -miljø (CEN/ISSS-utkast forventes godkjent 1. kv. 2001)
- Standard profil for tidsstempling (ETSI TS 101 861)
- Veiledning for testing av samsvar med EESSI-standarder (CEN/ISSS-utkast forventes godkjent 1. kv. 2001).

Av dette utvalget av standarder er det kun Standardkrav for sikre signaturframstillingssystemer som er faktisk forankret i direktivets artikkel 3.5 (og vedlegg 3). De øvrige standardene vil ha en veiledende funksjon i forhold til praktisk tolkning av direktivets vedlegg 1 2 og 4.

Det synes å foreligge en uenighet mellom enkelte av medlemslandene når det gjelder hvordan direktivets artikler 3.4 og 3.5 skal tolkes med hensyn til å stille bindende krav til sikre signaturframstillingssystemer. Enkelte land tolker disse artiklene slik at en nasjonal myndighet som er oppnevnt i samsvar med minimumskriterier for utpeking av slike organer publisert i en beslutning fra Kommisjonen nr. 2000/709/EC av 6.11.2000 kan godkjenne et slikt system etter de standarder som de mener er relevante eller at Europakommisjonen kan publisere relevante standarder i EU-Tidende og på den

måten fastlegge hva som skal legges til grunn for godkjenning av slike systemer. Dette er to alternative måter å godkjenne sikre signaturframstillingssystemer på. Det er viktig å bemerke at direktivet legger opp til at en godkjenning av et sikkert signaturframstillingssystem i ett av medlemslandene automatisk skal gjelde i alle andre medlemsland.

Andre land tolker disse to bestemmelsene slik at Europakommisjonen skal utpeke relevante standarder og at de nasjonale myndigheter deretter skal godkjenne sikre signaturframstillingssystemer på grunnlag av disse standardene.

Denne tolkningen åpner ikke for noen alternativ måte å godkjenne slike systemer på.

Videre utvikling i EUs implementeringsarbeid på dette området vil trolig ha stor betydning for hvordan nasjonale tilsynsmyndigheter vil utforme og håndheve det praktiske regelverket som skal understøtte lovgivningen vedrørende elektroniske signaturer.

I Norge arbeider Nærings- og handelsdepartementet i samarbeid med Post- og teletilsynet med utforming av forskrifter til lov om elektronisk signatur. Dette forskriftsverket er ikke ferdig i skrivende stund (januar 2001) men antas å bli påvirket av resultater av EESSI-arbeidet og deres videre behandling i EU.

Sikre signaturframstillingssystemer kreves for å kunne lage «kvalifiserte signaturer» dvs. signaturer som automatisk oppfyller kravene om underskrift i lovene som åpner for elektronisk kommunikasjon. For alle andre elektroniske signaturer er slike systemer ikke et krav.

eEurope

Europakommisjonen la i desember 1999 fram meddelelsen *eEurope – informasjonssamfunnet for alle*. Meddelelsen beskrev et initiativ som hadde som mål å framskynde utviklingen og anvendelsen av digitale teknologier i Europa samt å sikre nødvendig kompetanse for dette. EU-toppmøtet i mars 2000 vedtok å fremme en handlingsplan for utvikling av en digital kunnskapsbasert økonomi som skal bidra til vekst styrke konkurranseevnen og skape nye arbeidsplasser i Europa. eEurope-planen ble lagt fram i juni 2000. Nærings- og handelsminister Grete Knudsen la fram den norske «motparten» til eEurope – eNorge-planen – i slutten av juni samme år.

eEurope-planen omhandler 3 hovedområder for utvikling av e-økonomi i Europa. Innenfor område 1 har man definert tiltak for sikre nettverk og smartkort. Under dette tiltaket er det lagt opp til omfattende arbeid med «trailblazers» (fyrtårn-prosjekter) som skal legge til rette for sikker bruk av elektroniske nettverk ved hjelp av bl.a. PKI-teknologi og bruk av smartkort. I september 2000 ble prosjektet «Offentlig elektronisk ID» foreslått av Finland og Nederland som område 2. Prosjektet har som mål å lage en spesifikasjon og etablere pilotprosjekter for utprøving av et digitalt «identifikasjonsdokument» som skal kunne nyttes på tvers av grensene innen det europeiske fellesskapet. En slik felles elektronisk identitet skal basere seg på bruk av PKI og smartkort som lagringsmedium.

IDA-programmet

Det flerårige IDA-programmet (Interchange of Data between Administrations) har eksistert siden 1994. Programmet har som mål å legge til rette for effektiv elektronisk informasjonsutveksling mellom medlemslandenes forvaltninger og EU-organer. Programmet har gjennomført en rekke prosjekter fra utprøving av sektororienterte informasjonsnettverk til utvikling og implementering av felles infrastrukturer for informasjonsutveksling over landegrensene. PKI er blitt tatt i bruk i IDA i ett sektornettverk – på legemiddelkontrollområdet. Det sentrale EU-legemiddelkontoret i London nasjonale legemiddelkontrollmyndigheter samt farmasøytisk industri kan få adgang til en «sikker server» med dokumenter ved å bruke PKI-løsninger fra selskapet GlobalSign. Videre er det i tilknytning til det såkalte TESTA-prosjektet som skal utvikle et EU-stamnett for informasjonsutveksling tatt initiativ til etablering av en interoperabel PKI mellom landenes forvaltninger. Det legges opp til bruk av PKI for sikker utveksling av e-post mellom de europeiske organene og de nasjonale forvaltningene. Dette vil kreve sentrale løsninger for å få til samvirke (interoperabilitet) mellom de nasjonale PKI-løsningene. Arbeidet med dette ble startet tidlig i november 2000.

5.1.2 OECD

I OECD-landene ansees bruk av kryptering som viktig i elektronisk kommunikasjon. Først og fremst anser man at det i en situasjon med utstrakt kommunikasjon over åpne nett (Internett) er viktig å kunne identifisere seg overfor en annen part. Derfor er det lagt stor vekt på å belyse og få fram ulike lands tilnærminger når det gjelder politikk for elektronisk identifikasjon dvs. å kunne autentisere seg og kartlegge den rettslige situasjonen på området. På et tidligere tidspunkt da spørsmålet om bruk av kryptering til ulike formål var mer uklart og man ikke skilte klart mellom kryptering for å skjerme innhold for innsyn fra uvedkommende (konfidensialitet) fra kryptering til bruk for identifikasjon og for å sikre at informasjonen ikke endres underveis (autentisitet/integritet) trakk OECD opp retningslinjer for bruk av kryptering i OECD-landene. Disse retningslinjene har Norge sluttet seg til. De er omtalt nedenfor.

OECD Inventory of Approaches to Authentication (identifikasjon/autentisering)

En statusrapport over tilnærminger til bruk av autentiseringsteknologier er utarbeidet på grunnlag av innspill fra medlemslandene og ventes å foreligge våren 2001. Den skal danne grunnlag for en OECD-ministerrapport i 2001 vedrørende status for implementering av deklarasjonen vedrørende autentisering fra Ottawakonferansen i 1998.

OECD Inventory of Impediments to Electronic Communication (rettslige hindringer)

OECD besluttet i juni 1999 å gjennomføre en begrenset undersøkelse av medlemslandenes lovgivning med tanke på hvordan elektronisk kommunikasjon er behandlet og særlig spørsmålet om juridisk gyldighet av elektroniske signaturer samt eventuelle hindringer for slik gyldighet. Utkast til rapport ventes i januar 2001. Det legges vekt på å få oversikt over avtalerett forvaltningsrett transportområdet og finansielle tjenester.

På grunnlag av rapporten vil det bli vurdert om det er hensiktsmessig at OECD utarbeider og publiserer retningslinjer for bruk av elektroniske signaturer. Det har eksistert en intern uenighet i OECD om mulige retningslinjer. Den forventede kartleggingsrapporten kan bidra til at retningslinjearbeidet gjenopptas.

OECD's retningslinjer for kryptopolitikk

I mars 1997 vedtok OECD anbefalinger til medlemslandene om retningslinjer for «kryptopolitikk» [4]som også er tilgjengelig i en norsk oversettelse fra Nærings- og handelsdepartementet (både i hefteform og på nettsiden deres).

I retningslinjene anbefales medlemslandene å unngå umotiverte hindringer for bruk av krypteringsteknologi fordi slike hindringer kan ha negativ effekt på framveksten av internasjonal handel og kommunikasjonsnettverk.

Retningslinjene legger til grunn at brukerne fritt skal kunne velge mellom ulike krypteringsteknologier og at teknologier og standarder skal være styrt av markedets behov. Videre skal individets rett til å kommunisere uten andres uautoriserte innsyn respekteres og lovhjemlet adgang til kryptert kommunikasjon må respektere disse prinsippene. Dette innebærer bl.a. at man må skille mellom krypteringsteknologi benyttet for innholdskryptering og denne teknologien brukt i forbindelse med signering og integritetssikring av meldinger. I retningslinjene understrekes videre behovet for klarlegging av tjenestetilbydernes ansvar for tjenestene og brukernes ansvar for misbruk av krypteringsnøkler. Avslutningsvis påpekes behovet for internasjonalt samarbeid for å unngå hindringer for internasjonal handel.

4

Recommendation of the Council concerning Guidelines for Cryptography Policy 27 March 1997.

Retningslinjenes mål er å fremme bruk av krypto skape tillit til infrastrukturer nettverk og systemer og bruken av disse nasjonalt og globalt. Dette er både av hensyn til offentlig og privat sektor internasjonal handel og for den enkelte borger. Samtidig vektlegges det sterkt at denne utviklingen ikke må komme i konflikt med nasjonale hensyn knyttet til politi- og påtalemyndighetenes kriminalitetsbekjempelse eller rikets sikkerhet. Gjennom retningslinjene har de 29 medlemslandene i OECD understreket betydningen av at man på global basis har felles normer for bruk av krypto.

Sammen med retningslinjene og i samme dokument har OECD lagt fram en rapport om bakgrunnen for kryptopolitikk der en rekke problemstillinger knyttet til slik politikk gjennomgås. Denne rapporten er ikke ment som forarbeid til retningslinjene på en slik måte at den kan legges til grunn ved tolkning av disse.

Innholdskryptering vil ikke bare hindre uvedkommende innsyn i en kommunikasjon men også vanskeliggjøre eller umuliggjøre etterforskning og avlytting i regi av politi og myndigheter. Dette griper inn i forhold som også kan ha med nasjonal sikkerhet å gjøre. De fleste land har ført en streng eksportkontroll med teknologi som kan benyttes til kryptering. I mange dataprogrammer som selges fra USA har kryptofunksjonalitet blitt fjernet eller sterkt redusert. Andre land har også ført en til dels streng regulering med nasjonal bruk av krypteringsteknologi. Konfidensialitet er derfor et område der det har vært langt vanskeligere å komme fram til internasjonale løsninger enn for elektroniske/digitale signaturer og rene autentiseringstjenester.

Flere OECD-land har endret sin politikk etter å ha deltatt aktivt i det konsensusorienterte arbeidet med utarbeidelsen av retningslinjene. F.eks. har USA de siste årene gradvis lettet betydelig på sine eksportrestriksjoner antakelig av hensyn til sin egen krypto- og dataindustris konkurransemuligheter på et globalt marked. Fokus går nå i retning av at sivil sektor blir storbruker av ulike typer kryptoløsninger både forvaltninger og ikke minst handels- og næringslivet. Tiden da krypto «bare» ble sett på som våpen eller kun forbeholdt militære og diplomatiske hemmeligheter er forbi. Nå er parolen at man i tillegg og i sterkt økende grad trenger «krypto til folket» og til sivil og offentlig sektor utenfor anvendelser som knytter seg til rikets sikkerhet.

5.2 Utgangspunkter i Norge

5.2.1 eNorge 2.0

Nærings- og handelsdepartementet har i samarbeid med fjorten andre departementer laget en handlingsplan som kalles *eNorge*. eNorge har som mål å utvikle et informasjonssamfunn for alle. Dette er en operativ plan som beskriver løpende status hva som må gjøres hvem som har ansvaret og når tiltakene skal gjennomføres. Planen rulleres hver 6. måned. Den første utgaven kom 29. juni 2000 og versjon 2.0 ble presentert av nærings- og handelsministeren 11. desember 2000.

Regjeringen vil med dette bidra til at alle får tilgang til den nye teknologien øke befolkningens kompetanse samt gjennomføre tiltak som øker tilliten. Det er et mål at IKT (informasjons- og kommunikasjonsteknologi) skal være sikker og tilgjengelig for alle – uavhengig av kompetansenivå.

Noen hovedutfordringer i denne forbindelse nevnes innledningsvis i planen:

Fjerning av hindre for elektronisk kommunikasjon – Regjeringens mål er at elektronisk kommunikasjon skal bli like akseptert og få samme juridiske holdbarhet som skriftlig kommunikasjon. Utvalget legger til grunn at man med uttrykket «skriftlig» tenker på det som er papirbasert. At dette er et uttrykk som i økende grad brukes om elektronisk basert skriftlighet også er et annet tema. Det vises videre under dette punktet til arbeidet med å identifisere og fjerne hindringer i regelverket for elektronisk kommunikasjon jf. omtalen nedenfor om eRegel-prosjektet (tidligere kalt Kartleggingsprosjektet). Det understrekes at målet er en felles proposisjon for Stortinget som kan fremmes innen 1. august 2001.

Sårbarhet knyttet til IKT identifiseres som et innsatsområde der den videre utbredelsen av IKT i Norge ansees avhengig av tillit til systemene.

Regjeringens handlingsplan for bredbåndskommunikasjon ble lagt fram 11. oktober 2000. Målet er å bidra til en rask og bred utbygging av bredbåndsnett i regi av markedsaktørene med dekning av hele landet. Offentlig etterspørsel skal stimuleres for å kunne bidra til nye investeringer fra markedsaktørene som i sin tur kan bidra til å fornye offentlig sektor.

Ett viktig tiltak i Regjeringens fornyelsesprogram er en døgnåpen forvaltning og en effektivisering av forvaltningen ved hjelp av IKT. Dette skal bl.a. oppnås ved at forvaltningen skal bli lettere tilgjengelig for befolkningen ved selvbetjeningsløsninger over Internett slik at brukerne kan få utført tjenestene på en rask og sikker måte når de selv har behov for dem. Alle statlige etater skal utarbeide strategier og konkrete tiltak innen mai 2001 for å nå målet om en døgnåpen og brukerorientert forvaltning slik at elektroniske tjenester og elektronisk saksbehandling blir et hovedtilbud til brukerne innen ultimo 2003.

eNorge-planen skal sikre at Norge har minst like ambisiøse mål som det EU har formulert i eEurope-planen omtalt ovenfor. Målet er å følge opp alle initiativ som settes i gang på bakgrunn av eEurope. De viktigste mål og tiltak i eEurope 2002 – Action Plan er følgelig dekket i eNorge-planen som i tillegg inneholder tiltak med utgangspunkt i spesielle norske utfordringer.

Planen er delt inn etter fem hovedtemaer/brukerroller: Individ kultur og miljø – Læring hele livet – Næringslivet – Arbeidslivet – Offentlig sektor. For offentlig sektor pekes det på behovet for en moderne forvaltning der IKT skal bidra til å bedre kvaliteten på tjenestene innenfor rammene av personvern rettssikkerhet krav til dokumentasjon og innsynsrett med understrekning av at det er viktig med tilgang på informasjon som er oppdatert pålitelig og landsdekkende. For helsesektoren understrekes det at ny teknologi skal bidra til å bedre tjenestetilbud samarbeid og informasjonsutveksling med fokus bl.a. på å videreutvikle de regionale helsenettene knytte dem sammen til et nasjonalt helsenett tilby sikker tilgang til Internett og etablere tilbud av nasjonale informasjonstjenester. En ny statlig IKT-tiltaksplan for helse- og sosialsektoren for 2001–2003 ble lagt fram av helseministeren den 31.1.2001. Også samferdselssektoren og utenriks- og utviklingssektoren er framhevet spesielt i den delen av planen som omfatter offentlig sektor.

5.2.2 Rådet for IT-sikkerhet

Rådet for IT-sikkerhet (RITS) ble opprettet våren 1996 som et forum for erfaringsutveksling med en rådgivende funksjon overfor departementene. Rådet skulle ta opp saker av felles interesse og ta tverrsektorielle initiativer ved behov. Rådet ble etablert under Administrasjonsdepartementet og pr. januar 1998 flyttet til Nærings- og handelsdepartementet. Et antall departementer og direktorater deltok i RITS. Det ble etablert arbeidsgrupper for å lage utredninger på områder som det var enighet om å prioritere. Arbeidsgruppene fikk bred deltakelse også fra kommune-Norge og privat sektor. Dette resulterte i tre rapporter som ble behandlet av RITS og sendt videre til Næringsdepartementet med Rådets anbefalinger. Rapportene er omtalt nedenfor.

- *Digitale signaturer gir tillit til elektronisk kommunikasjon: Forslag til tiltak for aksept og utbredelse*. Rapport med forberedende utredning avgitt til Rådet for IT-sikkerhet 30.11.1998 [63].

Arbeidsgruppen som laget denne utredningen var bredt sammensatt med 17 deltakere fra departementer og direktorater næringslivet og universitetet. To tidligere utredninger for RITS dannet en bakgrunn:

- *Sertifisering av IT-sikkerhet i produkter systemer og organisasjoner* (Sluttrapport 13. november 1997) [64]

Regjering og Storting vedtok i 1998 at det skulle etableres to nye sertifiseringsordninger. Arbeidet med å etablere disse ble satt i gang i 1999 av Forsvarets overkommando/Sikkerhetsstaben som fikk i oppgave å etablere en sivil ordning for sertifisering av IT-sikkerhet i produkter og systemer og av Norsk Akkreditering som fikk i oppdrag å etablere en ordning for sertifisering av IT-sikkerhet i organisasjoner.

- *Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk* (10. november 1997) [65].

Ett politisk mål (av mange) var formulert slik i *Den norske IT-veien. Bit for bit* [70] pkt. 3.3.6:

Elektronisk kommunikasjon og bruk av nett som infrastruktur for samhandling skal bli like akseptert tillitvekkende og ha samme juridiske holdbarhet som tradisjonell papirbasert skriftlig kommunikasjon og dokumentasjon.

For å nå dette målet ble det presisert at det måtte avklares en rekke forhold og utvikles nye fellesordninger med klar ansvarsplassering.

Dette punktet kommenteres av arbeidsgruppen for kryptopolitikk nevnt over. Gruppen hevdet følgende:

Oppnåelse av dette mål medfører at informasjonen må beskyttes mot innsyn fra uvedkommende at den er beskyttet mot uautoriserte endringer at den må utstyres med elektroniske signaturer som er juridisk og teknologisk likeverdig med håndskrevne signaturer og at informasjonen er tilgjengelig for autoriserte brukere ved behov. Målet kan bare nås dersom det er etablert en homogen kryptopolitikk det etableres troverdige kryptoløsninger for å sikre konfidensialitet og det etableres en infrastruktur for elektroniske signaturer og sertifisering av disse dvs. en tiltrodd tredjepartstjeneste (TTP). Juridiske og policymessige aspekter må utredes.

I forlengelsen av dette ble utredningen om digitale signaturer datert 30.11.98 gjennomført. Den konkluderte med å foreslå 14 tiltak fordelt på tre hovedområder: For det første ble det anbefalt å prioritere sterkt et videre arbeid med regelverket for å oppnå rettslig aksept og likestilling (jf. det seinere Kartleggingsprosjektet/eRegel-prosjektet) for det andre burde man gå dypere inn i forutsetningene for å legge til rette og gi rammebetingelser for bl.a. en frivillig godkjenningsordning for TTP-er (jf. det seinere utvalget om myndighetsroller mv. Torvundutvalget) for det tredje burde man vinne betydelig mer erfaring gjennom praktiske forsøk og piloter med brede anvendelsesområder. Arbeidet med rettslig aksept og konkrete pilotforsøk ble ansett som viktigst å følge opp.

Det ble generelt understreket i rapporten at det er næringslivet og markedet som er hovedaktører med hensyn til styring av teknologisk og markedsmessig utvikling mens myndighetenes rolle er å gi bidrag ved å være god bruker samt på utvalgte områder legge til rette for særlig de delene av markedet som har behov for et noe høyere sikkerhetsnivå enn det ordinære og generelt lave nivået. Et viktig premiss var at markedet ikke skulle hemmes av myndighetenes tiltak. Et frivillighetsprinsipp skulle råde f.eks. i forhold til en eventuell godkjenningsordning for TTP-er. Norske løsninger måtte bygge på tilsvarende internasjonale normer kriterier og standarder og det ble anbefalt at Norge deltar aktivt i den videre utviklingen av disse.

Rådet for IT-sikkerhet ble nedlagt og et nytt *Forum for IT-sikkerhet* opprettet i år 2000 med nytt mandat og nye deltakere. Forumet er bredere sammensatt med faste representanter også fra næringslivet og det akademiske miljøet. Det skal identifisere viktige saker og gi grunnlag for Nærings- og handelsdepartementets prioriteringer.

5.2.3 Forvaltningsnettsamarbeidets rammeavtaler om digitale signaturer (produkter og tjenester)

Bakgrunn og historikk

Arbeids- og administrasjonsdepartementet og Kommunenes Sentralforbund tok initiativet til Forvaltningsnettprosjektet i 1996 på grunnlag av anbefalingene i KOSTIT-strategiplanen framlagt i 1995. Målet for prosjektet var å fremme enkel sikker og kostnadseffektiv elektronisk informasjonsutveksling innad i forvaltningen og utad mot andre brukere.

Målsettingen skulle realiseres ved å inngå rammeavtaler med utvalgte leverandører av datatjenester og -produkter teletjenester og -produkter samt leverandører av fellestjenester som f.eks. konvertering av e-post basert på felles kravspesifikasjoner. I tillegg skulle prosjektet sørge for etablering av en rekke andre typer fellestjenester som er nødvendige for en helhetlig og vel fungerende elektronisk infrastruktur.

Rammeavtalene for produkter og tjenester kan benyttes av virksomheter innen offentlig sektor (stat eller kommune) og i enkelte tilfeller også av aktører som i hovedsak finansieres av offentlig virksomhet f.eks. privatpraktiserende leger. Forvaltningsnettprosjektet tok i april 1998 initiativ til å etablere en arbeidsgruppe ledet av Arbeids- og administrasjonsdepartementet (AAD) som fikk i oppdrag å utarbeide en kravspesifikasjon for løsninger for digitale signaturer og tilhørende tiltrodde tredjepartstjenester. Bakgrunnen for dette var et stigende behov for slike tjenester i forbindelse med iverksetting av ulike prosjekter vedr. elektronisk informasjonsutveksling i forvaltningen.

I gruppen deltok i tillegg til AAD Nærings- og handelsdepartementet Sosial- og helsedepartementet Kommunal- og regionaldepartementet Statistisk sentralbyrå Skattedirektoratet Kompetansesenteret for IT i Helsevesenet og Norsk EDIPRO. Brønnøysundregistrene var observatør. Norsk Regnesentral var sekretær

for gruppen og hadde hovedansvaret for utforming av kravspesifikasjonen. Gruppen samarbeidet tett med RITS'[5]arbeidsgruppe for digitale signaturer som gjennomførte sin utredning da.

I desember 1998 ble det utlyst en forespørsel etter TTP-tjenester (sertifikattjenester) samt systemer for digitale signaturer og meldingskryptering.

Rammeavtale om digitale signaturer og TTP-tjenester ble undertegnet 12.5.1999 med varighet fram til 1.6.2000 seinere forlenget til 1.6.2001. De leverandørene som leverer TTP-tjenester (også sertifikattjenester) er Posten SDS (nå ErgoGroup) Strålfors og Telenor.

Avtalens innhold og struktur

Rammeavtalen om digitale signaturer og TTP-tjenester følger den generelle strukturen i alle rammeavtaler under Forvaltningsnettsamarbeidet. Dette innebærer at for denne avtalen gjelder «Generelle vilkår» samt en rekke «Spesielle vilkår». Det er utviklet «Spesielle vilkår» for TTP-tjenester spesielt for dette området. Kjøp av programvare og utstyr for digitale signaturer skjer under «Spesielle vilkår» for kjøp av programvare. Det er i tillegg anvendt en rekke «Spesielle vilkår» for kjøp av pakkeløsninger konsulenttjenester vedlikeholdsavtaler med mer. «Standard kjøpsavtale» inngår også i de juridiske rammevilkår for avtalen.

Den 15.9.1999 undertegnet de tre leverandørene av sertifikattjenester (TTP-tjenester) som finnes i avtalen en egen tredjepartsavtale om kryssertifisering seg imellom. Denne avtalen oppfyller vilkår stilt i «Spesielle vilkår» for TTP-tjenester punkt 1 om at disse leverandørene skal kryssertifisere. Rammeavtalen ble åpnet for bestilling fra samme dato. Kryssertifiseringsavtalen skal være et eget bilag til kjøpsavtalen ved bestilling via rammeavtalen.

Kryssertifiseringsavtalen berører hovedsakelig to forhold:

- Tillit til hverandres sertifikater og erstatningsvilkår knyttet til dette
- Samtrafikk mellom sertifikatkataloger hos de tre leverandørene for å tillate enkle søk etter sertifikater og enkel uthenting av CRL (tilbaketrekkingslister).

Grunnlaget for kryssertifisering/godkjenning av hverandres sertifikater er en felles sertifikatpolicy basert på SEIS S10 [68]. Policyen kalles FSP-1[6] Denne policyen ble også med tilbakevirkende kraft lagt til grunn for leveranse av TTP-tjenester under rammeavtalen (istedenfor SEIS S10).

I følge Kryssertifiseringsavtalen skulle alle leverandører gjennomføre en revisjon av sine TTP-virksomheter på to nivåer: 1) at sertifikatpraksis faktisk implementerer FSP-1 og 2) at den faktiske gjennomføringen av tjenesten samsvarer med sertifikatpraksis.

Revisjon ble gjennomført hos alle tre leverandørene og kryssertifikater ble utvekslet 15.9.2000 (5.10.2000 med Strålfors).

Leverandørene av TTP-tjenester forpliktet seg til å følge navne- og identifiseringsreglene til FNS. Disse er nedfelt i en egen rapport [28] og videre i sertifikatpolicyen FSP-1. Disse reglene innebærer bl.a. at det skal medtas offisielle navn fra folkeregisteret og fra Brønnøysundregistrene i sertifikater på henholdsvis personer og organisasjoner.

Grafisk kan avtalestrukturen illustreres som i figur 5.1.

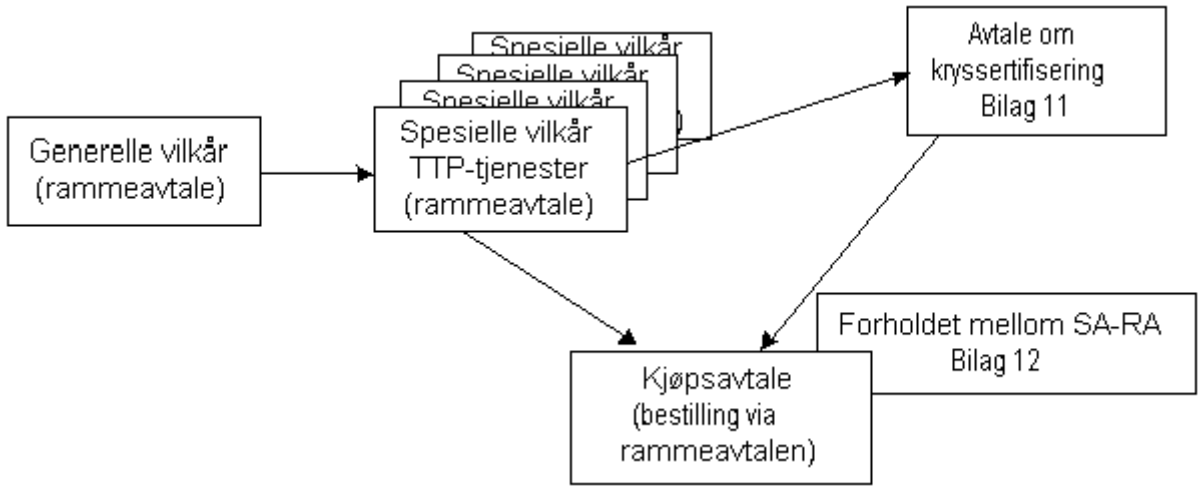
5

Rådet for IT-sikkerhet nå nedlagt erstattet av Forum for IT-sikkerhet.

6

Forvaltningsnettsamarbeidets sertifikatpolicy nr. 1.

.



Figur 5.1 Digital signatur

Relevante dokumenter

En rekke dokumenter foreligger i tilknytning til FNS-rammeavtale om digitale signaturer med tilhørende tjenester (se http://forvaltningsnett.dep.no):

- *Forvaltningsnettsamarbeidets Sertifiseringspolicy nr. 1 (FSP-1)*. Høysikkerhets sertifiseringspolicy for utstedelse av x.509-baserte sertifikater for personer og virksomheter i norsk offentlig forvaltning. (FNS-rapport 8/99) [2]
- *Navn og identifikatorer i sertifikater i Forvaltningsnettsamarbeidet. Anbefalinger fra arbeidsgruppe*. (FNS-rapport 6/99) [28]
- *Anskaffelse og innføring av digital signatur med tilhørende tjenester.* Veileder. (FNS-rapport 12/99)
- Avtale om kryssertifisering mellom Posten SDS og Strålfors AS og Telenor AS med vedlegg
- *Kravspesifikasjon for tiltrodde tredjepartstjenester digital signatur og meldingskryptering* versjon av 8.5.1999 (Vedlegg 1 til rammeavtalen)
- Spesielle vilkår for Tiltrodd Tredjepartstjenester med tillegg (endring av § 2.13)
- Generelt FNS-avtaleverk. (FNS-rapport 5/99).

5.2.4 Elektronisk forvaltning. Handlingsplan for tverrsektoriell IT-utvikling (1999–2001)

Arbeids- og administrasjonsdepartementet la fram handlingsplanen i januar 1999. Formålet med planen var å trekke opp utfordringer og definere strategier og tiltak som skal legge til rette for formålstjenlig og effektiv IT-anvendelse i hele statsforvaltningen på tvers av sektorene.

Handlingsplanen søker å svare på tre spørsmål om utvikling av bruken av informasjonsteknologi (IT) i statsforvaltningen:

1. Hvordan kan IT brukes for å understøtte overordnede mål for forvaltningsutviklingen?
2. Hvilke oppgaver må løses for å få IT-systemer og IT-løsninger i de ulike sektorer til å virke sammen i en helhetlig og effektiv elektronisk forvaltning?

3. Hvilke generelle grep og råd kan sikre effektiv og hensiktsmessig utvikling og anvendelse av IT i den enkelte sektor?

Det første spørsmålet dreier seg om strategisk anvendelse av IT for statsforvaltningen som et hele. Det andre spørsmålet fokuserer på koordinering og samordning av sektorenes IT-bruk. Det tredje spørsmålet omhandler metoder og retningslinjer for god utvikling og anvendelse av IT innen den enkelte sektor.

Til sammen definerer disse tre spørsmålene grunnlaget for den tverrsektorielle IT-utviklingen i statsforvaltningen. Det er innenfor de nevnte områdene at de sektorspesifikke IT-strategiene som utvikles av det enkelte fagdepartement bør suppleres og understøttes av tverrsektorielle strategier og tiltak.

Med dette utgangspunktet skisserer *Elektronisk forvaltning* planene for den tverrsektorielle IT-utviklingen i statsforvaltningen i perioden 1999 til 2001. Den er et supplement til IT-strategiene som utvikles av det enkelte fagdepartement.

Handlingsplanen definerer åtte innsatsområder for den tverrsektorielle IT-utviklingen i statsforvaltningen i perioden 1999–2001. Disse åtte områdene er:

1. År 2000-sikkerhet
2. Infrastruktur
3. IT-sikkerhet
4. Informasjonstjenester på Internett
5. Elektronisk saksbehandling
6. Elektronisk datautveksling
7. Elektronisk handel i offentlige innkjøp
8. Styring og organisering av IT.

Under området infrastruktur slås det bl.a. fast at i forbindelse med elektronisk handel elektronisk saksbehandling og datautveksling melder det seg et økende behov for etablering av en infrastruktur for offentlignøkkel-kryptografi (såkalt Public Key Infrastructure PKI). Etablering av elementer i en slik infrastruktur for autentisering digitale signaturer og kryptering (konfidensialitet) i statsforvaltningen er definert som ett av hovedtiltakene under området. Det skal legges til rette for slik etablering bl.a. gjennom innkjøpsordningen under Forvaltningsnettsamarbeidet se punkt 5.2.3.

5.2.5 eRegel-prosjektet (tidligere kalt Kartleggingsprosjektet)

Prosjektet for kartlegging og fjerning av bestemmelser i lover forskrifter og instrukser som kan hindre elektronisk kommunikasjon ble initiert i mars 1999 etter et felles initiativ fra arbeids- og administrasjonsministeren justisministeren og nærings- og handelsministeren. Prosjektet ble kalt Kartleggingsprosjektet.

Det overordnede målet for prosjektet er at elektronisk kommunikasjon skal være like pålitelig tillitvekkende og juridisk bindende som den papirbaserte.

Prosjektet har en styringsgruppe med representanter for de tre departementene. Det praktiske arbeidet ledes av Nærings- og handelsdepartementet (NHD). Den første fasen av prosjektet der samtlige lover forskrifter og instrukser ble gjennomgått med tanke på å identifisere hindringer for elektronisk kommunikasjon ble avsluttet 30.9.1999. Funnene fra kartleggingen ble presentert i en omfattende rapport som ble lagt fram medio juni 2000 [47]. Rapporten tar for seg typeeksempler på hindringer og vurderer hvorvidt hensynene bak forskjellige formkrav for papirbasert kommunikasjon også kan ivaretas ved elektronisk kommunikasjon.

Regjeringen besluttet i september 2000 at de identifiserte hindringene skal fjernes slik at et oppdatert lov- og regelverk kan tre i kraft innen 1.1.2002.

Det forelå tre ulike alternativer til måten endringene skulle gjennomføres på:

1. Vedta en generell lov om elektronisk kommunikasjon som vil likestille elektronisk kommunikasjon med den papirbaserte på tvers av hele lovverket. Forvaltere av lov- og regelverk må gå gjennom sine lover forskrifter med mer for eventuelt å gjøre særskilte

unntak fra denne generelle regelen der slik likestilling ikke er ønskelig ut fra begrunnede hensyn.
2. Endre relevante lover forskrifter og instrukser hver for seg slik at hindringene fjernes og det legges til rette for elektronisk kommunikasjon.
3. Innføre et pålegg i lovs form om å legge til rette for elektronisk kommunikasjon i regelverket med adgang til å klage på manglende tilrettelegging. Innebærer ellers en gjennomgang av og endring i hver enkelt bestemmelse.

Regjeringen besluttet at endringene skal gjennomføres etter alternativ 2.

Prosjektet som har endret navn til eRegel-prosjektet er nå i en ny fase. Arbeidet i denne fasen gjennomføres etter en plan der alle departementer skal sende ut lovendringsforslag på høring innen 15.1.2001 med høringsfrist 1.3.2001. Reviderte forslag skal så innarbeides i en felles Ot.prp. som skal fremmes av NHD. Proposisjonen skal etter planen fremmes 1.8.2001.

Det forventes at de foreslåtte endringene skal tre i kraft pr. 1.1.2002.

Samtidig med lovendringsarbeidet skal det foregå endringsarbeid i forskrifter og instrukser. Det forventes at endrede forskrifter og instrukser skal tre i kraft 1.7.2001. Forskrifter til lover som foreslås endret i den felles proposisjonen skal endres slik at de trer i kraft samtidig med den endrede loven dvs. 1.1.2002. Hvert departement skal også innen denne datoen rapportere til NHD om begrunnelse for de unntak som bør opprettholdes.

Som en del av arbeidet i eRegel-prosjektet skal forvaltningsloven endres slik at den eksplisitt skal legge til rette for elektronisk kommunikasjon i forvaltningssaker. Det forventes at det blir innført en ny hjemmel i denne loven for å kunne gi nærmere bestemmelser om hvordan slik elektronisk kommunikasjon skal foregå. Utvalget mener at utvalgets innstilling på mandatets punkt 6 kapittel 11 kan danne et grunnlag for slik regulering.

5.2.6 Stortingsmelding nr. 41 (1998–99) Om elektronisk handel og forretningsdrift

Mål og strategier for elektronisk handel og forretningsdrift i Norge ble presentert i 1998 i rapporten *En utkant i forkant. Næringsrettet IT-plan*. Den ble lagt fram av Nærings- og handelsdepartementet på grunnlag av St.meld. nr. 41 (1997–98) om næringspolitikk inn i det 21. århundre som trakk opp hovedlinjene for næringspolitikken framover.

Stortingsmelding nr. 41 (1998–99) ble godkjent i statsråd 11. juni 1999. Visjonen som lå til grunn var at Norge skal være i fremste rekke når det gjelder den globaliserte IT-utviklingen samtidig som man ønsket å legge en bevisst kurs når det gjelder de samfunnsmessige sidene ved utviklingen. Med denne stortingsmeldingen ønsket regjeringen å gi impulser til ny næringsutvikling og man så elektronisk handel som et viktig vekstområde. Regjeringen var samtidig opptatt av å utfordre næringslivet til å innta en offensiv holdning til samfunnsmessige hensyn som forbrukervern og personvern og heller gjøre dette til fortrinn framfor problemer.

Videre så regjeringen et behov for å gjøre opp status trekke opp hovedlinjene i politikken og identifisere viktige innsatsområder for videre arbeid. Fordi det har vært en viss usikkerhet om de rettslige rammebetingelsene for elektronisk handel var det et mål å informere om hva som ansees å være uproblematisk og derfor ikke til hinder for elektronisk handel og samtidig opplyse om de prosesser som er iverksatt for å fjerne hindringer.

Elektronisk handel reiser utfordringer som bør debatteres politisk. Regjeringen mente at elektronisk handel angår så mange ulike samfunnsområder og samfunnshensyn at en bred og engasjert debatt om samfunnsmessige utfordringer og muligheter for verdiskapning og næringsutvikling er nødvendig. Denne debatten vil samtidig bidra til spredning av kunnskap på området og gi innsikt i utviklingen internasjonalt. Dette kan bidra til raskere utvikling og utbredelse av elektronisk handel og forretningsdrift.

Hovedvekten i meldingen ble lagt på de næringspolitiske utfordringene og på hvilken rolle myndighetene og offentlig sektor for øvrig bør inneha for å tilrettelegge for utviklingen.

Meldingen slo fast at i arbeidet med elektronisk handel vil følgende prinsipper bli lagt til grunn:

1. Elektronisk handel vil bli drevet fram av markedet i form av produkter og tjenester som bedrifter og forbrukere vil etterspørre.
2. Der myndighetene griper inn må dette skje i full åpenhet og dialog med de berørte parter.
3. Reguleringene må være nøytrale i forhold til teknologi og ikke være bundet til bestemte teknologiske løsninger.

Meldingen slo videre fast at målene om utvikling og spredning av elektronisk handel i Norge skal nås gjennom systematisk arbeid i henhold til fem hovedstrategier:

- Det må utformes forutsigbare rettslige og økonomiske rammebetingelser for elektronisk handel som sikrer norske bedrifters konkurranseevne nasjonalt og internasjonalt
- Det må utvikles infrastruktur og tjenester som forenkler bruken og gir tilgang for alle potensielle brukergrupper over hele landet
- Det må bli tilstrekkelig mange brukere av elektronisk handel. Bl.a. vil offentlig sektor gjennom å ta i bruk elektronisk handel i offentlige innkjøp bidra til dette
- Det må utvikles kunnskap og innsikt i elektronisk handel for å skape valgfrihet og motvirke uheldige og uønskede konsekvenser
- Det skal arbeides for aktiv ivaretakelse av sosiale og samfunnsmessige hensyn som sikkerhet personvern og forbrukervern herunder hensynet til barn og unge og håndtere dette slik at det kan bli et konkurransefortrinn for norske aktører.

Elektronisk signatur ble ansett som et viktig virkemiddel i flere av disse strategiene. Forslag til regulering av elektroniske signaturer se punkt 5.2.8 ville bidra til forutsigbarhet i rammebetingelsene og infrastruktur for digitale signaturer (offentlignøkkel-infrastruktur) som er en viktig komponent i nødvendig infrastruktur for e-handel. Videre er målet om innføring av elektronisk handel i offentlige innkjøp avhengig av at slike infrastrukturer er tilgjengelige.

Meldingen ble debattert i Stortinget i mars 2000. I næringskomiteens innstilling S. nr. 127 (1999–2000) ble det bl.a. lagt vekt på at offentlig forvaltning må kunne dra nytte av utviklingen innen elektronisk handel og forretningsdrift bl.a. ved å legge til rette for omfattende elektronisk innrapportering fra bedriftene. Det ble pekt på at forvaltningen og næringslivet i denne sammenheng kan dra nytte av en felles infrastruktur. Det ble videre poengtert at det er behov for å ta i bruk internasjonalt forankrede sertifiseringsordninger for å øke sikkerheten og skape tillit til aktørene i elektronisk handel. Det ble særlig pekt på behov for sikre og pålitelige løsninger for betalingsformidling.

5.2.7 Elektroniske signaturer. Myndighetsroller og regulering av tilbydere av sertifikattjenester

Det såkalte Torvundutvalget ble oppnevnt av Nærings- og handelsdepartementet i juni 1999 og avla sin rapport i januar 2000 bl.a. på bakgrunn av Rådet for IT-sikkerhets (RITS) behandling av rapporten *Digitale signaturer skaper tillit* [63]. Utvalget skulle utrede rammebetingelser for leverandører av digitale signaturer i Norge med utgangspunkt i EU's forslag til regulering av området gjennom direktivet vedrørende rammebetingelser for elektroniske signaturer (EC/93/1999).

Hovedspørsmålene som utvalget skulle utrede omfattet:

1. Frivillig godkjenningsordning for TTP-virksomhet og krav til slik virksomhet. Utvalget skulle vurdere hvilket tillitsnivå som ansees nødvendig for at TTP-virksomhet skal kunne anerkjennes rettslig og med dette som utgangspunkt legge fram konkrete forslag til hvordan en frivillig godkjenningsordning og/eller tilsynsorgan skal etableres helst med utgangspunkt i allerede etablerte ordninger.

2. Anerkjennelse av sertifikater. Utvalget skulle legge fram forslag til hvordan gjensidig anerkjennelse av sertifikater mellom tjenesteleverandører i Norge og i forhold til utenlandske leverandører kan sikres på en hensiktsmessig måte.
3. Typer av roller i markedet. Hvilke roller og oppgaver bør utføres som ledd i forretningsvirksomhet i markedet og hvilke bør eventuelt utføres av sentrale myndigheter?
4. Finansiering av TTP-virksomhet. Dersom det offentlige gis ansvar for visse oppgaver knyttet til TTP-virksomhet hvordan bør de finansieres?
5. Modeller i andre land. Utvalget skulle kort gjøre rede for typiske modeller som er anvendt på spørsmålene 1–4 i andre land som f.eks. Danmark Sverige og England.
6. Økonomiske og administrative konsekvenser.

Utvalget besto av deltakere fra Institutt for rettsinformatikk Universitetet i Oslo (leder) Arbeids- og administrasjonsdepartementet Den norske Bankforening Post- og teletilsynet Finansdepartementet Norsk Hydro og Nærings- og handelsdepartementet. Sekretariatet ble ivaretatt av Statskonsult.

Det ble trukket fram som grunnleggende premisser for utvalgets innstilling at en regulering av sertifikatutstedere ikke bør være med på å øke prisene på sluttproduktene og -tjenestene i vesentlig grad samtidig som behov for ordninger som skaper tillit blir ivaretatt. Videre tok man hensyn til at de fleste av de etablerte utstederne ønsket en felles tilsynsmyndighet for sertifikatutstedere som skal utstede kvalifiserte sertifikater.

Utvalget slo fast at det så langt (i 1999) mangler noen kriterier og standarder for å kunne etablere en frivillig sertifiseringsordning for sertifikatutstedere i Norge. Sikkerhetsevalueringen av organisasjoner basert på standarden BS 7799 vil bli tilbudt også i Norge for sertifisering av informasjonssikkerhet i en organisasjon. Denne ordningen sertifiserer imidlertid ikke hele den virksomhet en sertifikatutsteder driver. Utvalget mente likevel at de utstedere som skal tilby kvalifiserte sertifikater bør kunne benytte denne standarden for å vurdere sikkerheten i egen organisasjon.

Utvalget konkluderte med at det bør utpekes en offentlig tilsynsmyndighet som skal drive tilsyn med alle sertifikatutstedere etablert i Norge som skal utstede kvalifiserte sertifikater. Tilsynet bør være så markedsorientert som mulig slik at man ikke legger unødvendige administrative byrder og derved kostnader på sertifikatutstedere.

Tilsynsmyndigheten ble foreslått lagt til Post- og teletilsynet. Det ble slått fast at tilsynsmyndigheten kan kreve å få alle de opplysninger som er nødvendige for å sikre at sertifikatutstedere som tilbyr kvalifiserte sertifikater oppfyller kravene i loven. Slik kontroll kan skje dersom tilsynet mener det er nødvendig eller etter «krav» fra brukere eller andre aktører.

Det ble videre foreslått at det etableres en registreringsordning for sertifikatutstedere som tilbyr kvalifiserte sertifikater. Sertifikatutstedere som skal utstede kvalifiserte sertifikater i Norge må melde denne virksomheten inn til tilsynsmyndigheten. Denne meldingen skal være en deklarasjon om at sertifikatutstederen oppfyller kravene til kvalifisert sertifikat herunder opplyse om hvilke sertifikatpolicyer de følger og hvordan deres sertifikatpraksis er. Tilsynet kan vise til hvilke policyer og praksis som oppfyller kravene. Dersom en tilbyder ønsker å anvende en annen policy/praksis som ikke er godkjent må tilsynet gjøre en realitetsvurdering av den. Denne realitetsvurderingen bør være tilgjengelig for tredjemann. Også policyer som ikke er godkjent bør være tilgjengelige.

Forslaget om registreringsordning innebærer at virksomheten blir registrert i et eget register med oversikt over sertifikatutstedere som utsteder kvalifiserte sertifikater. Deklarasjonen sendes kun inn ved oppstart av virksomheten og eventuelt ved endringer i registrerte opplysninger.

Utvalget uttalte at det på et seinere tidspunkt bør vurderes å opprette en frivillig registreringsordning for andre enn kvalifiserte sertifikater hvis det viser seg at markedet for denne typen sertifikattjenester er voksende.

Utvalget så positivt på at det etableres frivillige godkjenningsordninger for sertifikatutstedere i markedet men anbefalte at det ikke tas noe initiativ fra myndighetene for å få etablert dette. En frivillig godkjenningsordning kan kombineres med en frivillig ordning for registrering av sertifikatutstedere.

5.2.8 Lov om elektronisk signatur

Loven ble fremmet for Stortinget i oktober 2000 på grunnlag av Ot.prp. nr. 82 (1999-2000) og vedtatt i desember samme år [52]. Nærings- og handelsdepartementet utarbeider i samarbeid med Post- og teletilsynet utkast til forskrifter til loven. Det forventes at utkastet blir sendt på høring i februar 2001. Loven med forskriftene forventes å tre i kraft 1.7.2001.

Loven er en gjennomføring av EU-direktivet om en fellesskapsramme for elektroniske signaturer jf. omtale foran i dette kapitlet. Direktivet ble endelig vedtatt den 13. desember 1999 og ble publisert i De Europeiske Fellesskaps Tidende (EF-Tidende) den 19. januar 2000 med en implementeringstid for medlemslandene på 18 måneder. Denne fristen gjelder også for Norge.

Til grunn for lovforslaget ligger forutsetningen om behov for regulering av elektronisk signatur for å legge til rette for utviklingen av elektronisk handel og elektroniske tjenester i Norge. Lovreguleringen skal søke å påvirke det norske markedet for sertifikatutstedere og elektroniske signaturprodukter i en positiv retning. Ved å regulere tilbudet av det loven definerer som «kvalifiserte sertifikater» vil lovforslaget stimulere til bruk av sertifikater med et bestemt sikkerhetsnivå som kan brukes i mange sammenhenger både praktisk og ikke minst rettslig. Videre ble det ansett å være behov for lovregulering på området for å bidra til at tilliten til markedet og tilliten til bruk av elektroniske signaturer i samfunnet øker slik at signaturteknologi lettere blir tatt i bruk på bred basis.

Loven gir noen rettslige rammebetingelser for bruk av elektronisk signatur og tilknyttede tjenester. Et viktig formål med lovforslaget er å sikre kommunikasjon mellom to parter som ikke kjenner hverandre og som ønsker å samhandle elektronisk over åpne nett.

Loven skal bidra til å legge til rette for at i hvert fall en del av de signaturene og tilhørende sertifikater som tilbys på det norske markedet skal oppfylle et bestemt sikkerhetsnivå. Ett formål med dette er at de som mener å ha behov for et slikt kvalitets- og sikkerhetsnivå kan velge dette ut fra en tilrettelegging og en rettstilstand som er felles i EØS. Kravene til sikkerhet skal balanseres mellom forretningsmessige hensyn forbrukerhensyn og samfunnsmessige hensyn. De nærmere tekniske kravene vil bli regulert i forskrifter til loven. Loven åpner i § 5 for at det kan stilles tilleggskrav til kvalifiserte signaturer ved kommunikasjon med og i forvaltningen.

Loven skal ikke regulere det samlede tilbudet av signaturer og tilhørende sertifikater og sertifikattjenester men i all hovedsak regulere rammebetingelsene for bruk av kvalifiserte signaturer og kvalifiserte sertifikater. Sertifikatutstederne vil dermed falle utenfor denne lovreguleringen og det tilsynsregimet loven oppstiller ved ikke å kalle sine sertifikater for kvalifiserte selv om de ellers oppfyller kravene. Man ser for seg at sertifikater med et lavere sikkerhetsnivå eller andre sikkerhetsmekanismer kan tilfredsstille behovene for deler av markedet. Etterspørselen i markedet vil avgjøre hvilke sertifikater som vil bli benyttet framover.

Loven gir ingen generell regulering av rett til å kommunisere elektronisk men gjelder der lovgivningen for øvrig åpner for elektronisk kommunikasjon. Når det stilles krav om underskrift vil bruk av kvalifisert elektronisk signatur alltid oppfylle et slikt krav så fremt disposisjonen rettslig sett kan skje elektronisk. Dette betyr at en kvalifisert elektronisk signatur i henhold til loven alltid gis samme rettsvirkning som en håndskreven signatur. I tillegg slår loven fast at også en elektronisk signatur som ikke er kvalifisert kan gis samme rettsvirkning. Det at signaturen ikke er kvalifisert vil kunne ha betydning for signaturens beviskraft men direktivet stiller ikke krav i forhold til beviskraften. I forarbeidene til loven pekes det blant annet på at vi i norsk rett har fri bevisføring og fri bevisvurdering noe som vil få betydning i det enkelte tilfellet.

Reguleringen i loven er så langt som mulig nøytral i forhold til valg av tekniske løsninger for å unngå behov for hyppige justeringer. Samtidig er det vanskelig å gi rettslige virkninger til en ukjent eller ikke definert teknisk løsning. Her er det gjort en avveining mellom å være teknologinøytral og å gi de teknologier som omfattes av loven rettslige virkninger.

Loven regulerer utstedere av kvalifiserte sertifikater med to unntak: bestemmelsen i § 6 første ledd siste punktum om rettsvirkning og bestemmelsen i § 7 om innsamling og bruk av personopplysninger. Disse to bestemmelsene gjelder alle typer av sertifikater og alle sertifikatutstedere.

5.3 Personvern

5.3.1 Behandling av personopplysninger

Fra 1. januar 2001 trådte lov om behandling av personopplysninger i kraft [51]. Loven erstatter personregisterloven av 1978. Lovendringen markerer at reguleringsprinsipper for behandling av personopplysninger i Norge tilpasses reglene i EU's personverndirektiv 95/46/EF. Personopplysningsloven har som utgangspunkt at alle behandlinger skal være formålsbestemt. Videre er et grunnlag for å tillate behandling at denne er lovlig (jf. personopplysningsloven § 11) og som hovedregel basert på samtykke fra den personopplysningene gjelder (jf. §§ 8 og 9). Behandling av personopplysninger skal gjennomføres med tilfredsstillende sikring av opplysningenes konfidensialitet tilgjengelighet og integritet.

Sammen med personopplysningsloven trer utfyllende bestemmelser for behandling av personopplysninger i kraft i form av en egen «personopplysningsforskrift».[7]Forskriften inneholder krav til sikring av de personopplysningene som behandles. Gjennom planlagte og systematiske tiltak skal hver enkelt behandling gjennomføres med tilfredsstillende sikkerhet som resultat. Sikkerhetstiltak skal baseres på risikovurdering og tilpasses sikkerhetsbehovet knyttet til den enkelte behandling.

Datatilsynet skal føre tilsyn med at bestemmelsene i personopplysningsloven etterleves og kan gi pålegg om endring eller opphør av ulovlige behandlinger. Tilsynsansvaret omfatter kompetanse til å gi pålegg om konkrete sikkerhetstiltak.

5.3.2 Elektroniske spor

Bruk av elektroniske hjelpemidler for behandling av personopplysninger og i særlig grad elektronisk kommunikasjon genererer ofte elektroniske spor. Lagring og eventuell spredning av elektroniske spor kan være nødvendige operasjoner i den formålsbestemte behandlingen som gjennomføres og vil i seg selv ikke utgjøre et personvernproblem. Problemet oppstår når elektroniske spor tas i bruk til annet formål enn det opprinnelige. Det er i dag et betydelig press for å skaffe tilgang til elektroniske spor for sekundær bruk – for eksempel til profilering markedsføring kontroll- og forskningsmessige formål. Både private virksomheter og offentlige myndigheter øver press for å utvide grunnlaget for lovlig tilgang til personopplysninger «som jo likevel er tilstede i kommunikasjonskjeden». Tilsvarende øves et visst press på å utnytte potensialet i kommunikasjonssystemene for ytterligere registrering enn det som strengt tatt er nødvendig for det opprinnelige formålet.

Resultatet kan bli et stadig mer gjennomsiktig samfunn der opplysninger om bevegelsene behovene ønskene og preferansene til hver enkelt av oss er tilgjengelige og benyttes i en lang rekke behandlinger – lovlige eller ulovlige. Behandlingen av personopplysninger blir samtidig så variert og omfangsrik at vi som enkeltmennesker i liten grad har mulighet til å holde oss tilstrekkelig informert til å kunne utøve vår rett til å gi eller nekte samtykke.

Sekundær bruk som beskrevet over kan være ulovlig men vanskelig å hindre. Dette blir en følge av den store spredning og effektive tilgang moderne elektroniske kommunikasjonssystemer ofte gir. Det eneste praktiske virkemiddelet kan være å holde seg strengt til kravet om formålsbestemthet. Det vil si å ikke tillate behandling av andre personopplysninger enn de som er nødvendig for å oppnå det ønskede formål. I praksis betyr dette en kritisk vurdering av omfang type og metode for behandling av personopplysninger når nye tjenester eller systemer ønskes etablert. Alternative løsninger der behovet for behandling av personopplysninger er mindre må evalueres og en eventuell gevinst må ved den foreslåtte behandling

---

7

vurderes opp mot den enkeltes rett til beskyttelse av egen privat sfære. Disse vurderingene skal gjøres av den som beslutter formålet med behandlingen.

5.3.3 Digitale sertifikater

Ved å ta i bruk digitale signaturer ønsker forvaltningen moderne og effektive kommunikasjonstjenester samtidig som dagens nivå for sporbarhet og autentisitet bibeholdes. Som beskrevet foran vil bruk av elektronisk kommunikasjon normalt medføre generering av elektroniske spor. Sertifikater vil nødvendigvis kunne inneholde personopplysninger som kan knyttes til saksbehandleren eller den enkelte borger. Det er viktig å merke seg at selv om opplysningene er trivielle – eksempelvis kun navn – vil det elektroniske sporet gi viktig informasjon om hvem hvor og når. Sammenstilt med andre spor kan mange enkeltopplysninger utgjøre et personvernproblem i bestemte sammenhenger. Også ansatte i forvaltningen har krav på privatliv. En forvaltningsenhet skal kunne spore hva egne ansatte gjør i en tjenestesituasjon men det er vanligvis ikke slik at de automatisk skal kunne følge alle sporene de ansatte etterlater seg.

Bruk av personlige digitale signaturer tilfører ytterligere et grunnlag for elektronisk sporing. Dette «avtrykket» vil ikke bare avsettes sammen med sporene som etterlates ved selve meldingsoverføringen. Det vil også avsettes i andre situasjoner – eksempelvis ved utstedelse eller verifikasjon av sertifikater. En unik identifikator i et sertifikat gjør det noe enklere å knytte en digital signatur til en person enn ved søk i fri tekst etter navneinformasjon i selve tekstmeldingen. Bruk av personlige digitale signaturer medfører generering av flere elektroniske spor som er lettere tilgjengelig for uvedkommende enn anonyme eller pseudonyme sertifikater.

Det neste spørsmålet som må stilles er om slik generering er uunngåelig. Med utgangspunkt i dagens bruk av underskrift ser det tilsynelatende slik ut: Brev knyttes til den enkelte saksbehandler gjennom underskriften. Mottakers behov er ikke nødvendigvis å bli informert om saksbehandlers navn gjennom den digitale signaturen. Saksbehandlers navn og/eller forvaltningsorganets navn vil framgå av selve meldingsteksten. Det er dermed ikke snakk om «anonym» saksbehandling. Mottakers behov kan være å få visshet om at dokumentet ikke er endret underveis og at eieren av den digitale signaturen faktisk er ansatt i den oppgitte forvaltningsvirksomheten.

Eksempelet viser at digitale signaturer i enkelte sammenhenger ikke trenger å knyttes direkte til person. Det vil være mulig å spore meldingen tilbake til den personen som har signert meldingen hvis det er behov for det. Koplingen mellom signatur og person vil imidlertid være lagret internt i avsenders informasjonssystem. Det er verd å merke seg at all bruk av avsenders informasjonssystem herunder tjenester i eksterne nett skal autoriseres jf. personopplysningsforskriften.

5.3.4 Sikkerhetsnivåer

Sikkerhetsbestemmelsene gitt i medhold av personopplysningsloven pålegger den behandlingsansvarlige å iverksette sikkerhetstiltak i forhold til den risiko behandlingen medfører. Kravet til forholdsmessighet medfører at valg av sikkerhetsnivå og -tiltak må baseres på risikovurdering utført for den enkelte konkrete behandling. Bildet kompliseres ved at personopplysninger skal sikres ut fra forskjellige ofte avvikende hensyn: konfidensialitet integritet eller tilgjengelighet. Eksempelvis vil en for sterk konfidensialitetssikring kunne forårsake utilstrekkelig tilgang til opplysningene og dermed medføre et sikkerhetsproblem.

Dette innebærer at evaluering og valg av sikkerhetsnivå må baseres på en forutgående vurdering av risiko knyttet til den enkelte behandling. Slike risikoanalyser bør ta med vurderinger om hvorvidt systemer som har akseptabelt risikonivå for systemeier gir for høy risiko for den enkelte private bruker.

5.3.5 Fødselsnummer

Fødselsnummer åpner for sporing samtidig som det i visse situasjoner kan være ønskelig eller nødvendig for et enkeltindivid å identifisere seg på en unik måte. De nordiske land er så å si alene om å benytte ett og samme system for identifikasjon av borgere i alle sektorer og bransjer. I denne sammenheng er det interessant å merke seg at Europarådet ved gjennomgang av bruk av «personal identification numbers» i medlemslandene har uttrykt skepsis til systemer tilsvarende vårt. Problemet er selvsagt de muligheter for

kontroll og (utilsiktet) datakopling som oppstår når en borger gjennomgående identifiseres ved bruk av det samme løpenummeret.

I Tyskland benyttes forskjellige identifikasjonssystemer for de forskjellige sektorer: helse sosial justis etc. En slik løsning gir selvsagt praktiske problemer men er valgt nettopp som en sikkerhetsmekanisme mot for stor statlig kontroll av borgerne. Faktisk vil innføring av et universelt identifikasjonssystem oppfattes som grunnlovsstridig i Tyskland. Tyskernes valg av identifikasjonssystem er historisk betinget. Selv om Tyskland i dag er et stabilt demokrati oppfattes separate identifikasjonssystemer som en nødvendig sikkerhetsgaranti. Tilsvarende identifikasjonssystemer med tilsvarende begrunnelse benyttes blant annet i Nederland.

Fødselsnummer er ikke en sensitiv personopplysning jf. personopplysningsloven. Det omfattes som hovedregel heller ikke av uttrykket «noens personlige forhold» jf. forvaltningslovens § 13 om taushetsplikt. Publikum oppfatter imidlertid ofte fødselsnummeret som en «følsom» opplysning blant annet som følge av betraktningene beskrevet foran. En annen viktig grunn er nok at private virksomheter og offentlige myndigheter tilsynelatende har glemt at fødselsnummer er en identifikasjonskode – et løpenummer – og ikke en autentiseringsmekanisme. Fremdeles kan en oppleve at personopplysninger utleveres til den som presenterer seg med navn og fødselsnummer.

Foruten at fødselsnummer er en unik identifikasjonskode gir nummeret også informasjon om vedkommendes alder (fødselsdato) og kjønn (personnummerets tredje siffer). Med mindre den behandlingsansvarlige har saklig behov for kunnskap om vedkommendes alder og kjønn vil bruk av fødselsnummer faktisk gi overskuddsinformasjon.

Hvorvidt fødselsnummer tillates brukt i behandling av personopplysninger avhenger av om den behandlingsansvarlige har saklig behov for slik bruk. Konkret bør minst følgende to spørsmål kunne besvares med ja før fødselsnumre kan benyttes:

- Er det i behandlingen behov for entydig identifikasjon av en enkelt person?
- Skal opplysningene lovlig koples med personopplysninger i andre behandlinger?

I tillegg må den behandlingsansvarlige grundig vurdere bruken av fødselsnumre opp mot den enkeltes behov for personvern. En viktig parameter i slik vurdering er den utbredelsen slik bruk vil få. Dersom bruk av personlige digitale signaturer begrenses til det absolutt nødvendige minimum eksempelvis ved utbredt bruk av «upersonlige» signaturer vil bruk av fødselsnumre i de resterende tilfellene lettere kunne aksepteres. Erstatning av fødselsnummeret med en annen identifikator som er unik i hele landet løser ikke problemet. Utbredt bruk vil fort gjøre denne identifikatoren til et «fødselsnummer nr. 2» og – med unntak for den nevnte overskuddsinformasjonen – resultere i tilsvarende personvernproblemer som beskrevet foran.

Utvalget bemerker samtidig at det i forskriften til personopplysningsloven § 9-2 om forsendelse som inneholder fødselsnummer framgår at: *Postsendinger som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten. Tilsvarende gjelder sendinger som formidles ved hjelp av telekommunikasjon.* Bestemmelsen kan medføre at informasjon om fødselsnumre i sertifikater må konfidensialitetssikres særskilt – for eksempel ved kryptering når slike opplysninger overføres i eksterne datanett. Programvare for signering/verifisering har imidlertid i dag begrensede valgmuligheter for hvilke informasjonselementer i sertifikatet som kan vises for brukeren. De vanlige opplysningene som vises er hvem sertifikatet er utstedt av hvem som er eieren av sertifikatet (navn) og hvor lenge sertifikatet er gyldig. Det gis også muligheter for «andre navn» dvs. et egendefinert alternativt navn (som ofte er e-postadressen til sertifikateieren). Fødselsnummer vil derfor normalt ikke framgå av slike sertifikater – med mindre det spesielt tilrettelegges for det. Det kan derfor synes som om vanlig bruk av digitale sertifikater selv om de inneholder fødselsnummer ikke kommer i strid med forskriftsbestemmelsen. Med tanke på den teknologiske utviklingen bør det likevel ikke legges avgjørende vekt på de begrensninger som følger av dagens programvare. Tvert imot kan det forventes at enhver som i framtiden ønsker tilgang til sertifikatinnehavers fødselsnummer skaffer seg dette gjennom nødvendig programvare.

5.3.6 Elektroniske ID-kort og tillit

Eventuell innføring av et elektronisk ID-kort for alle borgere framhever de problemstillingene knyttet til elektroniske spor og universelle identifikasjonssystemer som er beskrevet foran. Spesielt gjelder dette dersom ID-kortet – tilsiktet eller utilsiktet – tas i bruk i mange sammenhenger. Det er åpenbart mer praktisk å benytte én metode for identifisering i flere anvendelser enn å la borgeren operere med en lang rekke kort legitimasjonsbevis eller andre autentiseringsmekanismer. Innføring av elektroniske ID-kort er ikke kun et valg av praktisk anvendbar teknologi det er også et valg av hvilket samfunn man ønsker å utvikle. Separate identifikasjonssystemer for forskjellige samfunnssektorer kan være upraktisk men utgjør samtidig en sikkerhetsgaranti i forhold til den enkeltes personvern.

Utvikling av tillit er mer enn teknologiske løsninger. Utvalget har ikke som mandat å utrede generelle identitetskort. Dette er et eget tema som eventuelt trenger en grundig drøftelse. Dette gjelder bl.a. i forhold til bruk av identitetskort tidligere i historien.

5.4 Leverandører tjenesteytere og brukere i markedet

Omtalen nedenfor av de største leverandørene og enkelte utvalgte brukere viser noen hovedtrekk i utviklingen.

5.4.1 ErgoGroup

ErgoGroup (tidligere Posten SDS) lanserte sin Elektronisk ID-tjeneste (EID) allerede i 1998. Tjenesten tilbød kundene en elektronisk ID (et sett med personlige digitale sertifikater) plassert i et smartkort. Kortet kunne også tjene som et visuelt ID-kort (Postens ID-kort). På denne måten kunne kunden identifisere seg både fysisk overfor personer og elektronisk overfor datasystemer. Denne tjenesten ble bl.a. tatt i bruk av Norsk Tipping for utstedelse av elektroniske «tippekort». Slike kort inneholder også en elektronisk pengepung for innlasting av spillpenger som kan brukes på de ulike spill som er tilgjengelig fra Norsk Tipping på Internett. Kortene skal prøves i ca. 3000 husstander i første kvartal av 2001. Smartkort med EID benyttes også i Skattedirektoratets pilot på området elektronisk innrapportering av MVA-oppgaver og selvangivelser fra bedrifter. Sertifikatene benyttes for autentisering og signering.

Styret for det industrielle rettsvern (Patentstyret) har lagt inn bestilling på Forvaltningsnettavtalens del for TTP-tjenester og vil benytte smartkort fra ErgoGroup basert på kravene i FSP-1 for så vel ansatte i etaten som for sine kunder oppfinnerne og deres fullmektiger. Prosjektet inneholder dermed digitale signaturer på elektroniske formularer lastet ned fra web foruten bruk av PKI i arkiv- og saksbehandlersystemene.

Etter en beskjeden start har markedet nå etter hvert begynt å benytte PKI-tjenester fra Posten. Dette gjelder først og fremst statlige organisasjoner som Rikstrygdeverket men også private organisasjoner som Storebrand og Falken. Totalt er det utgitt noen tusen smartkort som er i kommersielt bruk.

Tjenesten ble så videreutviklet og er blitt et sentralt element i Postens nye tjeneste ePosten. Denne tjenesten ble lansert i januar 2001. Hovedelementene i denne tjenesten er en standardisert e-postadresse som er unik for hele landet og en elektronisk ID tilknyttet denne unike adressen. Brukeren som vil ta i bruk tjenesten trenger ikke å bytte sin Internett-leverandør – e-post rutes via den standardiserte adressen til hennes vanlige e-postadresse. For å kunne ta i bruk tjenesten må kunden registrere seg online i et eget skjema. Det kreves at kunden oppgir fødselsnummer. Dette brukes til å verifisere opplysningene kunden gir og finne adressen som det skal sendes et engangspassord til. Dette passordet brukt på en spesifikk URL som kunden får oppgitt ved registrering er nødvendig for å kunne ta i bruk EID. Kundens private nøkkel og sertifikat (for autentisering) blir lastet ned og lagret i hennes nettleser på PC-en. Kunden må oppgi PIN-kode hver gang sertifikatet skal brukes mot en Internett-tjeneste. EID vil inneholde brukers navn og den standardiserte eAdressen. Dette åpner for at EID kan benyttes av andre som ønsker å verifisere korrekt bruker. Det er ikke forbundet med kostnader å registrere seg som bruker på ePosten.

EID er nyttig dersom kunden ønsker å ta i bruk tilleggstjenester som eKurer. Dette er en tjeneste for forsendelse av e-post (og annen post for elektronisk levering) på en sikker måte. Posten med ev. dokumenter blir lastet inn på en sikker server og et varsel om dette blir sendt mottakeren via vanlig e-post. Mottakeren kan så benytte sin EID for å logge seg inn på serveren og hente sin post/dokumenter. Avsenderen kan også logge seg inn på serveren og ev. trekke forsendelsen tilbake før mottakeren har hentet

den om det er ønskelig. En slik forsendelsesmåte gir også avsenderen en kvittering/et bevis på at mottakeren faktisk har fått forsendelsen. Både levering og henting av dokumenter via denne tjenesten skjer gjennom en kryptert kanal som hindrer uvedkommende i å få innsyn. Det skal være mulig å kryptere dokumentenes innhold slik at kun mottakeren kan låse det opp. Dokumentene kan også digitalt signeres av ErgoGroup for ytterligere autentisering og sikring av ikke-benekting.

Denne «myke» EID planlegger Skattedirektoratet å ta i bruk i forbindelse med elektronisk innlevering av personlige preutfylte selvangivelser (PSA) i 2001. Ved å benytte ErgoGroups EID til autentisering vil den som innleverer selvangivelsen over Internett kunne redigere innholdet i flere av feltene i selvangivelsesskjemaet enn det som er mulig kun ved bruk av PIN-kode.

5.4.2 Telenor – ZebSign

Telenor har arbeidet med å tilby tjenester knyttet til utstedelse av sertifikater (TTP-tjenester) og digitale signaturer siden begynnelsen av 90-tallet. Allerede i 1995–96 etablerte Telenor sin første TTP-tjeneste til dels basert på egenutviklede komponenter. Denne tjenesten ble erstattet av en ny tjeneste utviklet i samarbeid med PKI-leverandøren Entrust Technologies.

Tjenesten framstår nå som en massemarkedstjeneste hvor ZebSign skal fungere på tvers av PC Internett mobile nett «smart phones» og digital-TV. ZebSign ble lansert høsten 2000 og vil bli lansert på mobil GSM-plattform i 2. kvartal 2001. Hovedmålet med tjenesten er at brukeren skal få en elektronisk ID basert på kvalifiserte sertifikater som fungerer uavhengig av om brukeren betjener for eksempel nettbanken via PC mobiltelefonen eller TV.

Telenor har uttrykt ønske om å bidra aktivt til åpne ID-løsninger på tvers av nettoperatører og TTP-tilbydere. I denne sammenheng vil Telenor bygge videre på bl.a. det arbeidet som er gjort med kryssertifisering i forbindelse med Forvaltningsnettsamarbeidet.

ZebSign-tjenesten på mobil kan tilbys tilnærmet alle abonnenter av Telenor Mobil (unntatt de som benytter anonymt kontantkort). Løsningen for mobil PKI baserer seg på at nøkler og sertifikater lagres i telefonens SIM-kort. De kan så benyttes gjennom bruk av en såkalt SIM-browser en dedikert programvare til bruk på SIM-kortet som gjør det mulig å kople seg opp mot Internett.

Kunden skal registrere seg for bruk av digitalt sertifikat gjennom personlig frammøte hos en registreringsenhet godkjent av Telenor for registrering av brukere i henhold til krav som vil gjelde for kvalifiserte sertifikater.

Telenor har i samarbeid med DnB implementert en autentiseringstjeneste basert på ZebSign-sertifikater for elektronisk handel på markedsplassen DoorStep.

Telenor legger opp til at ZebSign skal kunne tilby kvalifiserte sertifikater og kvalifiserte signaturer iht. lov om elektronisk signatur.

Fordelen med mobil PKI er åpenbart den store utbredelsen av SIM-kort som befinner seg i hver enkelt mobiltelefon. Gjennom beskyttelse av privat nøkkel i et SIM-kort gir mobil PKI god grad av sikkerhet. Mobiltelefonen er godt egnet for signering av mindre datamengder som for eksempel i forbindelse med autentisering og betaling. Mobiltelefonen har på den annen side begrensninger når det gjelder signering av større datamengder som dokumenter og liknende hvor dagens brukergrensesnitt setter begrensninger på type dokument som kan signeres. På litt sikt vil trolig sammensmelting mellom mobiltelefoner håndholdte PC-er (PDA) og PC-er føre til at den «mobile enheten» vil kunne håndtere adskillig større datamengder enn mobiltelefonen klarer i dag. Da kan mobil PKI komme til sin fulle rett også når det gjelder dokumentsignering.

5.4.3 BankID

BankID er betegnelsen på bankenes felles satsning på TTP-tjenester. BankID-prosjektet ble etablert av Bankforeningenes Fellesutvalg i desember 1999. Prosjektets mål var å samordne autentiseringsløsninger som benyttes av norske banker/finansinstitusjoner i forbindelse med nettbank-tjenester. Første fase av prosjektet ble avsluttet høsten 2000 og det er nå etablert en felles operativ PKI.

I fase 1 er det utarbeidet en felles infrastruktur som bl.a. omfatter:

- Policy
- Interbank-regler om BankID
- Mønsteravtale til bruk mellom kunde og bank
- Felles varemerke
- Teknisk infrastruktur
- Standarder og spesifikke regler knyttet til bruk av standardene.

Samarbeidet er organisert på omtrent tilsvarende måte som for den samordnede betalingsformidlingen i Norge og bygger på de gode erfaringer bankene har på dette området.

Det er utviklet en felles sertifikatpolicy for BankID. Policyen legger opp til ett høyt sikkerhetsnivå og forutsetter bruk av tre separate nøkkelpar for hhv. autentisering signering og kryptering. BankID-sertifikatet inneholder et unikt identifikasjonsnummer for hver enkelt BankID-sertifikateier. Nummeret tildeles av hver enkelt bank som utsteder BankID-sertifikater. Nummeret skal kunne inneholde signifikant informasjon om sertifikateieren som for eksempel fødselsdato.

Den tekniske delen av BankID-prosjektet har etablert en rotnode SA hos BBS. Denne utsteder sertifikater til bankenes egne SA som i startfasen også driftes av BBS. Hver enkelt bank vil være ansvarlig sertifikatutsteder for sine egne sertifikater.

BBS har etablert rotnoden som er «sertifisert» (godkjent) av Bankenes Standardiseringskontor (BSK). Det er planlagt at minst 5 banker/bankgrupperinger vil ha etablert sine egne SA i løpet av 2001. Dette vil bl.a. være alle de største bankene i Norge.

BankID er basert på åpne standarder og på at løsningen skal være leverandøruavhengig i størst mulig grad. For å oppnå dette har BBS etablert et BankID Testsenter der ulike leverandørers løsninger skal kunne testes og ev. godkjennes for bruk med BankID. De aktuelle løsninger som kan testes er SA-utrustning klientprogramvare nøkkelbeskyttelsesløsninger («token») og integrasjonsløsninger for ulike komponenter av PKI. Baltimore Technologies er en av de godkjente leverandørene. Andre leverandører vurderes.

Den felles infrastrukturen for BankID utgjør basis for den enkelte banks tilbud av TTP-tjenester i markedet. Infrastrukturen skal sikre at banker kan tilby TTP-tjenester som gjør at kunder kan kommunisere seg imellom på en sikker måte over åpne nettverk uavhengig av bankforbindelse.

I fase 1 skulle BankID sikre elektronisk meldingsutveksling mellom en bank og kunde ved å bekrefte rett identitet til partene (autentisering) sikre innholdet mot endring (integritet) knytte meldingen til en bestemt part (digital signatur og ikke-benekting) og/eller skjule innholdet for uvedkommende (kryptere). BankID vil i første omgang basere seg på et «mykt» sertifikat med private nøkler lagret på brukerens PC. Nøklene skal være beskyttet gjennom en egen «plug-in»-programvare til brukerens nettleser.

De første pilotløsningene for bruk av BankID startet høsten 2000. BankID testes for bruk med utvalgte nettbanker og som sikring av e-postkommunikasjon. Videre arbeider BBS med å integrere BankID i sin eFaktura-tjeneste som skal tilbys nettbankbrukere i 2001.

I fase 2 er BankID utvidet til å omfatte TTP-tjenester for elektronisk kommunikasjon direkte mellom alle norske bankers kunder. BankID tar nå i bruk «harde» sertifikater med private nøkler lagret på chip (for eksempel smartkort og SIM-kort). Et nettsted som er sertifikatbruker behøver kun å inngå avtale med sin egen bankforbindelse for å sikre at alle kunder med BankID fra andre banker kan benytte BankID i forbindelse med bruk av etatens tjenester. Bankforbindelsen vil også kunne tilby for eksempel betalingstjenester sikret med BankID.

Man ser for seg BankID som en mulig felles ID for bedrifter som ønsker å benytte elektroniske markedsplasser myndigheter som vil tilby elektroniske tjenester til enkeltpersoner m.fl.

Interbank-reglene for BankID sier at første gangs utlevering av BankID til bankkunden skal skje ved personlig frammøte i banken eller hos en som utstederbanken har inngått avtale med om kontroll av bankkundens identitet. Den som utstederbanken inngår avtale med skal nyte god tillit i markedet. Dersom banken finner det nødvendig samt ved fornyelse av BankID kan BankID også utleveres på annen måte som gir tilsvarende sikkerhet. Dette kan for eksempel skje ved at eksisterende kunder som benytter nettbank og

dermed allerede innehar en sikker autentiseringsmetode kan få tilsendt sitt BankID smartkort via posten mens tilhørende PIN-kode kan hentes etter pålogging i nettbanken.

Bankene har etablert sikre rutiner for å forvisse seg om kunders identitet og er også gjennom lover og regler pålagt markedets strengeste krav til identifisering og kontroll av kunden på det tidspunkt et kundeforhold opprettes. I tillegg har bankene lovpålagt ansvar knyttet til eventuelt misbruk av bankkonti i henhold til finansavtaleloven. Dette gir bankene et spesielt godt utgangspunkt for utstedelse av en sikker digital ID.

5.4.4 Store brukere – Norsk Hydro og Statoil

Norsk Hydro med sine 19 000 ansatte over hele verden har behov for en robust og sikker kommunikasjonsinfrastruktur mellom de ulike delene av konsernet og mellom de enkelte ansatte.

Norsk Hydro har utviklet en PKI-strategi siden 1998. Strategien er forankret i Information Systems (IS) – staben til konsernledelsen. En egen enhet er opprettet for dette formål. Enheten er Hydros «service supplier» når det gjelder PKI. Enheten har i oppgave å vurdere tilgjengelige løsninger stille krav inngå avtaler og godkjenne de leverte løsningene. Enheten utvikler også PKI-policy for hele konsernet.

Implementeringsprosjektet for PKI i Hydro er forankret i «Hydro Bridge» som er Norsk Hydros infrastruktur for IT og kommunikasjon.

I 2000 inngikk Norsk Hydro en større kontrakt med Telenor for leveranse av Entrust Technologies' PKI-løsninger for oppbygging av konsernets PKI. Leveransen blir godkjent etter at en pilotinstallasjon blir testet og godkjent.

Det er ulike piloter med bruk av PKI som gjennomføres nå. En av dem er tilgang til Hydros interne bank via en web-basert nettbankløsning. Andre piloter involverer bl.a. støtte til elektronisk innkjøp og sikker e-post basert på verktøyet Lotus Notes (Domino).

Det er opprettet en sentral registreringsenhet i Norsk Hydro som er koplet opp mot Telenors sertifikatutsteder-tjeneste. Det er utpekt en sertifikatansvarlig i hver forretningsenhet i Norsk Hydro som har ansvaret for å samle opp og levere registreringsforespørsler til registreringsenheten. Hvert sertifikat som utstedes er et ansattsertifikat som inneholder en unik identifikator ansattnummeret. Utstedelse av sertifikater foregår i samspill med Hydros sentrale X.500-kataloger som inneholder informasjon om alle ansatte. Private nøkler og sertifikater lagres i brukernes PC. Hydro har foreløpig ingen planer om å gå over til smartkort-baserte sertifikater.

I november 2000 satte Norsk Hydro i gang testing av WebBank-løsningen med 35 prøvebrukere som ble utstyrt med sertifikater. Resultater fra bl.a. denne testingen skal avgjøre videre utplassering av PKI i konsernet.

Statoil som har liknende kommunikasjonsinfrastruktur planlegger også å innføre PKI til støtte for sikker informasjonsutveksling og -tilgang. Ved slutten av 2000 var konsernet i ferd med å utvikle detaljerte planer for dette.

6 Oversikt over PKI-politikker for offentlig sektor i utvalgte OECD-land

Dette kapitlet er skrevet hovedsakelig på grunnlag av et to dagers møte med representanter for de land som omtales (Australia deltok ikke) gjennomført i Oslo i mai 2000 [3]. Opplysningene har siden blitt komplettert ved å gjennomgå relevante rapporter og utredninger fra enkelte land. Omtale av hvert land er forsøkt strukturert etter følgende kriterier:

- Sentrale tiltak i forvaltningen
- PKI for eksterne tjenester til brukere
- Lovgivning og andre tiltak.

6.1 Sverige

Den svenske interesseorganisasjonen SEIS[8]har i flere år arbeidet med utvikling av PKI-standarder.

Sentrale tiltak i forvaltningen

I 1999 ble det etablert sentrale rammeavtaler for elektroniske ID-kort og andre typer sertifikater for forvaltningen. Avtalene forvaltes av Statskontoret. Det har til nå vært relativt lite salg i forbindelse med rammeavtalene men dette har tatt seg opp i den seinere tid. Avtalene varer fram til 1.8.2001. Selv om de i utgangspunktet er forbeholdt staten har flere kommuner sluttet seg til ordningen på individuell basis og anskaffet seg løsninger. De anvendelser som er kommet i gang gjelder sykehus og helse allterminalkort som skiftes ut kommunale tjenester (Stockholm kommune) og elektronisk bilregistrering (Vegvärket).

Den svenske forvaltningen satser på PKI som hovedinfrastruktur for autentisering både innad i forvaltningen og mot forvaltningens brukere. Den svenske forvaltningen planlegger å etablere en rekke elektroniske tjenester på ulike områder som skatt sykeforsikring arbeidsmarked studielån og eiendomsregister.

PKI for eksterne tjenester til brukere

Ulike utredninger på PKI-området konkluderer med at det bør opprettes et felles statlig organ (utredningen benevner dette CA = Certification Authority men man mener egentlig et organ for koordinering av utbygging av en offentlig PKI) som skal få i oppgave å sørge for at enkeltpersoner blir utstyrt med sertifikater til bruk i elektroniske offentlige tjenester. Oppgaven foreslås lagt til Riksskatteverket. Det anbefales tre grunnleggende sikkerhetsnivåer som man ser behovet for i transaksjoner med forvaltningen. Det høyeste nivået tilsvarer kvalifiserte signaturer/sertifikater i samsvar med EU-direktivet. Mellomnivået er også et nivå der PKI-tjenester skal utnyttes men med lempeligere krav til nøkkelbeskyttelse. Laveste nivå tenkes knyttet til bruk av PIN-koder og passordbasert autentisering.

Statens CA skal få følgende oppgaver:

- Utvikle og forvalte den statlige sertifikatpolicyen. Dette innebærer utforming av tekniske krav sertifikatformater m.m. samt utvikling av et avtaleverk for bruk av PKI.
- Ha ansvaret for godkjenning av sertifikatleverandører som skal kunne levere til staten eller statens brukere gjennom rammeavtaler.

8

www.seis.se (SEIS – Sikker Elektronisk Informasjon i Samfunnet).

- Samordne aktiviteter innenfor anvendelse av PKI i forvaltningen herunder håndtering av tilgangen til tilbaketrekkingslister og i samarbeid med Statskontoret gjennomføre anskaffelsesprosesser.
- Markedsføre og informere om den sentrale infrastrukturen.

Man ser for seg at Statens CA skal kunne inngå to typer rammeavtaler:

- Rammeavtale med sentrale aktører som allerede benytter PKI mot sine kunder som f.eks. bankene eller posten. Avtalen innebærer at staten betaler for bruk av signerings- og autentiseringstjenester. Staten vil trolig betale pr. transaksjon i en slik ordning.
- Rammeavtale om produkter og tjenester. Dette tilsvarer dagens rammeavtaler men der også sertifikater for borgere og bedrifter vil kunne kjøpes. Her vil betalingsmodellen være en årlig pris pr. sertifikat.

I forhold til begge avtalene er de PKI-anvendelser som tenkes støttet autentisering signering og kryptering av sesjonsnøkler. Svenske myndigheter ser foreløpig liten anvendelse av PKI for dokumentkonfidensialitet.

Lovgivning og andre tiltak

Arbeidet med statlig sertifikatpolicy er påbegynt. Denne skal baseres på ETSI-standardutkastet til QCP (Qualified Certificate Policy). Svenske myndigheter vurderer også om et tjenestesertifikat vil kunne brukes som borgersertifikat. Det er ønskelig å se en praksisutvikling først før man fatter sentrale beslutninger på dette området.

EU-direktivet blir implementert i svensk lovgivning som en egen lov om elektroniske signaturer med innhold svært nær den norske loven. For øvrig er det ingen planer i Sverige om å innføre en generell lovgivning for elektronisk kommunikasjon. Tilrettelegging for dette skal skje innenfor rammen av eksisterende regelverk.

6.2 Danmark

Sentrale tiltak i forvaltningen

Forskningsministeriet (FSK) i Danmark koordinerer arbeidet med bruk av digitale signaturer i offentlig forvaltning. FSK har støttet 8 pilotprosjekter med 15 mill. DKK. Prosjektene ble gjennomført i perioden høsten 1998–våren 2000 og evaluert sommeren 2000. Rapporten konkluderer med at målene med dette initiativet å stimulere til at digitale signaturer blir tatt i bruk i offentlig sektor i Danmark og å bidra til utviklingen av det danske markedet for digitale signaturer ble nådd. Men det gjenstår en del spørsmål og problemstillinger som må løses. Det var også et mål for satsingen at den skulle stimulere til utvikling av nødvendige standarder.

Prosjektene spente over et vidt spekter av elektroniske tjenester fra innrapportering av årsberetninger og regnskaper til Erhvervs- og Selskabsstyrelsen til elektronisk behandling av byggetillatelser og eiendomsopplysninger i Vordingborg kommune.

Flere av pilotprosjektene skal gå over i driftsfase og de etablerte løsninger implementeres i større skala. Flere av prosjektene ser på utbredelse av sluttbrukerutstyr f.eks. kortlesere som en kritisk faktor for fortsatt utbredelse av PKI. Utstyret må i startfasen finansieres av det offentlige. Kommunenes Landsforening (KL) har derfor tatt til orde for at det bør utvikles en offentlig strategi for utbredelse av digital signatur i forbindelse med selvbetjente elektroniske tjenester fra det offentlige. Arbeidet er satt i gang i regi av Koordinerende Informasjonsutvalg under Forskningsministeriet. Kommuner og fylker deltar også i arbeidet.

Leverandører til pilotprosjektene har i samarbeid med det danske standardiseringsforbundet etablert et Forum for Digital Signatur. Forumet har drevet videreutvikling av standardene som lå til grunn for pilotprosjektene. Det har bl.a. utviklet en standard for koding av personnumre i sertifikater. Videre ble det i regi av forumet utarbeidet en standard for innholdet i sertifikater og profil for smartkort.

Erfaringer fra pilotprosjektene berører arkivering av elektroniske dokumenter med eller uten digitale signaturer. I dag arkiverer Statens Arkiv elektroniske dokumenter uten digitale signaturer og i en ikke-kryptert form. Erfaringene tilsier at brukere av offentlige tjenester helst vil benytte ett sertifikat mot flere tjenester. Dette krever at samtrafikken mellom de ulike sertifikatutstedere (de kalles nøkkelsentre) må løses. Det kan gjøres enten gjennom gjensidig kryssertifisering eller ved at myndigheter inngår spesielle avtaler med alle nøkkelsentre eller at det etableres en sentral enhet (en bro) som skal sørge for samspillet mellom dem.

Det danske IT-Sikkerhetsrådet har utviklet retningslinjer[9]for praktisk bruk av kryptering og digitale signaturer. Disse retningslinjene behandler bl.a. spørsmålet om deponering av kopier av private krypteringsnøkler.

PKI for eksterne tjenester til brukere

I oppfølgingen av pilotprosjektene har FSK slått fast at det ikke ser behov for etablering av offentlige sertifikatutstedere heller ikke at det offentlige sentralt skal yte økonomisk støtte til utplassering av utstyr hos befolkningen. På samme tid oppfordres offentlige virksomheter til utvikling av egne forretningsmodeller for elektroniske tjenester der man ut fra et kost-/nytteperspektiv kan tenke seg å støtte brukere økonomisk dersom innsparingen på myndighetenes side er så stor at den rettferdiggjør dette. Samtidig arbeider det tidligere nevnte koordineringsutvalget med PKI-strategi som skal omfatte:

- Retningslinjer for web-baserte grensesnitt til elektroniske tjenester
- Klassifisering av sikkerhetsnivåer og retningslinjer for bruk av kryptering og digital signatur
- Utarbeidelse av grunnlaget for en offentlig anskaffelsesprosess rammeavtaler som skal dekke produkter og tjenester for offentlig elektronisk informasjonsutveksling.

Det forventes at rammeavtaler skal inngås våren 2001.

Lovgivning og andre tiltak

De danske myndigheter poengterer behovet for informasjonskampanjer om bruk av digitale signaturer der målet skal være at befolkningen skal bli like fortrolig med denne teknologien som med bruk av bankkort og EFTPOS-terminaler i butikkene.

Nye offentlige initiativer i Danmark omfatter flere forslag til etablering av elektroniske tjenester fra forvaltningen. Disse er beskrevet i rapportene *Det digitale Danmark* og *Netværkssamfundet*. Flere av disse initiativene forutsetter eller vil ha nytte av digitale signaturer.

Danmark utarbeidet forslag til ny lov om digitale signaturer på grunnlag av EU-direktivet og delvis på grunnlag av erfaringer fra gjennomførte pilotprosjekter. Loven ble vedtatt den 31.5.2000. Den regulerer driften av nøkkelsentre (sertifikatleverandører) og gir digitale signaturer rettsvirkning i samsvar med direktivet.

6.3 Finland

Sentrale tiltak i forvaltningen

---

9 *Praktisk brug af kryptering og digital signatur*. http://www.fsk.dk/fsk/publ/2000/praktiskbrug/praktiskbrug.pdf

Finske myndigheter har i de siste årene fått vedtatt en rekke lover som la grunnlaget for etablering av en nasjonal løsning for elektronisk identitet/elektronisk signatur som skal kunne brukes i forbindelse med elektroniske tjenester fra forvaltningen. Løsningen baserer seg på elektroniske ID-kort (et visuelt identitetskort preget på et smartkort med digital signatur og identitet i kortet). I november 2000 utstedte de sentrale myndigheter en forordning om å ta i bruk elektroniske identitetskort for alle tjenestemenn i finsk forvaltning. Kortene kan skaffes via den sentrale ordningen eller hos andre tilbydere i markedet.

PKI for eksterne tjenester til brukere

Det første elektroniske ID-kort fra folkeregisteret ble utstedt til presidenten i det finske parlamentet den 7.12.1999. Kortene utstedes i samarbeid med politiet som forestår registrering og utlevering av kort. Kortet er samtidig et visuelt identitetskort som følger EU-standarden. Det kan derfor fungere som forenklet passdokument ved grensepassering i alle land som er medlemmer i Europarådet. Kortet kostet i 2000 ca. 180 FIM.

Det er til nå utstedt ca. 6–7000 slike elektroniske ID-kort. Utstedelseshyppigheten har sunket etter de første månedene tjenesten har vært i drift. Dette skyldes primært mangelen på elektroniske tjenester som støtter bruken av kortet. Utviklingen hos finske offentlige etater har på dette området gått langsommere enn ventet. Folkeregisteret har derfor startet forhandlinger med banksektoren i Finland som viser stor interesse for kortene og vurderer avtaler der kortene skal kunne benyttes som autentiseringsmetode for nettbanktjenester. I den forbindelse arbeider folkeregisteret også med muligheter for å utstede sertifikater til bruk i mobiltelefoner med nøkler lagret på SIM-kort eller eget innstikkskort.

Den finske forvaltningen har definert tre sikkerhetsnivåer for utstedelse av sertifikater:

- Grunnleggende nivå for intern bruk. Dette skal tilsvare EU-direktivets kvalifiserte sertifikater men også sertifikater av lavere sikkerhetsnivå.
- Grunnleggende nivå for virksomhet-til-virksomhet-transaksjoner og transaksjoner mellom virksomhet og enkeltpersoner tilsvarer kvalifiserte sertifikater.
- Utvidet nivå som tilsvarer EID-kort. Det tilsvarer sertifikater med høyere sikkerhetskrav enn kvalifiserte sertifikater slik det er åpning for i direktivets artikkel 3.7.

Pr. i dag er sertifikater utstedt i det private markedet ikke akseptert som sertifikater til bruk mot offentlige myndigheter. Dette kan endre seg når lov om elektronisk signatur trer i kraft.

Eksempler på elektroniske tjenester i Finland som støtter bruk av digital signatur er bl.a. elektronisk melding til folkeregisteret om adresseendring elektronisk levering av patentsøknader og elektronisk levering av selvangivelse fra bedrifter og andre virksomheter.

Lovgivning og andre tiltak

Lov om elektroniske ID-kort legger opp til at slike kort skal benyttes i forbindelse med offentlige elektroniske tjenester. En modifikasjon av lov om folkeregister ga det nasjonale folkeregisteret i oppgave å forestå utstedelse av elektroniske identitetskort til befolkningen. Videre innfører man et nytt unikt identifikasjonsnummer (FINUID) for personer spesielt til bruk i sertifikater i kortene. Nummeret skal være helt forskjellig fra det nasjonale personnummer og det skal kunne lagres i det sentrale folkeregisteret på linje med andre befolkningsdata. Disse reguleringene trådte i kraft 1.12.99. Videre trådte lov om elektroniske tjenester i forvaltningen i kraft den 1.1.2000. Loven regulerer elektronisk kommunikasjon innad i forvaltningen samt mellom forvaltningen og enkeltpersoner/bedrifter herunder bruk av digitale signaturer og sertifikattjenester for dette formålet. Lov om elektronisk signatur som er en implementering av EU-direktivet forventes å bli vedtatt våren 2001.

6.4 Storbritannia

Sentrale tiltak i forvaltningen

Det sentrale PKI-initiativet gjennomført innenfor den britiske forvaltningen ble kalt «Cloud Cover». Dette initiativet hadde som mål å sikre at offentlige virksomheter skal ha adgang til bredest mulig utvalg av sikre interoperable og kostnadseffektive løsninger for intern innføring av PKI. For dette formålet ble det bl.a. etablert en sentral sertifikatutsteder for forvaltningen hos CESG (Communications Electronics Security Group) ekvivalent av FO/S i Norge. Alle større offentlige virksomheter skal etablere egne sertifikattjenester basert på anskaffelser. Det blir utviklet krav til nødvendige produkter på sentralt nivå. CESG skal evaluere sikkerheten i kryptografiske moduler i slike produkter. Mindre virksomheter vil kunne få utstedt sertifikater direkte fra CESG. Det skal også etableres sentrale sertifikatkataloger som skal være tilgjengelig i GSI (Government Secure Intranet) som dekker 65 offentlige virksomheter.

Arbeidet fra Cloud Cover videreføres i en rekke tiltak. Disse omfatter interoperabilitetstester mellom mange leverandører sårbarhetsvurderinger av PKI samt utvikling av rutiner og prosedyrer knyttet til den sentrale sertifikatutsteder.

PKI for eksterne tjenester til brukere

Information Age Government (IAG) er den politiske rammen for en rekke tiltak som skal føre til at innen 2005 skal alle offentlige tjenester i Storbritannia være tilgjengelige elektronisk. For å legge til rette for det ble det utarbeidet en rekke sentrale retningslinjer herunder retningslinjer for autentisering som inneholder definisjoner av nødvendige sikkerhetsnivåer for ulike elektroniske tjenester. Det er definert fire sikkerhetsnivåer avhengig av graden av sårbarhet samt mulige tap som følge av sikkerhetsbrudd. De to høyeste sikkerhetsnivåene skal støttes av PKI-løsninger.

Den britiske forvaltningen satser på en felles løsning for autentisering av brukere av offentlige elektroniske tjenester. Denne løsningen baserer seg på en felles portal til det offentlige «UK Online» der funksjoner for autentisering skal være integrert. Både ID-/passord-baserte løsninger og PKI-basert autentisering skal være tilgjengelig. Sertifikater som skal benyttes må være godkjent under såkalt tScheme som er en frivillig godkjenningsordning for leverandører av sertifikater i det britiske markedet. tScheme har utarbeidet en rekke krav og kriterier for sikre tiltrodde tjenester.

UK Online-portalen skal være hovedinnfallsporten til offentlige elektroniske tjenester. På sikt skal direkte tilgang til etaters web-baserte tjenester sperres slik at all kommunikasjon vil ledes via portalen. Konfidensialitetsbeskyttelse skal ivaretas av SSL-krypterte forbindelser. Portalen skal inneholde funksjoner for kvitteringer og revisjonssporing av transaksjoner mellom borgere/bedrifter og forvaltningen. Selv om det legges opp til sentralisert autentisering av brukere av de ulike offentlige tjenester kan hver enkelt etat definere eventuelle tilleggsordninger for større sikkerhet mot deres systemer. Dette kan inkludere krav til tilleggsopplysninger for å kunne fastslå unik identitet. Britisk forvaltning benytter ikke noen felles unik identifikator for fysiske personer.

Lovgivning og andre tiltak

Offentlige virksomheter må selv finansiere sine PKI-relaterte aktiviteter. Disse befinner seg nå i hovedsak på pilotprosjekt- og planleggingsstadiet. Virksomheter kan søke midler for dette arbeidet fra en sentral bevilgning til IAG.

Den britiske lovgivningen anerkjenner juridisk bevisverdi ved elektroniske signaturer gjennom lov om elektronisk kommunikasjon. Loven regulerer ikke tilbydere av sertifikattjenester direkte. Dette overlates foreløpig til markedet gjennom tScheme-ordningen. Representanter for forvaltningen sitter i styret for tScheme.

6.5 Nederland

Den nederlandske forvaltningen planlegger å ha 25 % av offentlige tjenester tilgjengelig elektronisk innen utgangen av 2002. For å oppnå dette og målsettingen om effektiv elektronisk forvaltning ser man for seg en PKI-basert infrastruktur for sikkerhet ferdig utbygget mot slutten av 2002.

Sentrale tiltak i forvaltningen

I januar 2000 etablerte den nederlandske regjeringen en arbeidsgruppe (task force) med navnet PKI Overheid (PKI for forvaltningen). Arbeidsgruppens mandat på kort sikt er å etablere en begrenset PKI for intern bruk i forvaltningen mot slutten av 2000. Dette innebærer bl.a. utarbeidelse av en felles

sertifikatpolicy med ett sikkerhetsnivå som vil passe til de fleste administrative behov forvaltningen kan ha. Det skal også foreslås standarder for navngiving og identifisering av sertifikateiere.

Den nederlandske forvaltningen ser ikke behovet for mange ulike sikkerhetsnivåer. Man anslår at 75 % av alle anvendelser både innenfor forvaltningen og mellom forvaltningen og dens brukere vil kunne dekkes av ett sikkerhetsnivå. De resterende 25 % vil trolig kreve spesielle løsninger som kan gi adekvat beskyttelse til gradert informasjon. Man ser for seg samme type sertifikat både for forvaltningen internt og for enkeltpersoner/bedrifter. Private nøkler skal beskyttes i smartkort.

PKI for eksterne tjenester til brukere

Forvaltningen vurderer også muligheter for godkjenning av sertifikater utstedt av andre enn det offentlige. Bankene er en nærliggende samarbeidspartner i så måte. Det har imidlertid vært uttrykt tvil om registreringsprosessen i bankene er god nok for å godta sertifikater utstedt av bankene til bruk i offentlige tjenester.

Et begrenset antall prøveprosjekter innenfor områdene skatt arbeidsledighetstrygd sosialstøtte og «elektronisk borgerkort» med bruk av PKI-løsninger er gjennomført så langt. Det planlegges å sette i drift en løsning for elektronisk levering av selvangivelse fra bedrifter i løpet av 2001. Denne løsningen skal benytte PKI for sikkerhet.

Lovgivning og andre tiltak

Nederland har en etablert frivillig godkjenningsordning for leverandører av sertifikattjenester TTP.NL. Det er likevel ingen stor utbredelse av sertifikatbruk i det private markedet. Man ser forvaltningen som et viktig «lokomotiv» for bruk av PKI-løsninger og som en stimulator for markedsutviklingen på området.

Nederland implementerer EU-direktiv om elektroniske signaturer gjennom en ny lovgivning. I den forbindelse vil det bli etablert en tilsynsordning for leverandører av sertifikater som vil være forskjellig fra TTP.NL.

6.6 USA

Sentrale tiltak i forvaltningen

Den føderale forvaltningen etablerte i 1998 Federal PKI Steering Committee en interdepartemental gruppe med oppgaven å koordinere PKI-aktiviteter i amerikansk forvaltning. FPKISC har fått utarbeidet en rekke retningslinjer felles sertifikatpolicy og ordninger for samtrafikk mellom etatenes PKI-er. Sommeren 2000 etablerte man i tillegg et sentralt organ kalt Federal PKI Policy Authority (FPKIPA). FPKIPA er etablert under Federal Chief Information Officers Council (FCIOC).

Hver offentlig etat i USA kan fritt anskaffe produkter og tjenester for å etablere sin egen sertifikatutstederfunksjon. Samtrafikkspørsmålet skal løses gjennom en sentral brofunksjon (Federal Bridge Certificate Authority FBCA). Det er blitt utarbeidet en sertifkatpolicy for FBCA. Denne støtter fire ulike sikkerhetsnivåer – basis grunnleggende mellomnivå og høynivå. Etatene forventes å kryssertifisere mot FBCA. Bruk av FBCA er ikke obligatorisk men det antas at de fleste etater vil benytte seg av den. FBCA vil også ha ansvaret for drift av en sentral katalogtjeneste som vil inneholde alle kryssertifiserte etater. Broen drives av General Services Agency (GSA) som på noen områder tilsvarer vår egen Statens forvaltningstjeneste.

Sertifikatene benyttes hovedsakelig til autentisering og signering. Kryptering basert på PKI er lite utbredt i amerikansk forvaltning.

Flere offentlige etater som Department of Defense Federal Aviation Authority NASA m.fl. har fått utstedt betydelige mengder sertifikater for sin interne bruk. Det planlegges også å utstede sertifikater for bruk i informasjonsutveksling mellom offentlige myndigheter.

Det ble i juni 2000 publisert en egen rapport[10]som beskriver den amerikanske forvaltnings PKI-arbeid.

PKI for eksterne tjenester til brukere

For borgere skal en spesiell type sertifikater utstedes under sentrale rammeavtaler som forvaltes av GSA. Disse sertifikatene kalles ACES (Access Certificates for Electronic Services). Etatene kan kjøpe sertifikater for brukere av deres elektroniske tjenester. Den amerikanske trygdeetaten vil bli en av de første storskalabrukerne av disse rammeavtalene. Målet er at ca. 100 000 enkeltpersonerssertifikater skal være utstedt ved slutten av 2000. Det forventes at et ACES-sertifikat vil koste ca. 20 USD og at det vil være gyldig i 6 år. Etatene skal betale både for utstedelsen av sertifikatet og for transaksjonskostnader knyttet til bruken av sertifikatene (f.eks. oppslag i sperrelister). Slike transaksjonskostnader estimeres til ca. 0 40 til 1 20 USD avhengig av transaksjonsvolum.

Det forutsettes at registreringsprosessen for ACES skal skje online. Brukeren skal generere sitt eget nøkkelpar og så sende den offentlige nøkkelen til den relevante etaten som vil utstede brukerens sertifikat. Sertifikatet vil bli lastet ned i brukerens nettleser. Kun sertifikater for autentisering og signering vil bli utstedt. (Den amerikanske forvaltningen benytter ett sertifikat for begge formål.) Konfidensialitetsbeskyttelse i kommunikasjon med det offentlige skal ivaretas av SSL.

Av hensyn til personvernet vil ACES-sertifikater kun inneholde en brukers fulle navn. Den første gangen brukeren benytter sertifikatet mot en etats elektroniske tjeneste vil etaten autentisere vedkommende ved å innhente en rekke tilleggsopplysninger som identifiserer brukeren unikt for seinere transaksjoner.

Lovgivning og andre tiltak

GPEA (Government Paperwork Elimination Act) satt ut i livet i oktober 1998 og ESIGN (Act on Electronic Signatures in Global and Interstate Commerce) vedtatt i juni 2000 er de to føderale lovene som omhandler elektronisk signatur.

GPEA krever at offentlige virksomheter skal kunne motta dokumenter og skjemaer elektronisk. Det settes frist til 2003 for skjemaer som har volum over 50 000 pr. år. Videre gir loven full rettslig virkning til elektroniske signaturer brukt i forbindelse med kommunikasjon med og i forvaltningen. Loven tillater også elektronisk lagring av forvaltningens dokumenter.

ESIGN-loven gir rettslig virkning til alle elektroniske signaturer brukt i transaksjoner mellom private parter utenom forvaltningen. Loven gir elektroniske dokumenter samme status som de papirbaserte i slike transaksjoner.

6.7 Canada

Canada er et foregangsland når det gjelder bruk av PKI i offentlig sektor. I 1993 ble det tatt en strategibeslutning om å etablere en forvaltnings-PKI for sikker elektronisk informasjonsutveksling og sikre transaksjoner.

Sentrale tiltak i forvaltningen

GOL (Government Online) initiativet i den føderale kanadiske forvaltningen har som mål at alle viktige tjenester skal være tilgjengelig elektronisk innen 2004. Også delstatsforvaltninger ser PKI som en viktig infrastruktur for leveranse av elektroniske tjenester til sine borgere.

Den sentrale enheten som forvalter PKI-politikk er TBS (Treasury Board Secretariat). Det er utviklet et PKI-rammeverk som omfatter modell for sertifikatpolicy metodologi for kryssertifisering og policy for elektronisk autentisering og autorisasjon.

10

The evolving federal PKI. http://gits-sec.treas.gov

Hver offentlig virksomhet skal etablere sin egen sertifikatutstederfunksjon. Virksomhetene skal kryssertifisere mot en sentral sertifikatutsteder som drives av Canadian Central Facility (CCF) en ekvivalent til FO/S i Norge. I tillegg opererer GTIS (Government Telecommunications and Information Services) en felles katalogtjeneste.

Det er etablert en koordinerende komité for PKI-aktiviteter Policy Management Authority. Denne komiteen rapporterer til TBS når det gjelder utviklingen og oppfølgingen av forvaltningens PKI-politikk. Alle forespørsler om kryssertifisering med CCF skal være godkjent av PMA den skal også godkjenne avtaler med parter utenfor forvaltningen som ønsker å kryssertifisere med CCF. Det er til nå gjennomført 4 kryssertifiseringer. Det er planer om å kryssertifisere CCF med det kanadiske bankvesenets felles sertifikatløsning i 2001.

Den sentrale sertifikatpolicy-modellen støtter fire sikkerhetsnivåer[11]med 2 nøkkelpar for hvert nivå (ett for digitale signaturer og ett for kryptering). Dette avstedkommer åtte ulike varianter av policy. Private krypteringsnøkler for offentlig ansatte skal kopieres til et nøkkeldeponi for å kunne hentes fram ved eventuelt tap av nøkkel.

PKI for eksterne tjenester til brukere

Den kanadiske forvaltningen har siden 1998 gjennomført et program (Pathfinder) som omfatter en rekke prosjekter for implementering av elektroniske tjenester med støtte i PKI. Programmet omfatter ca. 17 ulike prosjekter som bl.a. omfatter elektronisk registrering av nye selskaper informasjonsutveksling i helsenettverk sikker meldingsutveksling i sentralforvaltningen osv. Prosjektene er beskrevet i rapporter publisert på web.[12]

Erfaringer fra dette programmet peker bl.a. på behovet for å utvikle en «business model» for bruk av PKI behovet for sårbarhetsanalyser i forbindelse med anvendelse av PKI behovet for samarbeid ved implementering av PKI og behovet for å legge stor vekt på informasjon og kunnskapsformidling om PKI.

Strategi for PKI-støttet kommunikasjon med enkeltpersoner er nå under utvikling i den kanadiske forvaltningen. Strategien baserer seg på bruk av standard nettlesere med «plug-in» levert av forvaltningen. Private nøkler forventes lagret på en maskinvareenhet (token) og registrering skal foretas online med nødvendig hensyn til personvernspørsmål. Rammeverket for autentisering mot elektroniske offentlige tjenester utelukker ikke bruken av PIN-koder/passord. Slike løsninger skal likevel primært benyttes i «engangs-transaksjoner» med forvaltningen og ikke for flergangsbruk.

Lovgivning og andre tiltak

Det utvikles også retningslinjer for langtidslagring av elektroniske dokumenter som er blitt signert digitalt. Det vurderes bl.a. om verifikasjonsspor kan lagres sammen med dokumentet istedenfor selve signaturen.

Det kanadiske rettslige rammeverket for elektroniske tjenester er sammenfattet i Personal Information Protection and Electronic Documents Act. Loven regulerer elektroniske transaksjoner og autentisering generelt og er ikke spesielt rettet mot PKI.

11

Se beskrivelse av USA.

12

http://www.cio-dpi.gc.ca/pki/pki_index_e.html

6.8 Japan

Sentrale tiltak i forvaltningen

Den japanske forvaltningen legger opp til at hvert enkelt departement og underliggende virksomheter skal være egne utstedere av sertifikater. Det skal etableres en sentral bro (Bridge CA) for krysssertifisering av de ulike etaters løsninger. Broløsningen skal være på plass innen mars 2001. Denne oppgaven skal utføres av Koordinerings- og forvaltningsetaten under Statsministerens kontor. Broløsningen skal også benyttes for krysssertifisering av forvaltningens PKI med privat sektor og også med forvaltnings-PKI-er i andre land. Det er utviklet en generell sertifikatpolicy for forvaltningens PKI. Policyen baserer seg på ett felles sikkerhetsnivå.

Etablering av sertifikatutstedere i departementer og underliggende virksomheter skal være avsluttet i løpet av 2003/våren 2004. Noen departementer skal være pilotvirksomheter med etablert PKI våren 2001.

Spesifikasjoner for de nødvendige løsninger utarbeides i løpet av 2000 av Interdepartementalt Råd for IT i forvaltningen. Videre skal Rådet utvikle kriterier for evaluering av sikkerhet i nødvendige produkter og retningslinjer for deres anskaffelse. Departementer og underliggende virksomheter skal fritt kunne velge hvilke produkter de ønsker å kjøpe innenfor rammen av retningslinjer gitt av Rådet for IT i forvaltningen.

PKI for eksterne tjenester til brukere

Den japanske regjering har besluttet å innføre «papirløs» forvaltning i løpet av 2003. Rammebetingelser for dette tiltaket er sammenfattet i en handlingsplan som ble vedtatt i desember 1997.

Elektroniske tjenester til borgere skal baseres på en offentlig PKI (GPKI). Denne infrastrukturen skal kunne brukes til autentisering av både borgere og offentlige virksomheter.

Forvaltningen ønsker i samarbeid med banksektoren å utvikle løsninger for elektronisk betaling av offentlige avgifter. Et slikt system skal støttes av PKI. Systemet skal være i funksjon i løpet av 2003.

Lovgivning og andre tiltak

Det er etablert et forum for PKI i forvaltningen der også leverandører deltar. Formålet med forumet er å utveksle erfaringer når det gjelder teknologivalg og innføring av PKI-løsninger.

Det japanske parlamentet har vedtatt en lov om elektroniske signaturer som skal tre i kraft i april 2001. Loven likestiller elektroniske signaturer med håndskrevne signaturer eller det japanske «bumerket» Hanku. Det skal også utvikles regelverk som skal dekke virksomheten til utstedere av sertifikater.

6.9 Australia

Sentrale tiltak i forvaltningen

Det sentrale tiltaket for innføring av PKI i forvaltningen er det såkalte Gatekeeper-programmet som definerer rammeverket for offentlig PKI-politikk. Enhver sertifikatutsteder innenfor offentlig eller privat sektor må være godkjent etter Gatekeeper-kriterier.[13] Videre er det etablert en sentral Government Public Key Authority (GPKA) som har ansvaret for Gatekeeper. Det forventes at mange sertifikatutstedere (opptil 14) vil bli godkjent av Gatekeeper i nærmeste framtid.

PKI for eksterne tjenester til brukere

13

http://www.ogo.gov.au/publications/gatekeeperstrategy.pdf

Den australske forvaltningen følger også en strategi for elektronisk forvaltning.[14] Denne strategien forutsetter etablering av elektroniske tjenester fra forvaltningen i løpet av 2001. En av de etatene som tar i bruk PKI for å tilby tilgangen til sine elektroniske tjenester er det australske skattevesenet ATO (Australian Taxation Office).

ATO sin løsning for elektronisk innlevering av selvangivelser fra privatpersoner forutsetter bruk av et engangssertifikat utstedt for det formålet å signere en selvangivelse. Sertifikatet blir straks etter tilbakekalt. Brukere laster selv ned klientprogramvare fra Internett for utfylling av skjema og signering. I 2000 forventet man at ca. 80 000 selvangivelser ville bli levert på denne måten mot 50 000 i 1999.

For selskapers levering av selvangivelser og MVA-oppgaver utstedes det sertifikater fra den pr. i dag eneste Gatekeeper-godkjente sertifikatutstederen ATO. Registrering for sertifikat er knyttet til utstedelsen av et unikt nummer til hver firma Australian Business Number. Det er ekvivalent til vårt organisasjonsnummer. Pr. 1.11.2000 er det blitt utstedt ca. 290 000 sertifikater til private firmaer fra ATO. Av disse er det 46 000 firmaer som er klare til å starte med elektronisk levering av selvangivelse og MVA-oppgaver (de har nøkkelpar og klientprogramvare).

På lang sikt vurderer australsk forvaltning det slik at den beste løsningen for distribuering av nøkler er at brukeren selv genererer sine egne nøkkelpar og installerer dem i sin nettleser.

ATO sin pilotbruk av PKI setter på mange måter standarden for hele den australske forvaltningen og vil danne mønster for utbredelse av PKI i tiden framover.

Lovgivning og andre tiltak

Australia har egen lov om elektronisk kommunikasjon og -handel som anerkjenner elektroniske signaturer.

6.10 Oversikt over PKI-politikker i utvalgte OECD-land

Tabell 6.1 Oversikt over PKI-politikker i utvalgte OECD-land

Land	Modell for utbygging av PKI	Antall sikkerhetsnivåer	Felles profiler og sertifikatpolicy	Unik identifisering av personer
Sverige	Rammeavtaler for forvaltningen og publikum; avtaler med banker og post	3; høyeste nivå likt kvalifiserte sertifikater	Profiler finnes policy under utvikling	Fødselsnummer i sertifikatet
Danmark	Stimuleringsmidler til forsøksprosjekter rammeavtaler for offentlig elektronisk informasjonsutveksling	Uklart utvalg arbeider med dette	Profiler finnes uklart om felles policy vil utvikles	Utstedere genererer et unikt nummer etter gitte regler (felles struktur); nummeret kan være flyttbart; koples til CPR-nr. (fødselsnr.)
Finland	Sentral ordning for elektroniske ID-kort v/folkeregisteret. Forvaltningen kan	3; høyeste nivå (ID-kort) er strengere enn kvalifiserte sertifikater	Profiler finnes sertifikatpolicy for ID-kort	Nytt unikt nasjonalt nummer – FINUID Lagres i folkeregisteret i

14

http://www.govonline.gov.au

Land	Modell for utbygging av PKI	Antall sikkerhetsnivåer	Felles profiler og sertifikatpolicy	Unik identifisering av personer
	kjøpe i markedet			tillegg til fødselsnummer. Kun til bruk i sertifikater
Storbritannia	Sentralt initiativ for intern bruk styres fra sikkerhetsmyndigheter. Markedsmodell for publikumstjenester	4; de to høyeste skal dekkes av PKI-løsninger de 2 laveste av andre teknologier	PKI-løsninger skal være godkjent iht. tScheme en nasjonal ordning med omfattende krav basert bl.a. på BS 7799	Ingen unik identifikator
Nederland	Sentral arbeidsgruppe sentralt koordinert utbygging av PKI for intern bruk; samarbeid med markedet for publikumsløsninger bankene aktuelle	1; vurderes brukt både for interne formål i forvaltningen og for tjenester til publikum; krever smartkort	Uklart men skal være under utvikling (profiler)	Uklart skal utvikle retningslinjer for dette
USA	Hver etat utsteder egne sertifikater koordinering via sentral bro; sentral styringsgruppe for forvaltningens PKI; rammeavtaler for sertifikater til publikum	4 for forvaltningen internt; eget nivå for publikumssertifikater (ACES)	Felles sertifikatpolicy for broløsningen felles sertifikatprofiler for forvaltningen	Ingen unik identifikator
Canada	Hver etat utsteder egne sertifikater; koordinering via sentral rotnode og kryssertifisering; sentral styringsgruppe for PKI i forvaltningen; arbeider med strategi for publikum	4 for forvaltningen internt; uklart hva som vil gjelde for publikum	8 felles sertifikatpolicyer to for hvert nivå – en for signering/ autentisering og en for kryptering; uklart om profiler finnes	Uklart men trolig ingen unik identifikator
Japan	Hver etat utsteder egne sertifikater; også for publikum?	Trolig 1	Arbeider med utvikling av felles policy uklart om felles profiler finnes	Uklart men har det nasjonale Hanku-systemet med personlig segl – sertifikatutstedelse vil knyttes til det
Australia	Hver etat utsteder egne sertifikater; må være godkjent under det sentrale Gatekeeper-programmet; planlegger at	Uklart	Trolig en del av kravene under Gatekeeper	Uklart

Land	Modell for utbygging av PKI	Antall sikkerhetsnivåer	Felles profiler og sertifikatpolicy	Unik identifisering av personer
	publikum selv kan skaffe seg nøkler			

Del III
Elementer i en PKI-politikk for forvaltningen

7 Krav til digitale sertifikater som forvaltningen vil benytte

I dette kapitlet omtales ulike typer sertifikater som forvaltningen kan ha behov for. Innholdet i slike sertifikater drøftes med særlig vekt på unik identifisering av eiere av sertifikater.

7.1 Innledning

Et sertifikat er den digitale «legitimasjon» som eieren får utstedt for å garantere at den offentlige nøkkelen som vedkommende har fått virkelig er hennes. Sertifikater kan utstedes for fysiske personer virksomheter og roller men også for PC-er servere nettverkskomponenter og programvare. PKI kan med andre ord brukes til å autentisere hvem som helst og hva som helst når de er elementer i elektronisk samhandling over nett.

De mest aktuelle sertifikattypene er sertifikater for personer generelt for ansatte i en organisasjon og for en virksomhet. Som regel utstedes slike sertifikater som identitetssertifikater dvs. sertifikater som inneholder informasjon som entydig identifiserer eieren av sertifikatet.

Sertifikater for enkeltpersoner kan knyttes til og gi informasjon om eierens rolle i en virksomhet eierens profesjon autorisasjon eller andre egenskaper ved eieren. Personlige sertifikater kan utstedes med et pseudonym eller på en slik måte at eieren forblir anonym.

Virksomhetssertifikater kan brukes ved autentisering av forvaltningens web-anvendelser. Slik autentisering vil foregå automatisk og gi brukeren sikkerhet for at hun kommuniserer med den rette serveren og det rette systemet. Virksomhetssertifikater kan også benyttes der det f.eks. er aktuelt å signere som virksomhet og ikke som enkeltperson ansatt i virksomheten.

Rollesertifikater er sertifikater for roller og autorisasjoner. Rollesertifikater kan utstedes på ulike måter: enten som et personlig sertifikat der det finnes spesielle informasjonselementer som beskriver hvilken rolle personen har i en gitt sammenheng (f.eks. styreformann i et selskap eller ordfører i en kommune) eller som et såkalt sekundærsertifikat som knyttes til eierens personlige identitetssertifikat og som inneholder den samme offentlige nøkkelen som identitetssertifikatet. Et slikt sekundærsertifikat vil kunne inneholde referanse til identitetssertifikatet og beskrivelser av roller/autorisasjoner for eieren av identitetssertifikatet. Mangel på standardiserte løsninger for rollesertifikater gjør det vanskelig å ta slike sertifikater i bruk på kort sikt. Det mangler også standarder for å representere autorisasjoner og roller slik at brukere av sertifikatet (f.eks. innenfor hele EØS-området) vil kunne forstå hva som menes. I tillegg kan den praktiske håndteringen av rollesertifikater medføre vedlikeholdsproblemer siden roller kan endre seg forholdsvis raskt.

7.2 Teknologiske begrensninger

7.2.1 Standarder

Sertifikater må være standardisert for å kunne brukes mellom kommunikasjonspartnere som ikke kjenner hverandre fra før. Den mest anvendte standarden er X.509 v3 (dvs. versjon 3 av ITU-standarden X.509).

X.509 v3 [37] er en omfattende standard med mange valgmuligheter. Standarden omhandler bare i begrenset grad innholdet i de forskjellige felter og attributter som kan inngå i et sertifikat. Sertifikater fra ulike tjenester kan se svært forskjellige ut.

Denne typen sertifikater kan ha utvidelser som gir mer informasjon bl.a. informasjon om hvordan sertifikatet kan brukes. Enhver utvidelse som ikke implementeres hos aktuelle motparter vil kunne begrense bruken. Ved automatisert bruk av sertifikater må reglene for fortolkning av de enkelte feltene være helt entydige og like f.eks. tolkningen av feltet som forteller hva den offentlige nøkkelen kan brukes til.

En spesifikasjon av hvordan en standard brukes i et bestemt tilfelle f.eks. hvilke felt som tas med i et sertifikat og hvordan dette kodes kalles en profil. En profil er en presisering av en standard tilpasset et konkret anvendelsesområde. Det finnes internasjonale standardprofiler for X.509-sertifikater. Internettstandarden RFC 2459 [37] beskriver en profil av X.509 v3 som skal kunne brukes innen PKI-basert

kommunikasjon på Internett. Denne profilen er imidlertid ganske omfattende og trenger ytterligere presisering dersom man skal bruke den til konkrete formål.

På internasjonalt nivå er man avhengig av internasjonale standarder for profiler. Men det mangler mye på internasjonal koordinering av profiler og nasjonale profiler i forskjellige land varierer en god del.

Programvare som benyttes for å signere autentisere kryptere samt verifisere signatur og dekryptere dokumenter kan også sette begrensninger for bruk av sertifikater. Senders system og mottakers system må behandle sertifikater likt. Er systemenes behandlingsmåte meget forskjellig kan dette skape hindringer selv om man legger standardiserte sertifikater til grunn.

7.2.2 Kvalifiserte sertifikater

I lov om elektronisk signatur [52] defineres kvalifiserte sertifikater på grunnlag av EU-direktivets definisjon. Kvalifiserte sertifikater skal kunne benyttes for å framstille kvalifiserte elektroniske signaturer som ifølge loven skal gis eksplisitte rettsvirkninger. Betegnelsen kvalifisert sertifikat skal kunne brukes om sertifikater som oppfyller krav til bestemt innhold (definert i § 4 i loven) og utstedes for en bestemt periode av en sertifikatutsteder som oppfyller bestemte krav i lovens §§ 10–15 som f.eks. krav til at opplysninger om sertifikateier kontrolleres gjennom sikre rutiner og at relevante opplysninger lagres.

Informasjonsinnholdet i kvalifiserte sertifikater har flere tilleggskrav i forhold til Internett-profilen RFC 2459. Et kvalifisert sertifikat skal bl.a. ha felter som indikerer at det er et kvalifisert sertifikat mulighet for avgrensing av bruksområdet for sertifikatet og eventuelt en grense for hvilken verdi en transaksjon kan ha.

Gjennom arbeidet utført av EESSI (jf. punkt 5.1.1) har Europakommisjonen sørget for at det ble utarbeidet en profil for kvalifiserte sertifikater. Denne er også blitt til en Internett-standard[15] Det kan være naturlig for forvaltninger i EØS-land som implementerte EU-direktivet om elektroniske signaturer å ta utgangspunkt i denne profilen når man skal anbefale nasjonale standarder for sertifikater.

7.2.3 Profiler for sertifikater som kan anvendes av den norske forvaltningen og av brukere av forvaltningens tjenester

I vedlegg 2 er det beskrevet sertifikatprofiler som utvalget anbefaler at man legger til grunn for utstedelse av sertifikater til bruk for forvaltningen og forvaltningens brukere. Disse profilene baserer seg på internasjonale standarder og profiler beskrevet ovenfor.

7.3 Ulike typer sertifikater

Forvaltningsnettsamarbeidet har i forbindelse med inngåelse av rammeavtaler om digitale signaturer med tilhørende tjenester gjennomført en utredning av behovet for standardisering av innholdet i sertifikater som forvaltningen kan bruke. Dette arbeidet ble oppsummert i en rapport [28] som ble lagt til grunn for anskaffelsen av løsninger på avtalen. I rapporten er det beskrevet fire typer sertifikater: medarbeidersertifikater virksomhetssertifikater rollesertifikater og profesjonssertifikater. Rapporten beskriver ikke sertifikater for servere eller anvendelser internt i forvaltningen heller ikke sertifikater for privatpersoner og private virksomheter.

Utvalget har gjennomgått dette tidligere arbeidet samtidig som man har vurdert ulike behov for sertifikater i forbindelse med elektronisk samhandling innad i forvaltningen og med forvaltningens brukere.

15

ftp://ftp.isi.edu/in-notes/rfc3039.txt

.

På grunnlag av dette og på grunnlag av en vurdering av status i det internasjonale standardiseringsarbeidet og eksisterende teknologibegrensninger har utvalget kommet fram til forslag til ulike typer sertifikater som det kan være behov for i forvaltningen.

7.3.1 Ansattsertifikat

Et ansattsertifikat er et personlig sertifikat for personer som er ansatt i en offentlig eller en privat virksomhet. Ansattsertifikat er et identitetssertifikat.

Formålet med et slikt sertifikat er entydig å kunne identifisere en person som ansatt i en virksomhet. Dette innebærer at sertifikatet bør inneholde opplysninger om selve virksomheten (navn organisasjonsnummer) og om den ansatte (navn og ev. informasjon som unikt identifiserer den ansatte i virksomheten). Det kan i tillegg være hensiktsmessig å inkludere en e-postadresse til den ansatte og eventuelt navnet på den organisasjonsenheten den ansatte vil tilhøre.

Utvalget anbefaler at ansattsertifikater utstedes iht. profilen som er beskrevet i vedlegg 2.

Bruk av ansattsertifikater

Ansattsertifikater kan brukes til manuelle og halvautomatiserte forsendelser ut fra virksomheten. Arbeidsgivers organisasjonsnummer sikrer at mottaker med sikkerhet kan slå fast hvor forsendelsen kommer fra. Dette gjelder enten en saksbehandler eller en arkivar signerer og eventuelt krypterer forsendelsen. Autorisasjon til å utføre ekspederingen vil være en intern sak i virksomheten. En privatperson som mottar et digitalt signert brev med et ansattsertifikat vil kunne verifisere både at dokumentet ble signert av den angjeldende offentlige ansatte og at dokumentet faktisk kommer fra en offentlig virksomhet.

Behovet for personlige digitale signaturer i forvaltningen kan diskuteres særlig i lys av personvernet for de ansatte. Utsendelse av meldinger fra virksomheten kan imidlertid gjøres uten at det er nødvendig med personlig digital signatur. Se omtalen av virksomhetssertifikater nedenfor og forslag til regler i kapittel 11. Den ansattes navn vil uansett framgå av selve saksdokumentet som oversendes.

7.3.2 Virksomhetssertifikat

Et virksomhetssertifikat skal sikre kommunikasjon til og fra virksomheter og organisasjonsenheter. Det er ikke knyttet personinformasjon eller personidentifikasjon til virksomhetssertifikater.

Et virksomhetssertifikat bør inneholde informasjon om virksomhetens navn og organisasjonsnummer. Det er nærliggende at informasjon som skal ligge i slike sertifikater hentes fra Enhetsregisteret i Brønnøysund. I tillegg til virksomhetens navn slik det er registrert i Enhetsregisteret bør det også inkludere det navnet virksomheten til vanlig er kjent under. Virksomhetens felles e-postadresse (postmottaket) kan også tas med.

Utvalget anbefaler at virksomhetssertifikater utstedes iht. profilen som er beskrevet i vedlegg 2.

Bruk av virksomhetssertifikater

Virksomhetssertifikater kan benyttes av personer som er autorisert til å signere ekspedisjoner med slikt sertifikat. Det er nærliggende å tro at dette vil være personer knyttet til arkiv og/eller postekspedisjon. Men det kan også være saksbehandlere og ev. ledere som vil kunne bruke slike sertifikater. Det vil måtte utarbeides klare rutiner for tilgang til og bruk av virksomhetssertifikater i en offentlig virksomhet.

Den mest vanlige bruken av virksomhetssertifikater vil trolig være automatisert. Ved automatisert behandling av forsendelser fra en virksomhet vil det ikke være en fysisk person som utfører signeringen av en forsendelse men det vil være en fysisk person som starter prosessen som fører til slik signering.

Bruken av virksomhetssertifikater gir mulighet for å få vite avsender og integritetsbeskytte forsendelsen. Dette skjer ved å bruke nøkler og sertifikater men det diskuteres om det er passende å kalle det signering. Slik signering kan på mange måter sammenliknes med bruk av brevhodet ved papirkorrespondanse.

Virksomhetssertifikater kan brukes til å dekke behovene innen elektronisk datautveksling nemlig meldinger til og fra en tjeneste på en server.

Offentlige virksomheter har behov for å motta elektronisk post til seg eller til en avdeling på samme måte som de mottar fysisk post. Postmottaket eller et annet mottakende system vil måtte være i stand til å dekryptere e-post. Kryptering ved hjelp av nøkler knyttet til virksomhetssertifikater vil ikke være koplet til personer men det vil måtte finnes rutiner og autorisasjoner for tilgang til virksomhetens private nøkkel for dekryptering.

Det kan være aktuelt å utstede sertifikater med nøkler for dekryptering til enheter i en virksomhet f.eks. avdelinger.

For at enkeltpersoner og næringsliv skal kunne sikre konfidensielle forsendelser til forvaltningen trengs det en mekanisme for spredning av virksomhetssertifikater med den offentlige krypteringsnøkkelen.

7.3.3 Profesjonssertifikat

Et profesjonssertifikat er et personlig sertifikat som bekrefter at personen har et bestemt yrke eller en utdanning og eventuelt autorisasjon/godkjenning fra en myndighet eller en organisasjon som godkjenner profesjonsrettigheter. Profesjonssertifikat kan betraktes som en kombinasjon av identitetssertifikat og rollesertifikat. Profesjonssertifikater kan f.eks. angi at man er lege advokat eller skipsfører.

Et profesjonssertifikat vil i informasjonsinnhold likne på et personsertifikat men den unike identifiseringen av eieren vil være en kode eller et nummer som inngår i et register over innehavere av relevant yrke/utdanning. Videre vil sertifikatet inneholde navnet på den myndighet eller organisasjon som har ansvaret for godkjenningen av yrket/utdanningen og som også administrerer rettigheter knyttet til det/den.

I tillegg kan sertifikatene inneholde et tittelfelt som gir en tekstlig beskrivelse av profesjonen[16] Denne beskrivelsen egner seg ikke for maskinell behandling men kan brukes av en menneskelig mottaker for å vurdere autorisasjoner. Autorisasjoner må ellers sjekkes ved å sammenholde informasjonen i sertifikatene med informasjon i et register (f.eks. helsepersonellregisteret).

Profesjonssertifikater kan utstedes av den myndighet/organisasjon som godkjenner profesjonen. Myndigheten/organisasjonen kan kjøpe den fysiske tjenesten for dette i markedet. Et alternativ er at kommersielle sertifikatutstedere sjekker profesjonstilhørighet hos aktuelle organisasjoner og utsteder sertifikater med unik identifikator innen den profesjonen.

Utvalget vil ikke ta stilling til hvilket alternativ som er det beste. Dette bør kunne avgjøres av hver enkelt sektor.

Utvalget anbefaler at profesjonssertifikater utstedes iht. profilen som er beskrevet i vedlegg 2.

Bruk av profesjonssertifikater

Profesjonssertifikater vil særlig være aktuelle i de tilfellene en person ikke tidligere er registrert i et mottakende system eller det ikke er hensiktsmessig med slik registrering. Mottakere av signerte meldinger/dokumenter kan i visse sammenhenger ha behov for å vite ikke bare hvem avsenderen er men også hva slags rolle vedkommende opptrer i samt om dette gir vedkommende autorisasjon til å utføre visse handlinger.

Denne problemstillingen kan være aktuell for enkelte selvstendig næringsdrivende f.eks. advokater revisorer eller leger. Et eksempel på bruk av et profesjonssertifikat kan være at en privatpraktiserende lege skal sende en digitalt signert resept til et apotek. Mottakersystemet må verifisere at sertifikatet er ekte og gyldig ved å sende en forespørsel til sertifikatutsteder. I tillegg må det sjekke at legen kan foreskrive

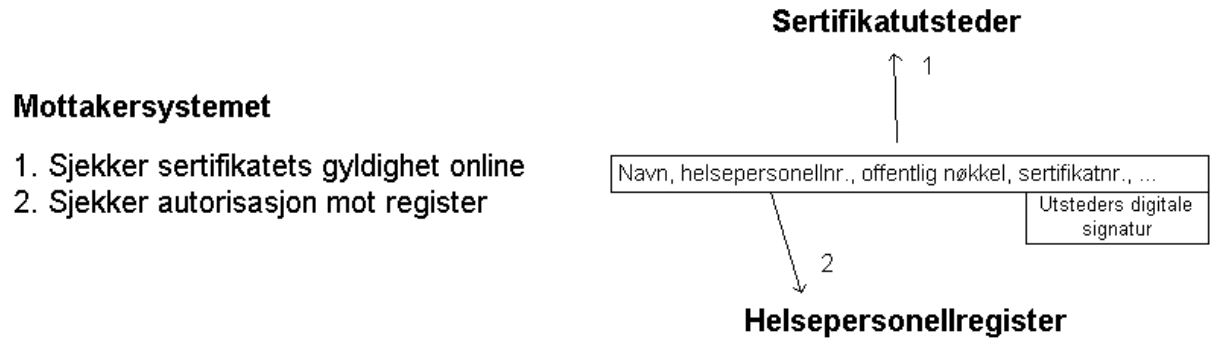
---

16

F. eks. «Lege spesialist indremedisin».

.

medikamentet ved å sende en forespørsel til helsepersonellregisteret (dette vil innebære at det gjøres et oppslag i dette registeret på det unike helsepersonellnummeret som står i sertifikatet).



Figur 7.1 Eksempel på bruk av profesjonssertifikat

7.3.4 Offentlig personsertifikat

Et offentlig personsertifikat er et sertifikat for privatpersoner til bruk mot forvaltningens tjenester og systemer.

Der forvaltningen ønsker å kommunisere med enkeltpersoner ved hjelp av sertifikater må sertifikatene ha det informasjonsinnholdet som er nødvendig for at forvaltningen skal kunne forsikre seg om at man har med riktig person å gjøre. Hvis forvaltningen går inn for at et bestemt felles sertifikatinnhold kan brukes mot flere av tjenestene/systemene vil det lette enkeltpersoners samhandling med forvaltningen.

Kravene til identifisering av personer kan variere med sakstypen og de enkelte datasystemene jf. *Henvendelser som utløser veiledningsplikt* punkt11.2.3.2. Det vil f.eks. ikke alltid være nødvendig for alle systemene i forvaltningen å kjenne til fødselsnummeret til den personen som signerte en elektronisk henvendelse.

Det vil neppe være hensiktsmessig at kommunikasjon mellom forvaltning og enkeltpersoner foregår med anonyme sertifikater. Hvis henvendelsen ikke er knyttet til et personlig forhold er det rimelig å anta at det heller ikke er behov for sertifikat.

Et offentlig personsertifikat bør inneholde personens vanlig brukte navn. Utvalget ser det ikke som nødvendig at navnet skal hentes fra folkeregisteret. Det er tilstrekkelig at det ved registrering av personen i forbindelse med sertifikatutstedelse sjekkes mot folkeregisteret (gjennom oppslag på fødselsnummer) at det oppgitte navnet eksisterer og at personen som registrerte seg for å få utstedt et sertifikat samsvarer med personen som er registrert.

I flere tilfeller vil det være behov for å identifisere personer unikt og derfor bør sertifikatet inneholde en eller annen form for unik identifikator. Dette spørsmålet behandles i detalj i punkt 7.4.5.

Der det er ønskelig med slik informasjon kan man i tillegg legge inn personens e-postadresse (dette er foranderlig informasjon og endring her kan føre til at hele sertifikatet må utstedes på nytt) og personens fulle navn slik det er registrert i folkeregisteret.

Utvalget anbefaler at offentlige personsertifikater utstedes iht. profilen som er beskrevet i vedlegg 2.

Bruk av offentlige personsertifikater

Offentlige personsertifikater skal kunne brukes både for autentisering mot forvaltningens tjenester og for signering av henvendelser det være seg i form av et web-skjema eller elektronisk post. Autentisering vil trolig være den mest hyppige anvendelsen som kan erstatte bruk av PIN-koder fødselsnummer passord osv. for å identifisere seg overfor en offentlig personalisert tjeneste.

Det er lite sannsynlig at offentlige personsertifikater vil bli brukt til kryptering av forvaltningens kommunikasjon til privatpersoner selv om slik bruk ikke kan utelukkes. Konfidensialitetssikring av privatpersoners kommunikasjon med forvaltningen vil for det meste skje gjennom bruk av krypterte forbindelser til forvaltningens systemer.

7.3.5 Sertifikater for private bedrifter

Utvalget ser at det i pilotanvendelser legges opp til at forvaltningen selv utsteder nødvendige sertifikater til bedrifter som skal drive elektronisk samhandling med forvaltningen. Dette kan kalles en «bransjemodell» der sertifikater er tilpasset den konkrete anvendelsen som forvaltningen har lagt opp til. I en seinere fase vil bedriftene trolig selv anskaffe sertifikater på markedet gitt at forvaltningen godtar slike. På dette området kan det tenkes at forvaltningen i framtiden vil kunne godta bruk av sertifikater tilsvarende ansattsertifikater samt virksomhetssertifikater i forvaltningen og bruk av sertifikater tilsvarende offentlige personsertifikater.

7.3.6 Sertifikater fra andre land

Offentlig forvaltning vil kunne trenge å samhandle elektronisk med forvaltninger organisasjoner privatpersoner og bedrifter i andre land. De mest aktuelle landene er land i EØS-området men flere etater som f.eks. Rikstrygdeverket vil ha behov for kommunikasjon med land utenom EØS der det finnes mottakere av deres ytelser. Kommunikasjonen vil mest sannsynlig gjelde utveksling av dokumenter/skjemaer. Pengetransaksjoner utføres i dag i stor grad gjennom det verdensomspennende banksystemet SWIFT og på andre avtalte måter. Utbredelsen av globale sertifikattjenester som IDENTRUS[17]vil bidra til at bedrifter vil kunne benytte sertifikater i kommunikasjon over landegrensene.

Forvaltningen vil være avhengig av en felles forståelse når det gjelder bruk av sertifikater fra utlandet. Dette omfatter bl.a. tolkning av innholdet i feltene i sertifikatene. EU-direktivet om rammeverk for elektroniske signaturer gir et rettslig utgangspunkt for aksept av sertifikater fra andre land. Implementeringen av direktivet vil imidlertid variere fra land til land. Dette kan skape utfordringer for de praktiske løsningene på området.

Håndtering av sertifikater fra andre land er et spørsmål som forvaltningen må utrede videre. Den internasjonale situasjonen på dette området er i stadig endring med ny lovgivning og utvikling av nasjonale politikker for bruk av PKI i mange land.

Utvalget anbefaler at den norske forvaltningen deltar i internasjonale fora der forvaltninger i andre land drøfter bruk av PKI.

Utvalget anbefaler at spørsmålet om håndtering av sertifikater fra utlandet utredes videre når implementeringen av EU-direktivet er avsluttet i EØS-land.

7.4 Standardisert bruk av navn og unike identifikatorer i sertifikater

7.4.1 Hvorfor trenger man standardiserte navn og unike identifikatorer?

Automatisk behandling av sertifikater krever entydige regler for identifisering av sertifikateier som gir sikkerhet for at man samhandler med riktig person eller virksomhet/organisasjon. Informasjon som kan hentes ut fra sertifikatet vil bli brukt til videre behandling av henvendelsen i forvaltningens interne systemer.

17

http://www.identrus.com/

I noen systemer vil det være et krav at navnet er i samsvar med det navnet som er registrert i folkeregisteret. Selv om navnet står i folkeregisteret gir det ikke nødvendigvis en entydig identifikasjon av sertifikatets eier selv om det også kan finnes andre opplysninger i sertifikatet som kan gi nærmere identifisering f.eks. fødselsdato. Det kan finnes flere personer med navnet Petter Olsen som er født på samme dag. Derfor trenger man en unik identifikator som entydig identifiserer sertifikateieren innen det domenet (anvendelsesområdet) som brukeren av sertifikatet vil forholde seg til. For ansattsertifikater vil et slikt domene være virksomheten selv mens det for offentlige personsertifikater vil dreie seg om hele landet fordi slike sertifikater skal kunne utstedes til enhver registrert innbygger i Norge.

Noen systemer og anvendelser f.eks. e-post vil ikke nødvendigvis kreve at sertifikater inneholder navn og identifikator iht. folkeregisteret. Hvorvidt forvaltningen trenger å standardisere navn og unike identifikatorer vil avhenge av hvordan hvert datasystem skal bruke informasjonen i sertifikatene. Og hvis det oppstår problemer med hvem som har sendt en e-post kan identiteten sjekkes ytterligere på et seinere tidspunkt. Saksbehandleren bør vurdere behovet for ytterligere autentisering i forhold til den aktuelle saken jf. punkt 11.2.3.

I forbindelse med tildeling av navn til eiere av sertifikater har man definert en egen funksjon – navngivingsfunksjonen. En slik funksjon må operere innenfor et navnerom eller et navnedomene. Et navnerom er en samling av navn som kan tildeles visse objekter (personer virksomheter datamaskiner osv.). Regler som styrer denne tildelingen kalles navngivingsregler [28] og skal sørge for at det ikke utstedes to ulike sertifikater og nøkler med identiske navn for samme formål. En offentlig virksomhet som ønsker å utstede sertifikater til egne ansatte kan ha sitt eget navnerom.

Bruken av navn kan variere avhengig av hva sertifikatet anvendes til. Noen systemer vil ikke lese navnet i sertifikatet i det hele tatt. Enkelte av Rikstrygdeverkets anvendelser der PKI brukes leser ikke navnet i sertifikatet.

Er det ønskelig sett fra forvaltningens side at enkeltpersoner identifiserer seg på samme måte overfor dens systemer? Hvis navnet i offentlige personsertifikater kommer fra folkeregisteret har alle forvaltningens systemer én måte å forholde seg på. Men navn er uansett ikke unikt så behovet for og nytten av å inkludere slikt navn i sertifikater vil være begrenset.

I lov om elektronisk signatur [52] kreves det at kvalifiserte sertifikater skal inneholde undertegnerens navn eller pseudonym men det stilles ikke ytterligere krav til navnet. Dette kan endre seg når det foreligger ferdig forskriftsverk til loven.

Pseudonyme sertifikater er nok mest anvendelige i forbindelse med handelstransaksjoner der det for selgeren ikke er viktig hvem som er kjøperen men om kjøperen er i stand til å betale varen/tjenesten. I forvaltningens transaksjoner med brukere er det derimot svært viktig å vite hvem man har med å gjøre. Korrekt og pålitelig identifisering av personer er en grunnleggende forutsetning for at enkeltpersoner kan utøve sine rettigheter og plikter overfor forvaltningen.

Et system i forvaltningen må ha standardiserte navngivingsregler å forholde seg til for hvert sertifikat det behandler. Jo flere sertifikatutstedere som følger en standard for navngiving f.eks. en sertifikatprofil jo enklere kan bruken av PKI bli.

7.4.2 Unik identifisering av ansatte i ansattsertifikater

Et ansattsertifikat bør inneholde minimum følgende opplysninger:

- Personens vanlig brukte navn (hentet fra personalregisteret eller tilsvarende)
- Ansattnummer eller tilsvarende unik identifikator innenfor virksomheten f.eks. initialer
- Personens arbeidsgiver (virksomhetens vanlig brukte navn)
- Arbeidsgiverens organisasjonsnummer
- Landkode.

Utvalget mener at disse opplysningene til sammen vil kunne identifisere en person som er ansatt i en offentlig virksomhet på en entydig måte. Koding av denne informasjonen skal skje iht. profilen som er beskrevet i vedlegg 2.

7.4.3 Unik identifisering av virksomheter i virksomhetssertifikater

Et virksomhetssertifikat bør inneholde minimum følgende opplysninger:

- Virksomhetens vanlig brukte navn (oppgis av virksomheten selv)
- Virksomhetens organisasjonsnummer (hentet fra Enhetsregisteret)
- Virksomhetens registrerte navn (hentet fra Enhetsregisteret)
- Landkode.

Virksomhetssertifikater skal kunne benyttes for å autentisere en virksomhet (juridisk person) og dennes offentlige nøkkel. Det er naturlig å benytte det navnet som virksomheten selv velger å bruke til daglig samtidig som det er behov for entydig identifisering av den juridiske personen. Enhetsregisteret er navne- og nummerautoriteten på dette området og det anbefales derfor å ta med både organisasjonsnummer og det fulle virksomhetsnavnet slik det er registrert i dette registeret. Disse opplysningene gir til sammen gode muligheter til å verifisere at det dreier seg om riktig juridisk person.

Koding av opplysninger i virksomhetssertifikatet bør skje iht. den foreslåtte profilen i vedlegg 2.

7.4.4 Unik identifisering av personer i profesjonssertifikater

Et profesjonssertifikat bør inneholde minimum følgende opplysninger:

- Personens vanlig brukte navn
- Unik identifikator for denne personen som utøver av et yrke eller innehaver av en utdanning (hentes fra relevant register hos den myndighet eller organisasjon som har i oppgave å godkjenne yrke/utdanning og føre slikt register)
- Yrkes- eller utdanningstittel (f.eks. lege spesialist psykiatri)
- Organisasjonsnummer til den myndighet/organisasjon som fører registeret
- Vanlig brukt navn til den myndighet/organisasjon som fører registeret
- Landkode.

Profesjonssertifikater vil bli brukt på en annen måte enn ansattsertifikater fordi det er personen som utøver av et yrke/innehaver av en utdanning som er subjektet her og ikke personen som ansatt i en virksomhet. Unik identifisering av personen i en slik sammenheng vil kunne skje på grunnlag av den unike identifikatoren og på grunnlag av opplysninger om den myndigheten/organisasjonen som fører registeret der personen er registrert med denne identifikatoren.

For lukkede anvendelser innenfor helsesektoren kan det være aktuelt med rene personsertifikater med bruk av helsepersonellnummer som unik identifikator [8]. Dette vil bli nærmere drøftet i sektoren.

Koding av opplysninger i virksomhetssertifikater bør skje iht. den foreslåtte profilen i vedlegg 2.

7.4.5 Unik identifisering av personer i offentlige personsertifikater

Ut fra tidligere argumentasjon framgår det at det er nødvendig å kunne identifisere eiere av offentlige personsertifikater unikt. I praksis betyr det at man via sertifikatet skal kunne få tilgang til innehaverens fødselsnummer. Den enkleste måten å løse dette på vil være å ha fødselsnummeret i sertifikatene. Det finnes også andre måter å ivareta identifiseringsbehovet på.

Brønnøysundregistrene Skattedirektoratet og Statistisk sentralbyrå ba i brev av 10.5.2000 utvalget om å ta hensyn til etatenes behov for å kunne identifisere enkeltindivider på en sikker måte. Som mulig løsning foreslår de at det stilles krav til sertifikatutstedere i markedet om at de kopler personlige sertifikater med fødselsnummer og at alle utstedere skal inngå avtale om kryssertifisering (jf. omtale i kap. 10) for bruk av slike sertifikater.

Forvaltningen må spesifisere hvordan unike identifikatorer (fødselsnummer eller annet) skal brukes i sertifikater som skal benyttes innenfor og mot forvaltningen. Dersom fødselsnummer skal brukes må betingelsene for dette avklares spesielt med tanke på personvern og tilgang til kataloger.

Det vil eksistere frykt i opinionen for at fødselsnummer vil kunne spres og brukes/misbrukes i stor grad. Fødselsnummer vil følge med i det tilhørende sertifikatet når man signerer digitalt. Mange mennesker ser på fødselsnummeret sitt som sensitiv informasjon selv om det ikke er å betrakte som det ut fra bestemmelser i lov om behandling av personopplysninger. Man trenger programvare for å lese innholdet i sertifikater og lesing av annen informasjon enn navnet utsteder og gyldighetsperiode krever spesialtilpasninger i programvaren. Det kan likevel tenkes at de som ønsker å spore en persons aktiviteter ved å lese sertifikater som brukes i ulike transaksjoner på nettet vil kunne skaffe seg slik tilpasset programvare og tilgang til de aktuelle sporene.

Ut fra hensynet til opinionen kan det være ønskelig å finne alternativer til å bruke fødselsnummer direkte i sertifikater.

Ett alternativ som er tatt i bruk i Finland i forbindelse med at det finske folkeregisteret utsteder elektroniske ID-kort til befolkningen er å ta i bruk en ny nummerserie for å tildele unike identifikatorer for bruk i sertifikater. Det nye nummeret – FINUID – blir definert som et unikt nummer for brukere av det elektroniske ID-kortet. Gjennom regulering i lov har finnene sørget for at dette nummeret legges inn i folkeregisteret i tillegg til det «vanlige» personnummeret.

Dersom bruken av et slikt nummer blir svært utbredt vil det fort kunne føre til at dette nummeret vil få samme funksjon som fødselsnummeret. Videre kan det være kostbart å vedlikeholde to parallelle nummersystemer.

Et annet alternativ er at fødselsnummeret kjøres gjennom en beregning (en enveis hash-algoritme) som genererer en ny unik identifikator. Brukere av sertifikatet som har adgang til fødselsnummeret og annen nødvendig informasjon kan da bruke samme algoritme for å fastslå samsvar. Ved bruk av dette alternativet bør det defineres krav til slik algoritme både når det gjelder kvalitet og ytelse dvs. hvor pålitelig algoritmen er og hvor raskt prosessering av fødselsnummeret kan skje.

Et tredje alternativ går ut på at sertifikatutsteder genererer en identifikator som er unik for hver sertifikateier innen denne utsteders domene. Hvis identifikatoren f.eks. svarer til serienummeret i sertifikatet vil det endres ved hver nyutstedelse. Det legger til rette for å hindre sporing men vil bli vanskelig å administrere. Identifikatoren bør derfor være unik for personen over tid f.eks. personens levetid. Utsteder vil ha en tabell som kopler den unike identifikatoren fødselsnummer og eventuelt navn se figur 7.2. En institusjon som har tjenstlig behov for det vil få tilgang til tabellen f.eks. ved sjekk av sertifikatet mot en tilbaketrekkingsliste. Institusjonen vil så kunne hente fødselsnummeret ut av tabellen og bruke det i sin videre behandling.

Unik ID	Fødselsnummer	Navn
A123	120322 45032	Else Buer
A124	210834 54122	Petter Olsen
A201	010153 63311	Petter Olsen
A231	010168 46647	Solveig Hermansen

Figur 7.2 Tabell for unik identitet

På denne måten unngår man at fødselsnummeret inngår direkte i sertifikatet samtidig som det er forholdsvis lett tilgjengelig for de som har autorisasjon til å bruke nummeret. Det vil heller ikke være slik at den unike identifikatoren knyttet til én utsteder vil erstatte fødselsnummeret. Dersom det finnes minst to sertifikattilbydere med hver sin unike identifikatorserie kan enkeltpersoner velge og man slipper en landsdekkende unik identifikator.

Et eksempel på hvordan et slikt system vil kunne fungere med flere utstedere vises i figur 7.3. (Navn er tatt med for å lette forståelsen av eksempelet. Implementasjonen kan være en annen.)

Utsteder 1

Unik ID	Fødselsnummer	Navn
A123	120322 45032	Else Buer
A124	210834 54122	Petter Olsen
A231	**010168 46647**	Solveig Hermansen

Utsteder 2

Unik ID	Fødselsnummer	Navn
PS123	100522 54034	Kari Sira
PS158	211254 56133	Petter Olsen
PS431	**010168 46647**	Solveig Hermansen

Figur 7.3 Tabeller for unik identitet og fødselsnummer hos ulike utstedere

En slik løsning brukes i ELEKTRA-prosjektet i Skattedirektoratet. Leverandøren av sertifikattjenester til Skattedirektoratet utsteder sertifikater med en unik identifikator og har et register som oversetter denne til fødselsnummer før de innrapporterte opplysningene sendes fra leverandørens formidlingssentral til Skattedirektoratet. ELEKTRA-prosjektet er et eksempel på at sertifikater som behandles maskinelt må inneholde unik identifikator for å utføre de rette operasjoner/behandlinger av den informasjonen som er signert ved bruk av dette sertifikatet. Løsningen i ELEKTRA fungerer godt fordi formidlingssentralen der signaturen verifiseres og sertifikatutstederen som har koplingen mellom unik identifikator og fødselsnummer er en og samme organisasjon.

Det må likevel pekes på at en slik løsning kan skape problemer ved automatisk behandling av sertifikater der det ikke benyttes såkalte formidlingssentraler i og med at det må gjøres flere sjekk/oppslag mot sertifikatutsteder enn det som ville vært nødvendig om fødselsnummeret lå direkte i sertifikatet. Dette kan øke kostnadene og skape sårbarhet.

Ved helautomatisk behandling av sertifikater vil innholdet i svært begrenset grad eksponeres for mennesker. Der det tjenstlige behovet tilsier det bør derfor bruk av fødselsnummeret direkte i sertifikatet være mulig.

Utvalget mener for øvrig at unik identifisering av personer i offentlige personsertifikater vil kunne oppnås ved at sertifikatet inneholder minimum følgende opplysninger:

- Personens vanlig brukte navn
- Unik identifikator tildelt av sertifikatutstederen eller fødselsnummer
- Landkode.

Opplysningene i sertifikatet bør kodes iht. den foreslåtte profilen i vedlegg 2.

7.5 Oppsummering av utvalgets anbefalinger

Utvalget anbefaler at det for bruk internt i forvaltningen og i forbindelse med elektroniske tjenester til enkeltpersoner tas i bruk fire ulike typer sertifikater:

- Ansattsertifikater
- Virksomhetssertifikater
- Offentlige personsertifikater
- Profesjonssertifikater.

Utvalget anbefaler at sertifikatene kodes og tolkes iht. respektive sertifikatprofiler utarbeidet på grunnlag av profil for kvalifiserte sertifikater i EU. Profilene er beskrevet i vedlegg 2.

Utvalget ser ingen enkel og generell løsning for sertifikater for autorisasjoner og roller på det nåværende tidspunkt.

Utvalget anbefaler at spørsmålet om utstedelse av profesjonssertifikater utredes nærmere og avgjøres av de myndigheter og organisasjoner som har ansvaret for føring av relevante registre over yrke/utdanning som gir rettigheter.

Utvalget ser ikke at forvaltningen har behov for anonyme eller pseudonyme sertifikater.

Utvalget ser ikke noe behov for at navn som er registrert i folkeregisteret skal legges inn i offentlige personsertifikater. Personens vanlig brukte navn bør benyttes. Det forutsettes at sertifikatutstederen foretar sjekk av identiteten gjennom oppslag på fødselsnummer i folkeregisteret.

Utvalget anbefaler at det for unik identifisering av ansatte i ansattsertifikater inkluderes opplysninger som: den ansattes vanlige navn og ansattnummer eller annen entydig kode f.eks. initialer arbeidsgiverens vanlig brukte navn og organisasjonsnummer samt landkode.

Utvalget anbefaler at det for unik identifisering av virksomheter i virksomhetssertifikater inkluderes opplysninger som: virksomhetens registrerte navn og organisasjonsnummer fra Enhetsregisteret samt landkode.

Utvalget anbefaler at det for unik identifisering av innehavere av et yrke/en utdanning i profesjonssertifikater inkluderes opplysninger som: personens vanlig brukte navn unik identifikator i det registeret der personen er registrert navn og organisasjonsnummer til den myndigheten/organisasjonen som fører registeret samt landkode.

Utvalget anbefaler at det for unik identifisering av privatpersoner i offentlige personsertifikater inkluderes opplysninger som: personens daglig brukte navn og en identifikator som er unik innen utsteders domene og som kan koples til fødselsnummer ved tjenstlige behov. Der spesielle behov gjør seg gjeldende kan fødselsnummer inngå direkte i sertifikatet.

Utvalget anbefaler at forvaltningen går i dialog med næringslivet om bruk av sertifikater. Det vil være ønskelig at næringslivet legger seg nært opp til forvaltningens felleskrav på området.

Utvalget anbefaler at håndtering av sertifikater fra utlandet må utredes nærmere når situasjonen i EØS-land er klarere mht. implementering av EU-direktiv om elektroniske signaturer.

Utvalget anbefaler at forvaltningen deltar i internasjonale fora der bruk av PKI i forvaltningen drøftes.

8 Behov for felles sertifikatpolicy i forvaltningen

Dette kapitlet omhandler krav som forvaltningen bør stille til sikkerhet i forbindelse med utstedelse og behandling av sertifikater som brukes av forvaltningen og sertifikater som skal brukes av enkeltpersoner og næringslivet i samhandling med forvaltningen.

8.1 Sertifikatpolicy

En *sertifikatpolicy* er et dokument som omhandler regler for hvordan digitale sertifikater utstedes og behandles på et gitt bruksområdet og hvordan ansvaret for sikkerheten ved dette ivaretas. Sertifikatpolicyen fastsetter sikkerhetsnivået for utstedelse og behandling av sertifikater og derigjennom tillitsnivået sertifikatet representerer.

En utsteder av sertifikater vil alltid måtte være i stand til å framvise den sertifikatpolicyen som han utsteder sertifikater etter.

En sertifikatutsteder kan operere etter flere sertifikatpolicyer. For eksempel spesifiserer policyer om en bruker trenger å møte fram personlig for å få utstedt et sertifikat eller om sertifikatet kan sendes via e-post. Ulike prosedyrer kan gi ulik tillit til sertifikatene.

Det er viktig å merke seg at en sertifikatpolicy er et dokument som er unikt identifisert på global basis. Dette skjer ved at en policy registreres hos den internasjonale standardiseringsorganisasjonen ISO og der får den tildelt et unikt nummer såkalt OID (Object IDentifier) som skiller dette dokumentet fra alle andre dokumenter. Vurdering av tillitsnivå for et sertifikat kan således foregå ved at det i sertifikatet står OID ved den sertifikatpolicy som sertifikatet er utstedt etter. Ved å følge pekeren til dokumentet og ved å lese det kan brukeren få et bilde av sikkerheten ved dette sertifikatet. Dette er selvfølgelig en altfor tungvint metode for å vurdere hvert enkelt sertifikat som man kommer over. Innføringen av kvalifiserte sertifikater gjennom EU-direktivet er ment å skulle forenkle dette ved at det skal være et standardisert sikkerhetsnivå for slike sertifikater (jf. omtalen under punkt 8.2.5).

En sertifikatpolicy vil blant annet omfatte følgende elementer:

1. Området policyen virker på (hvordan sertifikatene som utstedes vil bli brukt)
2. Organiseringen av sertifikatutsteders virksomhet
3. Utstederens generelle forpliktelser
4. Hvordan identitetskontroll ved utstedelse av sertifikater foregår
5. Operasjonelle krav til driften av utstedersystemet
6. Hvordan de fysiske og administrative sikkerhetstiltakene gjennomføres
7. Hvilket teknisk sikkerhetsnivå tjenesten opererer på og
8. Hvilke sertifikatprofilerog profiler for tilbaketrekkingslisten som tjenesten benytter.

Et eksempel på en sertifikatpolicy er Forvaltningsnettsamarbeidets sertifikatpolicy FSP-1 [2]. FSP-1 har OID 216578112111. Denne sertifikatpolicyen har ErgoGroup (tidl. Posten SDS) Telenor og Strålfors implementert i forbindelse med leveranse av tjenester under rammeavtalen under Forvaltningsnettsamarbeidet.

Private aktører i markedet som utsteder sertifikater kan definere egne sertifikatpolicyer i tillegg til å implementere policyer som f.eks. forvaltningen ønsker å benytte.

Sertifikatpolicyer utgjør en del av en politikk for bruk av digitale signaturer og PKI. Forvaltningen må derfor klargjøre sine krav til sertifikatpolicy. Kravene må baseres på forutsetninger i regelverket som ligger til grunn for offentlig virksomhet. Dette kan variere fra sektor til sektor og fra virksomhet til virksomhet. Regelverket vil danne utgangspunktet for krav til sikkerhet ved forvaltningens elektroniske tjenester og interne systemer. Krav til sikkerhet må så nedfelles i en sertifikatpolicy.

Ulike elektroniske tjenester som f.eks. tilgang til byggesaker eller innsyn i egen helseinformasjon kan ha ulike krav til sikkerheten ved de digitale signaturene (sertifikatene) som man ønsker å benytte i forbindelse med bruk av tjenestene. Hvis flere forvaltningsvirksomheter stiller tilnærmet like sikkerhetskrav til sine tjenester kan de benytte samme sertifikatpolicy.

8.2 Sikkerhetsnivåer

Sertifikatpolicyer kan tilhøre ulike sikkerhetsnivåer for sertifikatutstedelse. Sikkerhetsnivåer sier noe om hvilken tillit man kan ha til sertifikatene og dermed i hvilke sammenhenger de kan brukes.

Sikkerhetsnivåer vil vanligvis være *hierarkiske* i den forstand at sertifikater utstedt på et lavt sikkerhetsnivå f.eks. vil kunne brukes bare for tilgang til bestemte anvendelser. Sertifikater utstedt på et høyere sikkerhetsnivå vil kunne benyttes for andre typer anvendelser med strengere sikkerhetskrav. De samme sertifikatene vil også kunne brukes for de anvendelsene som sertifikatene med lavere nivå gir tilgang til.

8.2.1 Hva kan skille sikkerhetsnivåer?

Et sikkerhetsnivå for utstedelse av sertifikater hos en sertifikatutsteder vil bestemmes av kravene som beskrives i de ulike delene av en sertifikatpolicy for dette nivået. For de fleste sertifikattyper vil det finnes noen felles krav. De vil finnes i flere policyer for ulike nivåer. Men policyene vil skille seg fra hverandre på bestemte områder avhengig av hva slags sikkerhetsnivå det dreier seg om. Slike områder eller kriterier er:

- Hvordan sertifikateieren identifiseres og registreres
- Hvordan utlevering av private nøkler og sertifikater skal foregå
- Algoritmer som kan brukes og nøkkellengder
- Hvordan nøkler genereres
- Antall nøkkelpar og hvordan nøklene kan brukes
- Hvordan de private nøklene beskyttes
- Hvordan sertifikater trekkes tilbake.

8.2.2 Beskrivelse av kriterier for å bestemme sikkerhetsnivå

Identifisering av sertifikateier

Et sertifikat vil ha større tillit hvis sertifikatutsteder har sjekket opplysninger om sertifikateieren grundig og på grunnlag av tillitvekkende dokumenter. I Norge kan sertifikatutstedere be om personens fødselsnummer for så å foreta oppslag i folkeregisteret. De må imidlertid være sikre på at det oppgitte fødselsnummeret virkelig tilhører den personen som kom med det. Dette kan gjøres ved å vurdere en tillitvekkende legitimasjon med bilde av personen der nummeret er med. Dette innebærer at personen helst bør møte opp fysisk for helt sikker identifisering. Eksempel på identifiseringsprosedyrer er bankenes prosedyrer for registrering av nye kunder som reguleres av en egen forskrift.[18] Den internasjonalt kjente sertifikatutstederen VeriSign kan utstede en type sertifikat kun på grunnlag av e-postadressen som oppgis av den som ønsker sertifikatet utstedt.

Utlevering av private nøkler og sertifikater

18

Alle banker forholder seg til Kredittilsynets forskrift FOR 1994-02-07 nr. 118: *Forskrift om legitimasjonskontroll og tiltak mot hvitvasking av penger* sist endret i 1998.

Prosedyrer for utlevering av private nøkler og sertifikater er avhengig av hvordan og av hvem de private nøklene blir generert. Dersom eieren genererer sine nøkler selv behøver vedkommende i prinsippet ikke å møte opp personlig. Et sertifikat for eierens offentlige nøkkel vil utstederen legge i en katalog. Et sertifikat som hentes fra en katalog eller som sendes til eieren via e-post vil oppfattes som mindre sikkert enn der eieren må møte fram identifisere seg og vise at hun har tilgang til den tilhørende private nøkkelen. Et sertifikat som bare sendes sertifikateieren via e-post vil alltid være et «mykt» sertifikat dvs. at sertifikatet og den tilhørende private nøkkelen lagres i en datafil. Dersom den private nøkkelen genereres av sertifikatutstederen er det en sikrere prosedyre hvis sertifikateieren møter fram og mottar (etter legitimering) en diskett eller et smartkort med nøkkelen enn at den sendes/hentes kryptert over nett. Tilliten til et sertifikat vil også variere med om utstederen kan garantere at den tilhørende private nøkkelen alltid har vært under full kontroll av utsteder eller eier.

Algoritmer som kan brukes og nøkkellengder

Teknologien som ligger til grunn for digitale signaturer asymmetrisk kryptografi innebærer bruk av såkalte asymmetriske krypteringsalgoritmer. Disse algoritmene er i stand til å finne ut om det var den riktige private nøkkelen som ble brukt ved signering eller autentisering. Den samme algoritmen vil også kunne dekryptere den nøkkelen som ble brukt til forvrenging av dokumentinnholdet slik at innholdet i dokumentet kan dekrypteres også. Ved digital signering brukes i tillegg såkalte hash-algoritmer og ved kryptering av dokumentinnholdet brukes en symmetrisk krypteringsalgoritme i tillegg til den asymmetriske. Alle disse algoritmene må være av god kvalitet. For asymmetriske algoritmer betyr det at den private nøkkelen skal være umulig å utlede fra den offentlige for hash-algoritmer betyr det at sannsynligheten for å generere samme resultat på to ulike dokumenter bør være lik null og for symmetriske kryptoalgoritmer bør det være umulig å finne nøkkelen ved å analysere den forvrengte teksten. Kvaliteten på kryptoalgoritmer avhenger av hvor lange[19]nøklene er – jo lengre nøkler jo bedre kvalitet. Men nøkkellengden er ikke det eneste som er viktig – også selve den matematiske oppbyggingen av algoritmen har mye å si.

Tabell 8.1 over nøkkellengder og tiden det tar å bryte en symmetrisk kryptoalgoritme[*)]

Nøkkellengde	Individuell hacker	Liten gruppe	Akademisk gruppe	Stor virksomhet	Etterretningstjeneste
40 bit	Uker	Dager	Timer	Millisek	Mikrosek
56 bit	> 100 år	> 10 år	År	Timer	Sek
64 bit	> 1000 år	> 100 år	> 10 år	Dager	Minutter
80 bit	Ikke praktisk	Ikke praktisk	Ikke praktisk	> 100 år	> 100 år
128 bit	Ikke praktisk	Ikke praktisk	Ikke praktisk	Ikke praktisk	> 1000 år

[*)] Tabellen er hentet fra den danske utredningen *Sammenfattende evaluering af Forskningsministeriets pilotprosjekter om digital signatur* publisert i september 2000.

Som tabellen illustrerer kan kryptosystemer brytes over tid og nøklene bli for korte. Dette skaper sikkerhetsmessige utfordringer og er også årsaken til at nøkler og sertifikater utstedes for begrensede

19 Lengden for nøkler oppgis vanligvis i antall bits.

perioder. Kvaliteten på algoritmene har betydning for tilliten til signaturen og for tilliten til konfidensialitetssikringen som bruk av PKI kan gi.

Hvordan nøkler genereres

Nøkler kan genereres på ulike måter. Nøkler kan genereres enten av sertifikatutsteder eller dennes underleverandør. De kan også genereres av eieren selv. Det finnes programvare for PC-er som er lagt til rette for det. Nøkler til VeriSign-sertifikater[20]genereres i PC-en. Da reiser spørsmålet seg om hvor tillitvekkende denne programvaren er og hvor godt beskyttet en PC er mot ondsinnede angrep.

Nøkler generert av brukeren selv vil alltid være «myke» nøkler dvs. lagret i en kryptert fil i PC-en. Hos en sertifikatutsteder kan nøkler genereres i et lukket og beskyttet datasystem og deretter bli lagt på en spesialdiskett på et smartkort eller i en kryptert datafil som utleveres eieren (jf. avsnittet om utlevering). Nøkler kan også genereres direkte på smartkortet (av utstederen eller en kortprodusent) slik at den private nøkkelen aldri forlater dette kortet. Valg av genereringsmetode vil ha betydning for tilliten til nøklene og dermed tilliten til signering mv.

Hvordan nøkler kan brukes

En PKI kan gi støtte for tre ulike funksjoner – signering av dokumenter kryptering av dokumenters innhold og også identifisering (autentisering) av kommuniserende parter på nettet. Alle disse funksjonene kan i prinsippet utføres ved å bruke ett nøkkelpar der det i sertifikatet for den offentlige nøkkelen vil stå at denne nøkkelen kan brukes til alle tre. Dette er dog en mindre sikker måte å bruke PKI på. Av grunner omtalt nedenfor bør en bruker ha flere sett av asymmetriske nøkler:

- Én nøkkel til autentisering ved f.eks. pålogging til et system
- Én nøkkel til signering for ikke-benekting av et dokument/melding og
- Én nøkkel til kryptering (av symmetriske engangsnøkler).

Dersom man bruker en nøkkel som er merket for både signering og autentisering kan man ved autentisering overfor et ukjent system risikere å signere et dokument uten å vite det. Sannsynligheten for dette er neppe stor men det gir en utrygghet. Videre ønsker man i noen situasjoner ikke å signere et dokument digitalt men man vil sikre at det ikke endres ved oversendelse (integritet) og at mottakeren vet sikkert hvor det kommer fra. Da kan man bruke en autentiseringsnøkkel men den må kun være merket for den bruken ellers vil mottakeren anta at dette dokumentet er signert for ikke-benekting.

Forvaltningen og eventuelt andre arbeidsgivere kan ha behov for å ha kopi av ansattes private nøkler som brukes til kryptering (jf. kapittel 11). Hvis nøkkelen har flere funksjoner vil man f.eks. kunne komme til å ta kopi av nøkkelen for signering samtidig. Dette er en svært lite ønskelig praksis.

Dette tilsier at separate nøkkelpar for alle tre funksjoner er ønskelig. Programvare for signering og kryptering som finnes i markedet gir full støtte til bruk av to ulike nøkkelpar. Men ikke alle produkter kan bruke tre nøkkelpar. På grunn av dette vil det i en overgangsfase være behov for å bruke to nøkkelpar med de tre funksjonene «fordelt» på dem. Det pågår diskusjoner om hvordan slik fordeling skal være. Forvaltningen i enkelte land satser på ett nøkkelpar til både signering og autentisering mens andre heller vil ha et separat nøkkelpar for signering og det andre for de resterende funksjonene. Behovet for kopi av krypteringsnøkkelen tilsier igjen at dette nøkkelparet bør være separat.

Bruken av nøkkelpar påvirker også tilliten til digitale signaturer og PKI. Tre separate nøkkelpar gir ikke rom for uklarheter og inngir dermed størst tillit.

20

http://www.verisign.com/

Hvordan nøklene beskyttes og signaturer framstilles

En privat nøkkel kan lagres kryptert i en datafil på en spesialdiskett på et smartkort på et såkalt PCMCIA-kort[21]eller i spesialelektronikk (f.eks. i en server). Tilgang til å bruke nøkkelen får brukeren ved å taste inn en PIN-kode eller et passord. Man kan også bruke såkalte biometriske metoder istedenfor PIN eller passord for å få tilgang til private nøkler. Et eksempel på en slik metode er lesing av fingeravtrykket. Utbredelsen av utstyr til dette er ennå liten.

PIN-koder og passord bør kunne bestemmes av nøkkeleieren selv. Dette fordrer imidlertid at det finnes adekvat kontrollprogramvare som sørger for at de valgte PIN-kodene og passordene er av tilstrekkelig god kvalitet.

En nøkkel som lagres og brukes i et smartkort og beskyttes med PIN-kode regnes for å gi høy grad av tillit til at bare eieren kan benytte den. Private nøkler lagret i en PC vil også bli beskyttet med en PIN-kode eller et passord men det er større risiko for at nøklene kan bli kompromittert og de gir derfor ikke samme tillit. En potensiell angriper vil bl.a. trenge spesialutstyr for å «bryte seg inn» i et smartkort.

Enkelte programmer for signering/kryptering gir tilgang til nøkler lagret i en PC slik at de er «åpent» tilgjengelige over en gitt tidsperiode som kan bli lang. Brukeren kan selv bestemme varigheten men dette åpner for økt sårbarhet.

For å underbygge underskriftens varslingsfunksjon er det viktig å gjøre det å signere digitalt til en eksplisitt handling. I praksis kan dette innebære at man må taste en PIN-kode eller et passord hver gang man skal signere. På grunn av dette og av sikkerhetsmessige grunner bør brukeren som har private nøkler lagret i en PC eller på et smartkort som står i en leser taste sin PIN-kode eller sitt passord hver gang hun signerer et dokument autentiserer seg overfor et system eller dekrypterer et mottatt kryptert dokument.

I hht. lov om elektronisk signatur [52] kreves det sikre signaturframstillingssystemer for å kunne framstille kvalifiserte signaturer. På oppdrag fra EESSI (jf. punkt 5.1.1) utarbeider CEN for tiden krav til sikre signaturframstillingssystemer. Det er alminnelig antatt at slike systemer minimum innebærer bruk av smartkort. Situasjonen på dette området er imidlertid uavklart og det nasjonale arbeidet med forskrifter til loven vil måtte avvente resultater fra EU-prosesser før kravene i den norske loven kan presiseres.

Hvordan sertifikater trekkes tilbake

Tilbaketrekking (sperring) av sertifikater tilsvarer «svartelisting» av betalingskort som er blitt mistet eller stjålet. Et sperret sertifikat indikerer at en ikke kan stole på signaturen som ble laget med dette sertifikatet etter tilbaketrekkingstidspunktet.

Et sertifikat kan trekkes tilbake av mange grunner noen av dem så uskyldige som at man har endret navn og derfor må få et nytt sertifikat med det nye navnet. Sertifikater som har nådd utløpet av sin gyldighetsperiode vil også bli trukket tilbake og nye bli utstedt. Sertifikater må straks trekkes tilbake når det er mistanke om at den tilhørende private nøkkelen er kompromittert eller tapt.

Det er sertifikateierens ansvar å varsle utstederen om tap/kompromittering av nøkler eller om endringer i personlige opplysninger som vil påvirke innholdet i sertifikatet.

Det er utstederens ansvar å sperre sertifikatet. Dette gjøres ved å utstede såkalte tilbaketrekkingslister som er tidsstemplet og signert av sertifikatutstederen. Hvor ofte slike lister utstedes er svært viktig for tilliten til den digitale signaturen. Utstedes listene en gang om dagen er tilliten en annen enn om de utstedes hver halvtime.

Prosedyrer for tilbaketrekking har derfor stor betydning for hvor sikre sertifikater og signaturer er. Dersom man ikke har gode tilbaketrekkingsrutiner blir misbruk av en digital signatur mye vanskeligere å oppdage enn misbruk av en tilsvarende papirbasert signatur.

21

PCMCIA-kort er et standardisert innstikkskort til PC-er

8.2.3 Andre momenter som påvirker tillit til en sertifikatpolicy

En sertifikatutsteder skal beskrive i et eget dokument hvordan en gitt sertifikatpolicy følges hos ham. Dette dokumentet kalles sertifikatpraksis[22] For at en bruker av sertifikatutstederens tjenester skal ha mulighet til å vurdere om utstederen virkelig følger sertifikatpolicyen må det gjennomføres en sikkerhetsevaluering av utsteders virksomhet med tanke på om rutiner og tiltak beskrevet i sertifikatpraksis virkelig følges.

En slik evaluering kan gjennomføres av et IT-revisjonsselskap som også kan være akkreditert for evalueringer etter BS 7799. BS 7799 er en standard for evaluering av sikkerhet i organisasjoner. Den brukes i flere land og er nå også i bruk i Norge. Standarden regnes som fleksibel men noe uklar. Den kan derfor ikke brukes alene for evaluering av en sertifikatpraksis men kan være et godt hjelpemiddel.

Det foreligger pr. i dag ingen lovfestede krav til de IT-revisjonsfirmaene som kan gjennomføre revisjon av en sertifikatutsteder. Lov om elektronisk signatur § 17 fjerde ledd gir tilsynet anledning til å kreve slik revisjon av utstedere. Det er ikke et krav at revisorer skal ha akkreditering for BS 7799.

Sertifikatpolicyer er ofte tungt tilgjengelige dokumenter som i liten grad er forståelige for brukerne. De kan heller ikke tolkes automatisk av datamaskiner. Dette påvirker brukernes praktiske muligheter til å vurdere hva slags tillit de kan ha til en sertifikatutsteder.

En utsteder av kvalifiserte sertifikater vil måtte dokumentere at han i sin sertifikatpolicy oppfyller visse standardiserte krav og hans virksomhet vil være underlagt tilsyn. Dette kan gjøre det lettere å forholde seg til tillitsspørsmålet.

Sjekking av sertifikatpolicyer er ikke særegent for forvaltningen. Det vil være utfordrende i alle tilfeller der man ikke har avtaler med sertifikatutsteder. Det kan f.eks. tenkes en instruks for postmottaket om å sjekke sertifikatpolicyer ved manuelt mottak av visse typer e-post som kan utløse saksbehandling og der det følger med et sertifikat fra en ukjent utsteder. Dette kan f.eks. gjøres mot en separat samtrafikktjeneste jf. punkt 10.10.7.

8.2.4 Behov for sertifikatpolicy

Trenger forvaltningen egne sertifikatpolicyer? Trenger man én eller flere policyer? Disse spørsmålene kan besvares på flere plan.

For hver elektroniske tjeneste eller annen IT-anvendelse i forvaltningen er det nødvendig å bestemme krav til sikkerhet. Disse kravene vil være forankret i regelverket som ligger til grunn for tjenesten/anvendelsen. Dersom man skal ta i bruk digitale signaturer og PKI som sikkerhetsløsning må kravene omsettes i en beslutning om hvilket sikkerhetsnivå med tilhørende sertifikatpolicy som skal legges til grunn.

Sikkerhetsbestemmelsene gitt i medhold av personopplysningsloven pålegger den behandlingsansvarlige å iverksette sikkerhetstiltak i forhold til den risikoen behandlingen medfører. Kravet til forholdsmessighet medfører at valg av sikkerhetsnivå og -tiltak må baseres på risikovurdering utført for den enkelte konkrete behandling. Bildet kompliseres ved at personopplysninger skal sikres ut fra forskjellige ofte avvikende hensyn: konfidensialitet integritet eller tilgjengelighet. Eksempelvis vil en for sterk konfidensialitetssikring kunne forårsake utilstrekkelig tilgang til opplysningene og dermed medføre et sikkerhetsproblem.

Dette innebærer at evaluering og valg av sikkerhetsnivå må baseres på en forutgående vurdering av risiko knyttet til den enkelte behandling. Slike risikoanalyser bør ta med vurderinger om hvorvidt systemer som har akseptabelt risikonivå for systemeier gir for høy risiko for den enkelte private bruker.

22

eng. CPS – Certificate Practice Statement.

.

Hver enkelt etats vurderinger vil kunne føre til at det utvikles mange nesten like sertifikatpolicyer for ulike anvendelser i forvaltningen. Utvikling av sertifikatpolicyer krever kompetanse og innsikt i PKI-området noe som ikke vil være tilgjengelig i like stor grad for alle virksomheter. Det er derfor naturlig å vurdere noen felles tiltak som kan lette arbeidet i hver enkelt virksomhet. Ett slikt tiltak er felles rammeavtaler.

Eksisterende tilbud av digital signatur-produkter og -tjenester i forbindelse med Forvaltningsnettsamarbeidets rammeavtaler baserer seg på én sertifikatpolicy med høyt sikkerhetsnivå (FSP-1). Denne policyen dekker hovedsakelig forvaltningsinterne forhold og tar ikke hensyn til kommunikasjon med forvaltningens brukere f.eks. enkeltpersoner.

Ut fra spennvidden i forvaltningens behov ser utvalget det som hensiktsmessig at det defineres flere felles sikkerhetsnivåer med tilhørende felles sertifikatpolicyer. Slike nivåer kan danne en referanseramme for valg av sikkerhetsnivå for tjenester og anvendelser i forvaltningen og mot forvaltningens brukere.

Felles løsninger på en del områder vil kunne lette innføring av bruk av digitale signaturer og forenkle enkeltpersoners og næringslivets elektroniske kommunikasjon med forvaltningen som helhet.

Utgangspunktet for valg av policy er eksisterende policy hos leverandørene Forvaltningsnettsamarbeidets sertifikatpolicy FSP-1 som i praksis fungerer som offentlig anbefalt sertifikatpolicy i dag og de standard sertifikatpolicyer som er utarbeidet av ETSI (*Policy requirements for certification authorities issuing qualified certificates* ETSI TS 101 456) [23].

ETSI-standarden kan få betydning for implementeringen av direktivet 1999/93/EC når det gjelder hva som skal legges til grunn for utstedere av kvalifiserte sertifikater. Det vil trolig være naturlig at denne standarden vil danne en mal for de nasjonale tilsynsmyndigheter når det gjelder evaluering av sertifikatpolicy og derigjennom sikkerheten hos utstedere av kvalifiserte sertifikater.

ETSI-standarden definerer faktisk to sertifikatpolicyer – begge for utstedere av kvalifiserte sertifikater «til offentligheten» et begrep som vil fortolkes ulikt i nasjonale lovgivninger på området. I henhold til norsk lov om elektronisk signatur vil dette gjelde alle utstedere av kvalifiserte sertifikater. De to sertifikatpolicyene som defineres er identiske i innhold på de fleste punkter men skiller seg fra hverandre på området krav til sikkert signaturframstillingssystem og på måten private nøkler skal beskyttes på. Den ene av policyene stipulerer et sikkert signaturframstillingssystem (som pr. i dag stort sett vil bety smartkort) den andre gjør det ikke.

I tillegg til at ETSI-standarden definerer de to konkrete sertifikatpolicyene åpner man for at enkelte sertifikatutstedere skal kunne utarbeide egne mer detaljerte policyer på grunnlag av den ene av de to standardpolicyene. På denne måten fungerer standarden som en «rammepolicy» som kan fylles ut med mer detaljert innhold og tilpasses lokale forhold. En slik ny policy vil måtte registreres og identifiseres separat fra ETSI-policyer.

ETSI's sertifikatpolicy har ikke brukt Internettstandarden RFC 2527 som mal for struktur og disposisjon for policydokumentet. Den inneholder likevel en tabell som sammenholder de ulike avsnittene og kapitlene til strukturen iht. RFC 2527.

FSP-1 utarbeidet med utgangspunkt i den svenske SEIS S10-standarden [68] baserer seg på RFC 2527. Innholdsmessig tilsvarer FSP-1 ETSI's policy med sikkert signaturframstillingssystem selv om FSP-1 er mer detaljert og således representerer en videreutvikling i forhold til ETSI-policy.

8.2.5 Anbefaling om antall sikkerhetsnivåer og tilhørende policyer

Én sertifikatpolicy med høy sikkerhet som kan dekke de fleste behov vil kunne forenkle implementeringen av PKI både i forvaltningens interne samhandling og enkeltpersoners elektroniske kontakt med forvaltningen.

Utvalget ser likevel behov for minst ett nivå til med noe lavere sikkerhet. Grunnen er at løsninger for digitale signaturer og PKI som kan tilsvare høyt sikkerhetsnivå ikke er bredt tilgjengelig i markedet ennå. I tillegg vil implementering av sterke sikkerhetsløsninger for elektroniske tjenester som ikke nødvendigvis behøver slike kunne medføre unødige kostnader og eventuelle forsinkelser ved innføring av tjenestene.

Utvalget anbefaler to nivåer med høye krav til sikkerhet og ett nivå uten spesielle krav til sikkerhet. Nivåene er rangert slik at nivå 3 gir høyest sikkerhet og nivå 1 lavest sikkerhet. Nivå 3 krever sikkert

signaturframstillingssystem mens nivå 2 aksepterer annen lagring av private nøkler. Utvalget mener at digitale signaturer på nivå 3 vil tilfredsstille de kravene til kvalifisert elektronisk signatur som framgår av lov om elektronisk signatur.

Nivå 3

Felles sertifikatpolicy for dette nivået anbefales å være FSP-1 med visse modifikasjoner. Modifikasjonene bør omfatte tilpasning av FSP-1 til strukturen på ETSI's standard sertifikatpolicy med sikkert signaturframstillingssystem. Videre bør FSP-1 modifiseres for å tilpasses de nye anbefalte sertifikatprofilene for forvaltningen (jf. vedlegg 2).

Noen viktige momenter i policyen vil være:

- Tre separate nøkkelpar for henholdsvis signering kryptering og autentisering
- RSA kryptosystem med 1024 bits nøkler eller annet asymmetrisk kryptosystem med tilsvarende eller bedre sikkerhet
- SHA-1 hash-algoritme eller annet hash-system med tilsvarende eller bedre sikkerhet
- 3DES eller AES med 128 bits nøkler eller annet symmetrisk kryptosystem med tilsvarende eller bedre sikkerhet
- Private nøkler lagres på smartkort eller annet utstyr som vil oppfylle kravene til sikkert signaturframstillingssystem iht. lov om elektronisk signatur med forskrifter. Utvalget forutsetter at disse kravene blant annet vil innebære at:
- Signaturframstillingssystemet beskytter de private nøklene slik at de ikke kan forlate systemet bli slettet eller overskrevet
- Tilgang til private nøkler er beskyttet med PIN-kode eller passord med tilstrekkelig styrke

Signaturframstillingssystemet er evaluert til et tillitsnivå som minimum tilsvarer EAL 4 etter Common Criteria[23] [43]

- Systemer med automatisk tilgang til private nøkler for virksomheter må sikres mot uautorisert tilgang til nøklene med mekanismer evaluert til et tillitsnivå som minimum tilsvarer EAL 4 etter Common Criteria
- Ved identifisering av sertifikateier skal utsteder sjekke medbrakt legitimasjon mot folkeregisteret. Virksomhetssertifikater krever en tilsvarende mekanisme
- Identifisering av sertifikateier (for offentlige personsertifikater) ved hjelp av en identifikator som er unik innen utsteders domene ev. fødselsnummer
- Personlig frammøte minst én gang i forbindelse med utstedelse av sertifikat
- Tilbaketrekkingstjeneste tilgjengelig 24 timer i døgnet 7 dager i uken.

Nivå 2

23

Common Criteria er en internasjonal standardmåte å evaluere sikkerhet i IT-produkter og -systemer på.

Her stilles samme krav som til sertifikater på høyeste nivå bortsett fra at private nøkler ikke behøver å beskyttes ved hjelp av et sikkert signaturframstillingssystem. I praksis kan dette bety at nøklene kan lagres kryptert i PC-en på en server eller på en diskett. Felles sertifikatpolicy på dette nivået anbefales å være FSP-1 tilpasset ETSI's standard sertifikatpolicy uten krav til sikkert signaturframstillingssystem og modifisert som omtalt ovenfor.

Nivå 1

Dette nivået er definert av rent praktiske grunner og omfatter alle andre typer sertifikater enn de definert på nivå 3 og 2 (for eksempel sertifikater utstedt av den internasjonalt kjente tjenesten VeriSign). Likeledes kan andre former for elektroniske signaturer som PIN-koder grupperes her. På dette nivået er det ikke hensiktsmessig å kreve bestemte sertifikatpolicyer.

8.3 Obligatorisk eller anbefalt policy

Dersom det er ønskelig å legge til rette på en enkel måte for en PKI for forvaltningen med gjennomgående høy sikkerhet kan det være hensiktsmessig å pålegge forvaltningsvirksomheter å anskaffe PKI-løsninger med et bestemt høyt sikkerhetsnivå. Slike løsninger kan være tilgjengelige via en rammeavtale som virksomhetene vil være pålagt å bruke. Denne typen sentralt grep vil kunne forhindre at enkelte forvaltningsvirksomheter går utenom rammeavtalen og på egen hånd anskaffer løsninger i markedet med svakere sikkerhet enn den som tilbys i rammeavtalen. Slik tilnærming har imidlertid flere ulemper enn fordeler.

Hvis det sikkerhetsnivået og den sertifikatpolicyen som er knyttet til rammeavtalen ikke er dekkende for behovet enten fordi det er for høyt eller for lavt vil obligatoriske løsninger både ramme virksomhetens handlefrihet med henblikk på å løse oppgavene på en mest effektiv måte og generere unødige kostnader for virksomheten isolert.

Obligatoriske løsninger vil stå i motstrid til virksomhetens plikt og rett til å vurdere behovet for sikkerhet i dennes elektroniske samhandling med andre på grunnlag av egne behov og det regelverket som ligger til grunn for virksomheten for så å velge en optimal løsning.

På den andre siden er PKI en infrastruktur som skal tilby de samhandlende partene tjenester til felles bruk. Dersom de samhandlende partene velger ulike sikkerhetsnivåer på hver sin side vil samhandlingen ikke være sikrere enn tilsvarende det laveste av de aktuelle sikkerhetsnivåene.

Utvalget ser det derfor som hensiktsmessig at det finnes anbefalte sikkerhetsnivåer og tilhørende sertifikatpolicyer. Utvalget ser ingen tungtveiende grunner til å gjøre de foreslåtte felles sikkerhetsnivåene og sertifikatpolicyene obligatoriske for forvaltningen. Utvalget mener at det kan være hensiktsmessig å kreve at de felles anbefalte nivåene vurderes først før eventuelt andre løsninger velges.

Utvalget mener at de felles anbefalte sertifikatpolicyene vil kunne tas i bruk på frivillig basis av forvaltningen slik de er. Utvalget mener at disse sertifikatpolicyene om ønskelig også vil kunne fungere som rammepolicyer og benyttes som grunnlag for utvikling av spesifikke og mer detaljerte policyer for konkrete anvendelser i konkrete virksomheter.

8.4 Forvaltningsnettsamarbeidets sertifikatpolicy FSP-1

FSP-1 ble utarbeidet i 1999 av Forvaltningsnettsamarbeidet i forbindelse med rammeavtale om digitale signaturer med tilhørende tjenester. FSP-1 er en høysikkerhetspolicy som høyst sannsynlig oppfyller kravene til kvalifiserte signaturer slik kravene framgår av lov om elektronisk signatur. FSP-1 har godt omdømme både hos sertifikatutstedere og hos forvaltningen. FSP-1 har i praksis fungert som en anbefalt standard for forvaltningen.

Utvalget mener at FSP-1 er et godt utgangspunkt for en ny anbefalt standard for sertifikatpolicy for forvaltningen. Den nye standarden bør være de to sertifikatpolicyene for henholdsvis sikkerhetsnivå 3 og sikkerhetsnivå 2 som omtales i punkt 8.2.5.

8.5 Oppsummering av anbefalingene

Utvalget anbefaler at det for anvendelse av digitale signaturer og PKI i forvaltningen og i kommunikasjon med forvaltningens brukere defineres tre felles sikkerhetsnivåer.

Det høyeste nivået nivå 3 skal basere seg på en sertifikatpolicy som tar utgangspunk i Forvaltningsnettsamarbeidets sertifikatpolicy FSP-1 og tilsvarer den nylig vedtatte europeiske standarden fra ETSI for sertifikatpolicy for utstedelse av kvalifiserte sertifikater med sikkert signaturframstillingssystem.

Mellomnivået nivå 2 skal tilsvare nivå 3 i sikkerhet bortsett fra at det på dette nivået ikke skal kreves sikre signaturframstillingssystemer iht. lov om elektronisk signatur. Dette nivået skal også ha en tilhørende sertifikatpolicy som skal ta utgangspunkt i FSP-1 og den europeiske ETSI-standarden uten sikre signaturframstillingssystemer.

Laveste nivå nivå 1 omfatter alle andre sertifikater med sikkerhet lavere enn nivå 3 og 2. Andre typer sikkerhetsløsninger for autentisering som PIN-koder eller passord kan klassifiseres på dette nivået.

Utvalget anbefaler ikke at felles sikkerhetsnivåer og tilhørende sertifikatpolicyer gjøres til obligatoriske standarder for forvaltningen.

Utvalget mener at det bør vurderes om forvaltningen kan pålegges å ta stilling til fellesløsninger for PKI før andre løsninger kan velges.

Utvalget mener at Forvaltningsnettsamarbeidets sertifikatpolicy FSP-1 er et godt utgangspunkt for en ny anbefalt standard for forvaltningen. Den nye standarden bør være de to sertifikatpolicyene som utvalget anbefaler utviklet for sikkerhetsnivå 3 og sikkerhetsnivå 2 på grunnlag av ETSI-standarden TS 101 456.

9 Forvaltningens strategi for bruk av sertifikattjenester

Hensikten med dette kapitlet er å foreta en overordnet vurdering av hvordan forvaltningen skal kunne skaffe seg nødvendig infrastruktur for bruk av digitale signaturer og å anbefale en strategi framover.

9.1 Rammebetingelser for leveranse av sertifikattjenester til forvaltningens formål

9.1.1 Lover og regelverk

I § 5 i lov om elektronisk signatur slås det fast at Kongen kan fastsette nærmere regler om hvilke krav som skal stilles til kvalifiserte elektroniske signaturer som skal brukes ved kommunikasjon med og i offentlig sektor.

Nærings- og handelsdepartementet utarbeider i samarbeid med Post- og teletilsynet forskrifter til loven. Det ligger an til at leverandører av kvalifiserte sertifikater skal kunne avkreves opplysninger om hvilken sertifikatpolicy og sertifikatpraksis som benyttes ved utstedelse av kvalifiserte sertifikater. Når forskriften er på plass vil det være grunnlag for å vurdere hvorvidt det er nødvendig med tilleggskrav i offentlig sektor utover det som loven med forskrifter regulerer.

Enkelte offentlige aktører vurderer å stille krav om sikkerhetssertifisering av sertifikatutstedere som skal utstede sertifikater til visse anvendelser. En slik sertifiseringsordning basert på den britiske standarden BS 7799 er under etablering i Norge. Hvorvidt dette er nødvendig vil kunne vurderes når leverandørenes sertifikatpolicyer for levering av kvalifiserte sertifikater blir tilgjengelige.

9.1.2 Status blant aktuelle leverandører

Flere av leverandørene av sertifikattjenester har antydet at de vil utstede sertifikater med et innhold som tilsvarer kvalifiserte sertifikater. Det er fremdeles uklart hvor raskt migrasjonen til kvalifiserte sertifikater vil skje. Både tidsplanene og aktørenes vilje til å registrere seg som utsteder av kvalifiserte sertifikater vil være avhengige av myndighetenes politikk. Det synes som om aktørene avventer forskriften til loven før de fatter beslutninger på området.

Leverandører kan ønske å utstede sertifikater som ikke hører med til kategorien kvalifiserte. Slike sertifikater kan være like sikre eller sikrere enn kvalifiserte sertifikater men i forhold til lov om elektronisk signatur vil de falle under bestemmelser i § 6 annet ledd som sier at en elektronisk signatur ikke kan nektes rettsvirkning på grunnlag av at den er elektronisk.

9.2 Leveranse av sertifikater til forvaltningen

9.2.1 Hvor sikre sertifikater skal forvaltningen benytte?

Utvalget har ikke grunnlag for å anbefale hvilket sikkerhetsnivå for sertifikattjenester som bør benyttes for hvilke anvendelser i forvaltningen. Denne vurderingen må foretas av hver offentlig virksomhet individuelt i forbindelse med anskaffelse av PKI-løsninger. Se ellers kapittel 4 som peker på noen grunnleggende anvendelser med behov for digitale signaturer i forvaltningen.

Likevel vil utvalget mene at sertifikater som planlegges brukt av forvaltningen i hovedsak bør befinne seg på sikkerhetsnivå 3 (jf. kapittel 8) med tilsvarende sertifikatpolicy. Utvalget vil imidlertid ikke anbefale at sertifikater på nivå 2 skal utelukkes. Offentlige virksomheter bør kunne velge sertifikater på nivå 2 der behovet i forhold til en konkret anvendelse tilsier det. Samtidig bør virksomhetene ut fra et kost-/nytteperspektiv kunne vurdere om det er hensiktsmessig å investere i PKI-løsninger basert på sikkerhetsnivå 2 hvis man så skal gå over til løsninger på nivå 3 eller der man likevel har behov for løsninger på nivå 3 på visse områder mens det på andre områder bare er behov for løsninger på nivå 2. Det er kostbart å etablere en infrastruktur flere ganger eller å operere med doble ordninger.

9.2.2 Modeller for leveranse av sertifikater til forvaltningen

Det finnes tre grunnleggende modeller for leveranse av sertifikattjenester til forvaltningen:

- En sentral sertifikattjeneste etableres i forvaltningen
- Hver enkelt offentlig virksomhet (med behov for det) etablerer en slik tjeneste som en del av sine interne IT-funksjoner
- Tjenesten kjøpes i markedet enten direkte eller via rammeavtaler.

Disse modellene er ikke ekskluderende i forhold til hverandre og kan tenkes brukt i kombinasjon. Mer konkret kan følgende modeller overveies:

a) Hver enkelt etat kan kjøpe sertifikater fra en aktør i markedet etter anbudskonkurranse. Leverandøren forestår både registreringsfunksjonen og sertifikatutstedelsen. Alternativt kan etaten selv forestå registreringsfunksjonen. Denne modellen kan være egnet for store etater som har tilstrekkelig kompetanse og tyngde til å gjennomføre nødvendige anbudsprosesser. Etater med geografisk distribuerte enheter vil ha en tilleggsutfordring når det gjelder etablering av en effektiv registreringsfunksjon. Der må leverandøren enten sørge for en geografisk distribuert registreringsfunksjon eller etaten må selv finne interne løsninger for dette.

b) Hver enkelt etat kan kjøpe sertifikater gjennom Forvaltningsnettsamarbeidets rammeavtale. Dagens rammeavtale legger opp til at hver enkelt offentlig virksomhet som kjøper tjenesten skal forestå registreringsfunksjonen selv. Det er også lagt opp til en mulighet der en tredjepart kan forestå registreringstjenesten for flere virksomheter etter avtale med én eller flere sertifikatutstedere. Her bør det vurderes om denne ordningen bør suppleres med en mulighet der leverandørene selv forestår registreringsfunksjonen ev. også geografisk distribuert.

c) Offentlige etater etablerer sine egne sertifikatutstedelsestjenester. Dette er en modell som er aktuell for noen store statlige etater ev. store kommuner med mange etater. Egen sertifikattjeneste kan etableres enten ved å anskaffe nødvendig utstyr og programvare og sette opp hele tjenesten selv eller ved å kjøpe tjenesten i sin helhet i markedet som en underleveranse til etatens sertifikattjeneste. En slik anskaffelse kan enten skje via utlysning eller kjøp ifølge rammeavtaler gitt at Forvaltningsnettsamarbeidet tilbyr slike løsninger i tilknytning til sine avtaler.

d) Det etableres en sentral sertifikatutsteder for hele forvaltningen. Alternativt kan det etableres flere sentrale utstedere f.eks. en for departementene en for alle kommuner og en for statsforvaltningen for øvrig. Slike utstedere vil bli drevet i offentlig regi og vil mest sannsynlig være brukerfinansierte tjenester. Etablering av løsningene vil kunne skje som beskrevet for foregående modell der etater selv etablerer slike tjenester. Man må likevel merke seg at sertifikatutstedelse er en tjeneste som i grunnen ikke trenger å være distribuert i det hele tatt. Det som er viktig er å ha en rimelig distribuert løsning for registreringstjenester. Slik sett vil mest sannsynlig en variant av denne modellen være en sentral utsteder som har avtaler med flere enheter som kan forestå registrering av sertifikateiere. Slike enheter bør være geografisk (regionalt) distribuert for å kunne dekke hele forvaltningen. Det er nærliggende å tro at det vil være regionale offentlige virksomheter som kan ta på seg slike roller (f.eks. Fylkesmannsembeter eller administrasjonene i fylkeskommunene).

Man må ta stilling til om en slik offentlig sertifikatutsteder skal ha monopol på å utstede sertifikater til forvaltningen eller om dette skal skje i konkurranse med andre aktører i markedet slik det f.eks. legges opp til i Finland.

Fordeler med modeller som forutsetter anskaffelse av sertifikattjenester i markedet er:

- Fleksibilitet med tanke på valg av løsning og skifte av leverandør
- Mindre investeringskostnader for forvaltningen
- Bedre mulighet for å følge den teknologiske utviklingen og mulighet for valg av de til enhver tid mest optimale løsninger
- Gjennom konkurranse mellom aktører i markedet som utsteder sertifikater stimuleres utviklingen av markedet for sertifikattjenester.

Ulempene med disse modellene er:

- Begrenset offentlig kontroll over en vital infrastruktur hvis den f.eks. ikke fungerer etter forutsetningene
- Problemer med samtrafikk og teknisk samvirke mellom løsninger fra ulike leverandører
- Potensielt høye driftskostnader dersom leverandørtilfanget blir begrenset
- Mangel på nødvendig kompetanse for å ta løsningene i bruk.

Fordeler med en modell der forvaltningen selv driver sertifikatutstedelse for egne ansatte kan være:

- Bedre kontroll med sikkerhet og kvalitet i infrastrukturen
- Mer homogen infrastruktur lettere å eliminere samtrafikkproblemer og problemer med teknisk samvirke
- Bedre og rimeligere integrasjon av forvaltningens systemer med digitale signaturer (færre konsepter å ta hensyn til)
- Egen kompetanse i forvaltningen mindre avhengighet av leverandørene.

Ulempene kan være:

- Høye investeringskostnader potensielt høye driftskostnader usikker inntjening av utgifter
- Mindre fleksible løsninger. Det kan bli vanskeligere å tilpasse seg den teknologiske utviklingen på området
- Modellen kan forstyrre markedsutviklingen ved at det offentlige kan komme til å konkurrere med utstedere i markedet
- Dersom det blir en monopoltjeneste vil kvaliteten kunne synke over tid.

Utvalgets drøfting av ulike modeller har avdekket at etablering av en sentral offentlig utsteder av sertifikater er en lite aktuell løsning. Hensynet til markedsutvikling og hensynet til kontroll med offentlige utgifter må veie tungt når man skal vurdere valg av løsning for forvaltningen. Utvalget anser det som lite aktuelt å anbefale en modell der det offentlige skal pådra seg større utgifter samtidig som man vil kunne forstyrre konkurransen i markedet for sertifikattjenester.

Ved diskusjon av modeller der markedet skal kunne utnyttes til anskaffelse av løsninger la flere vekt på at det kan være hensiktsmessig å samordne krav og rammebetingelser for slike anskaffelser. Krav kan samordnes dersom man etablerer en sentral samordningsfunksjon (jf. punkt 9.6) for digitale signaturer i

forvaltningen men det kan være en tung oppgave særlig for mindre virksomheter selv å gjennomføre anskaffelsesprosessen. Man bør derfor kunne utnytte de felles innkjøpsordningene som finnes i forvaltningen i dette tilfellet innkjøpsordningen under Forvaltningsnettsamarbeidet som allerede har etablerte rammeavtaler for digitale signaturer og TTP-tjenester. Bruken av Forvaltningsnettsamarbeidets avtaler er frivillig.

Når det gjelder hva slags løsninger som bør omfattes av en slik rammeavtale mener utvalget at det bør åpnes for at enkelte store etater eller større kommuner selv skal kunne forestå utstedelse av sertifikater til egne ansatte. Dette fordrer at innholdet i rammeavtalen bør utvides med produkter og/eller tjenester som gjør det mulig.

9.2.3 Hvordan skal forvaltningen anskaffe sertifikater til egne formål?

Utvalget mener at for forvaltningens interne formål dvs. utstedelse av sertifikater til offentlige virksomheter og deres ansatte vil det være hensiktsmessig å videreføre ordningen med rammeavtaler under Forvaltningsnettsamarbeidet. Rammeavtaleinnholdet bør utvides slik at det kan omfatte:

- Sertifikattjenester (som i dag)
- Produkter for digitale signaturer og kryptering (som i dag)
- Smartkort og lesere (som i dag)
- Produkter for sertifikatutstedelse og produkter som støtter sertifikatkataloger (ny)
- Outsourcing av sertifikattjenester (ny).

Rammeavtalen bør baseres på krav utarbeidet av en samordningsfunksjon (jf. punkt 9.6) med utgangspunkt i utvalgets anbefalinger om sikkerhetsnivåer sertifikatprofiler unik identifisering og sertifikatpolicy. Til avtalen bør det være tilgjengelige tjenester og produkter som tilfredsstiller både sikkerhetsnivå 3 og 2. Videre bør det juridiske rammeverket for avtalen ta hensyn til nyreguleringen på området (lov om elektronisk signatur med forskrift kommende endringer i forvaltningsloven og ev. en ny forskrift om elektronisk kommunikasjon med og i forvaltningen).

Bruken av rammeavtalen bør være frivillig men samtidig bør det være en anbefalt løsning for anskaffelse av sertifikater til forvaltningen. Dersom en offentlig virksomhet skulle velge å gjennomføre en anskaffelsesprosess uten å benytte Forvaltningsnettsamarbeidets innkjøpsordning anbefaler utvalget at basiskrav og betingelser som legges til grunn for en slik anskaffelse er de samme som for rammeavtalen.

Når det gjelder spørsmålet om samtrafikk mellom leverandører som skal tilby løsninger til forvaltningen under rammeavtalen foreslår utvalget at dette løses utenom selve rammeavtalene og at det vil være en av samordningsfunksjonens oppgaver å finne gode løsninger for dette i samarbeid med leverandørene. Se for øvrig kapittel 10.

9.3 Leveranse av sertifikater til enkeltpersoner

9.3.1 Privatpersoners kommunikasjon med forvaltningen

Privatpersoner ønsker sannsynligvis å benytte færrest mulig sertifikater i sin kommunikasjon mot forvaltningen. Fordelen med PKI er nettopp muligheten til å kunne tilby autentiseringsløsninger som er universelle for flere anvendelser slik at befolkningen ikke skal behøve å forholde seg til mange PIN-koder passord og andre elektroniske identifikasjonskoder for hver enkelt tjeneste de skal kunne bruke på Internett. Det kan likevel tenkes at enkeltpersoner kan ende opp med en løsning der privatpersoner vil ha flere nøkkelpar og sertifikater for kommunikasjon med offentlig sektor. Slike løsninger må da tilrettelegges slik at sertifikateieren er klar over hvilket sertifikat og hvilken privatnøkkel som benyttes mot hvilken tjeneste.

Når man tar i bruk PKI og digitale signaturer for tilgang til forvaltningens elektroniske tjenester kan forvaltningen legge til rette for at ett og samme sertifikat kan benyttes mot flere offentlige tjenester. Det kan også tenkes at hver sektor eller virksomhet krever separate sertifikater for sine formål. Hva disse svært

ulike strategiene innebærer for enkeltpersoner kan vurderes ut fra to perspektiver: forbrukerperspektiv og personvernperspektiv. Ut fra det første vil ønsket om å ha færrest mulig sertifikater å forholde seg til være dominerende. Ut fra det andre perspektivet kan ønsket om å benytte flere ulike sertifikater være aktuelt for personer som ikke nærer slik tillit til forvaltningen at de vil benytte samme identifikasjonsmekanisme mot flere offentlige virksomheter. Det er i denne sammenhengen verdt å merke seg at i dagens løsninger for tilgang til elektroniske tjenester på nettet benyttes fødselsnummer kombinert med en PIN-kode. Dette gir vesentlig dårligere personvern enn bruk av et sertifikat hvor fødselsnummeret ikke inngår.

Valget mellom disse hensynene bør foretas av brukeren selv men for at valget skal være reelt må det være noe å «velge imellom». Dette i seg selv tilsier at forvaltningen ikke bør ta et hardt grep og forlange at ett sertifikat skal brukes mot alle offentlige tjenester som tilbys elektronisk.

Samtidig vil mange sertifikateiere se det som en fordel om det sertifikatet som de bruker mot offentlige tjenester også kan brukes i andre sammenhenger f.eks. mot banktjenester eller andre private tjenester på Internett. Det skaper utfordringer for forvaltningen dersom man skal velge sektorløsninger framfor felles løsninger. Valg av sektorløsninger kan innebære at de private aktørene (f.eks. bankene) vil måtte tilpasse mange ulike offentlige sertifikater til bruk mot sine egne tjenester dersom slike ønsker fra enkeltpersoner skal oppfylles.

Utvalget ser det ikke som hensiktsmessig å anbefale ett sikkerhetsnivå for offentlige personsertifikater. Valg av sikkerhetsnivå vil i sterk grad avhenge av behovene de enkelte sektorene eller virksomhetene har og som de konkrete anvendelsene vil ha når det gjelder elektronisk identifisering signering og kryptering. Videre vil valget avhenge av hva slags modell for leveranse av sertifikater til enkeltpersoner som blir lagt til grunn og hva markedet har å tilby av løsninger.

Ut fra behovet for et rimelig godt sikkerhetsnivå og ut fra de anbefalingene som utvalget gir når det gjelder typer sertifikater og profiler for offentlige personsertifikater er det naturlig å anbefale at sertifikater som enkeltpersoner skal benytte mot forvaltningens tjenester bør utstedes med minimum sikkerhetsnivå 2. Dette vil i praksis bety kvalifiserte sertifikater men uten krav til beskyttelse av nøkler i et smartkort. Når markedsforhold er lagt til rette for det bør sertifikater på nivå 3 anbefales.

I en startfase når bruk av digitale signaturer og PKI skal innføres er det likevel viktig å påpeke at virksomheter som skal ta i bruk slike løsninger ikke bør stille for strenge krav der sikkerhetsbehovet ikke tilsier det. For enkelte anvendelser vil sertifikater på nivå 1 fungere utmerket.

Sett fra enkeltpersoners perspektiv må man likevel tenke på spørsmålet om hvor mange sertifikater og hvilke sikkerhetsnivåer en privatperson skal kunne håndtere. Best mulig samordning av sikkerhetskravene mellom sektorene og virksomhetene vil kunne gi bedre og enklere løsninger for brukere av offentlige tjenester. Det er lett å tenke seg at en bruker velger feil sertifikat for en anvendelse og at sikkerheten ved dette sertifikatet ikke er tilstrekkelig for denne anvendelsen. Bruk av sertifikat med «høyest» sikkerhetsnivå vil avverge slike problemer fordi et slikt sertifikat vil dekke hele spekteret av mulige anvendelser fra de helt enkle til de som krever høy sikkerhet.

9.3.2 Modeller for leveranse av sertifikater til enkeltpersoner

Det kan finnes ulike modeller for å forsyne enkeltpersoner med sertifikater/digitale signaturer:

a) Publikum kjøper sertifikater fritt i markedet og må selv finne ut hvilke sertifikater de kan bruke mot offentlig forvaltning. Dette er en modell som gir få fordeler for enkeltpersoner som får en stor belastning med å finne ut hva de må kjøpe og hva sertifikatene kan brukes til. Modellen påfører forvaltningen merarbeid fordi den blir nødt til å yte veiledning til enkeltpersoner i stor skala samtidig som hver offentlig virksomhet som tilbyr elektroniske tjenester vil måtte lage tilpasninger av disse mot alle tilbud på sertifikattjenester i markedet som enkeltpersoner kan tenkes å benytte.

b) Hver sektor eller offentlig virksomhet utsteder sertifikater som skal brukes mot deres tjenester til enkeltpersoner. De etatene som har egne sertifikatutstedelsestjenester kan tenkes å benytte disse for å utstede offentlige personsertifikater i tillegg til sertifikater til sine egne ansatte. Andre etater vil benytte en underleverandør. Her er det flere

muligheter – enten at underleverandøren leverer hele den elektroniske tjenesten med sertifikatbruk integrert eller at underleverandøren leverer en sertifikattjeneste som etaten selv integrerer. I det siste tilfellet kan etaten enten selv påta seg sertifikatutstederansvaret eller underleverandøren gjør det. I denne modellen kan enten etaten eller underleverandøren (om en slik benyttes) forestå registreringstjenesten for enkeltpersoner.

c) Offentlige virksomheter utleverer sertifikater til sine kunder. Etatene kjøper sertifikatene via en sentral rammeavtale f.eks. under Forvaltningsnettsamarbeidet. Sertifikatene vil bli utstedt av en leverandør i tilknytning til avtalen som etatene kan bestille. Denne varianten fordrer at etatene selv etablerer løsninger for registrering av enkeltpersoner og utlevering av sertifikater.

d) Det etableres en sentral offentlig tjeneste (f.eks. under sentralkontoret for folkeregistrering i Skattedirektoratet) som utsteder offentlige personsertifikater. Dette vil i praksis tilsvare etablering av en ordning med elektroniske ID-kort selv om man kan tenke seg at en slik sentral tjeneste også kan utstede offentlige personsertifikater som ikke forutsetter beskyttelse av private nøkler i et smartkort (nivå 2-sertifikater). Mange av argumentene for og imot som for en tilsvarende løsning for ansatte i staten gjør seg her gjeldende.

e) Forvaltningen inngår sentrale samarbeidsavtaler med aktører i markedet som allerede har etablert sertifikattjenester med enkeltpersoner som målgruppe. Slike avtaler vil innebære at markedsaktører (leverandører av sertifikattjenester) utsteder offentlige personsertifikater på minimum nivå 2 og utleverer dem til enkeltpersoner gjennom sitt nettverk av registreringsenheter. Sertifikatene skal kunne brukes mot alle offentlige elektroniske tjenester. For offentlige virksomheter vil det kunne være en forenkling bare å måtte tilpasse sine elektroniske tjenester mot én type sertifikater selv om de leveres av flere leverandører. Videre slipper forvaltningen å etablere egne registreringsordninger for enkeltpersoner.

f) Sentrale samarbeidsavtaler inngås med markedsaktører som utsteder egne sertifikater til enkeltpersoner i forbindelse med elektroniske tjenester som de tilbyr selv f.eks. bank- eller posttjenester. Avtalene vil gjelde bruken av slike sertifikater mot offentlige tjenester. Avtalen vil i praksis innebære at den konkrete markedsaktøren vil bli offentlig godkjent leverandør av sertifikattjenester som enkeltpersoner kan benytte mot forvaltningen. En avtale behøves ikke for å gi godkjenning men kan likevel trengs for å regulere ev. deling av utgifter mellom det offentlige og leverandøren dersom sertifikater skal kunne brukes uten ekstra kostnader for enkeltpersoner.

Sannsynligvis vil offentlig sektor i Norge uansett bli nødt til å godta elementer av den første modellen i hvert fall så lenge det leveres kvalifiserte sertifikater og kvalifiserte signaturer. Det er likevel mulig at gjennom forskrifter hjemlet i lov om elektronisk signatur § 5 og/eller eventuelle nye forskrifter til forvaltningsloven kan forvaltningen stille tilleggskrav som i praksis ikke vil tillate at et «hvilket som helst» kvalifisert sertifikat vil godtas til bruk mot forvaltningen. Dette kan være krav på teknisk/administrativt nivå som ikke nødvendigvis står i motstrid til eller går utover kravene i lov om elektronisk signatur men som i praksis kan begrense enkeltpersoners valgfrihet med hensyn til kjøp av (kvalifiserte) sertifikater.

Modellen der hver forvaltningsenhet utsteder egne sertifikater til brukerne krever en utstrakt kryssertifisering mellom forvaltningsenhetene for ikke å komme opp i en situasjon med stadig behov for registrering av sertifikateieren og utstedelse av nye dedikerte sertifikater. Det må sannsynligvis tillates at en bruker kan få utstedt nytt sertifikat ved å presentere et sertifikat som er utstedt av en annen forvaltningsenhet.

Anbefaling av modell er vanskelig bl.a. på grunn av mangel på praksis på området (utenom enkelte banker). Det første tilfellet av bruk av sertifikater i forbindelse med en offentlig elektronisk tjeneste vil være Skattedirektoratets planlagte levering av selvangivelser på Internett i 2001 der det legges opp til å kunne bruke Postens EID for sterk autentisering. Her vil leveransen av sertifikater være integrert i den elektroniske tjenesten som skal benyttes for levering av selvangivelsen.

Ut fra hensynet til brukeren og behovet for samordning av autentiseringsløsninger for elektroniske tjenester fra forvaltningen (for å unngå store kostnader forbundet med tilrettelegging for ulike typer sertifikater i hver sektor/virksomhet) kan det være mest hensiktsmessig å konsentrere seg om de modellene som legger opp til en type offentlig personsertifikat som kan brukes mot flere ulike offentlige tjenester. Dette behovet ble sterkt poengtert av deltakere på et seminar om elektroniske signaturer som Statens dataforum arrangerte i november 2000. Et annet viktig element er hensynet til det norske markedet for sertifikattjenester som er i ferd med å etablere seg. Tunge offentlige løsninger som retter seg mot alle voksne personer i landet vil kunne ødelegge dette gryende markedet. Etablering av en mulig fellesordning for offentlige personsertifikater i offentlig regi bør derfor sees i sammenheng med behov for et elektronisk ID-kort. Se også kapittel 12.

Det tredje hensynet er behov for et visst garantert sikkerhetsnivå i de løsningene (sertifikatene) som enkeltpersoner vil bruke mot offentlige elektroniske tjenester. Dette behovet må igjen veies opp mot hva markedet kan/vil tilby på kort og lengre sikt og hvor enkelt det er for enkeltpersoner å ta løsningene i bruk. Krav om sertifikater på nivå 3 er på kort sikt svært vanskelige å imøtekomme mest av hensyn til manglende standardisering av kortlesere og deres integrasjon i standard PC-utrustning og pga. kostnader og andre belastninger som dette kan påføre enkeltpersoner.

9.3.3 Hvordan skal enkeltpersoner få sertifikater til bruk mot forvaltningen?

Etter å ha vurdert de ulike hensynene og den markedssituasjonen som eksisterer i Norge pr. i dag anbefaler utvalget at forvaltningen inngår avtaler med utvalgte markedsaktører om bruk av deres sertifikater for elektronisk samhandling med offentlig sektor. I praksis betyr det valg av modell e) og/eller f) i punkt 9.3.2. Slike avtaler bør forutsette at:

- Aktuelle sertifikatutstedere er villige til å tilpasse sine løsninger til kravene fra offentlig sektor (mht. sikkerhetsnivå sertifikatpolicy og sertifikatprofiler)
- De utstederne som det inngås avtale med skal kunne tilby en løsning for samtrafikk med de sertifikatutstederne som forvaltningen vil benytte for sine interne formål
- Tjenester fra de aktuelle utstedere er enkle å bruke for enkeltpersoner
- Prisen for bruk av tjenestene er akseptabel (det er mest sannsynlig tale om avgift pr. oppslag i sperrelister og sertifikatkataloger)
- Kostnader for bruk av sertifikater mot offentlige tjenester bør ikke belastes brukerne (det offentlige bør betale dem) i startfasen; dette må revurderes når løsningene er etablert hos enkeltpersoner og hos forvaltningen
- Det må utarbeides systemer hos sertifikatutstederen som gjør det mulig å avregne påløpte kostnader riktig (ved bruk av sertifikater) og å fakturere riktig offentlig virksomhet; for store offentlige etater eller for konkrete anvendelser der bruksvolumet kan estimeres nokså presist kan volumprising være aktuelt
- Det bør være inngått avtale med minst to sertifikatutstedere (av konkurransehensyn).

Konkrete markedsaktører kan f.eks. være bankene med BankID ErgoGroup (tidligere Posten SDS) med Postens EID og Telenor med mobil ZebSign. I forbindelse med avtaler med bankene kan det diskuteres om det offentlige skal inngå avtale med hver enkelt bank som utsteder BankID-sertifikater eller om det skal inngås avtaler med bankenes interesseorganisasjoner for å favne alle relevante bankinstitusjoner.

Et argument som taler mot rene «markedsmodeller» er at Norge representerer et forholdsvis lite marked når det gjelder digitale signaturer og PKI. Den totale størrelsen på markedet kan gjøre det vanskelig å styre leverandørene i den retning det offentlige ønsker. Enkelte store utenlandske underleverandører vil neppe gjøre store tilpasninger i sin maskin- og programvare for å tilfredsstille den norske forvaltningens særkrav. Samtidig er forvaltningen en såpass stor bruker i forhold til det norske markedet at man burde kunne påvirke aktørene tilstrekkelig for å ivareta offentlige interesser.

9.4 Samhandling med private virksomheter

Når det gjelder leveranse av sertifikater til private virksomheter som ønsker eller skal samhandle elektronisk med forvaltningen er situasjonen uklar pga. manglende praksis. Et eksempel vi kan se i dag er skatteetatens SLN-prosjekt. Der skjer innlevering av selvangivelser fra private virksomheter ved bruk av sertifikater med privatnøkler lagret på smartkort. Sertifikatene utstedes av underleverandøren til skatteetaten til revisjons- og regnskapsbyråer og til firmaer. Et annet eksempel vil være Patentstyrets TAKISAI-prosjekt der sertifikater til patentbyråer skal utstedes av en underleverandør til Patentstyret.

Næringslivet generelt (unntatt finansnæringen og delvis forsikringsbransjen) er kommet forholdsvis kort når det gjelder å ta i bruk sertifikater for egne interne formål. Norsk Hydro og Statoil er i en tidlig fase av etablering av intern PKI og man kan anta at mindre bedrifter har enda lenger fram. Norsk Hydros representanter har uttalt at de på nåværende tidspunkt ikke kan se at deres interne sertifikater vil kunne benyttes mot offentlig sektor.

Disse betraktningene tyder på at utstedelse av sertifikater til private virksomheter på kort sikt vil være en «bransjemodell» dvs. at relevante etater sørger for at sertifikatene utstedes til egen bransje (dvs. de private virksomhetene de vil samhandle med). Ved en slik modell vil det være viktig at etatene klarer å samordne sine tekniske og operasjonelle krav til sertifikater og deres bruk i den grad slik samordning er hensiktsmessig og mulig. Denne modellen er nok ikke å anbefale på lengre sikt fordi den i sin ytterste konsekvens kan føre til at private virksomheter blir pålagt av forvaltningen å få utstedt sertifikater (og også vil måtte installere tekniske løsninger) fra mange ulike leverandører hvert sertifikat til sitt formål. Spørsmålet må også sees i sammenheng med behovet for samordning av offentlige innrapporteringsordninger. På sikt kan man derfor tenke seg at private virksomheter benytter offentlige personsertifikater som deres ansatte har skaffet seg samt virksomhetssertifikater og ansattsertifikater (tilsvarende dem for offentlig sektor) som de kjøper i et åpent marked eller utsteder selv med egen underleverandør.

Utvalget vil ikke anbefale noen umiddelbare tiltak når det gjelder sertifikater til næringslivet. Man trenger å vinne flere erfaringer med pågående pilotprosjekter. Utvalget ser behov for at det føres en dialog med næringslivet og leverandørene om behov for samordning av PKI-løsninger mellom forvaltningen og næringslivet. En slik dialog kan f.eks. føres i et eget forum for erfaringsutveksling med deltakelse fra de tre partene.

Utvalget anbefaler at forvaltningen ved samordningsfunksjonen og i samarbeid med norske standardiseringsorganer tar initiativ til etablering av et Forum for digitale signaturer der felles standard løsninger for forvaltningen og næringslivet kan diskuteres med leverandører av sertifikattjenester.

9.5 Behov for stimuleringsmidler for å ta digital signatur i bruk i forvaltningen

Erfaringer fra noen prøveprosjekter med bruk av digitale signaturer og PKI i forvaltningen (f.eks. SESAM i helsevesenet eller SLN i skatteetaten) viser at denne teknologien ennå er forholdsvis umoden.

Det ble bl.a. avdekket problemer med integrasjon av systemer for digitale signaturer med systemer for ulike anvendelser i forvaltningen. På grunn av bl.a. dette er flere forsøksprosjekter med digitale signaturer blitt utsatt eller ikke satt i gang i det hele tatt.

Man må regne med at innføring av digitale signaturer og PKI i forvaltningen vil ta tid. Det er derfor viktig å komme i gang med utprøving pilotering og utvikling av standarder og felles grensesnitt.

Leverandørforumet etablert under Programmet for elektronisk saksbehandling i Statskonsult drøftet forslaget til felles spesifikasjoner for et kommunikasjonsgrensesnitt mellom programmer for signering/kryptering og systemer for elektronisk arkivering og saksbehandling. Dersom man kan enes om

felles utvikling og implementering av et grensesnitt vil flere leverandører kunne begrense sine utviklingskostnader samtidig med at viktige brukerkrav blir realisert.

Bred innføring av digitale signaturer i forvaltningen vil kreve tilpasninger til mange forskjellige anvendelsessystemer. Bare i helsesektoren finnes det tre leverandører av ulike pasientjournalsystemer til sykehus og to leverandører av slike systemer til primærhelsetjenesten. I tillegg finnes det en rekke fagsystemer hvor integrasjon kan være aktuelt.

Forvaltningen mangler erfaringer med innføring av digitale signaturer og PKI i stor skala. Slike erfaringer er nødvendige for å kunne utvikle fornuftige fellespolicyer rutiner og standarder.

Brukererfaringer med denne teknologien er også en viktig faktor ved framtidig innføring av masseløsninger for digitale signaturer blant publikum og i næringslivet. Skatteetaten er i ferd med å starte opp slike utprøvinger i stor skala. Man trenger imidlertid flere prosjekter i flere sektorer.

Utvalget mener derfor at det er behov for å avsette stimuleringsmidler for offentlige virksomheter som har planer om eller er i ferd å komme i gang med pilotprosjekter med bruk av digitale signaturer og PKI. Midlene kan tenkes disponert av den felles samordningsfunksjonen (jf. punkt 9.6) og tildelt etter gitte kriterier til prosjekter der digitale signaturer blir tatt i bruk for å understøtte tilbudet av elektroniske tjenester til forvaltningens brukere eller i forvaltningens interne samhandling.

Utvalget mener at ett av flere mulige kriterier for tildeling av midlene bør kunne være hvorvidt løsningene som skal utprøves følger felles anbefalte standarder og/eller benytter felles etablerte ordninger for forvaltningen f.eks. felles rammeavtaler.

Utvalget mener at det for budsjettåret 2002 bør kunne avsettes 9 mill. kr til en slik stimuleringsordning.

9.6 Behovet for en samordningsfunksjon for bruk av digitale signaturer og PKI i forvaltningen

Etablering av en PKI i forvaltningen og for forvaltningens brukere krever at det tas stilling til mange ulike spørsmål av teknisk organisatorisk juridisk og til dels politisk art. Det er viktig at infrastrukturen kan brukes mellom og mot de ulike forvaltningsenhetene. Det er også viktig at infrastrukturen fungerer på en mest mulig enhetlig måte overfor forvaltningens brukere. Samordning blir derfor et viktig virkemiddel. Slike spørsmål kan ikke behandles fullt ut gjennom rene anskaffelsesprosesser eller enkeltvirksomheters IT-strategier. Bredden i utvalgets mandat indikerer i seg selv kompleksiteten av problemstillinger knyttet til hensiktsmessig bruk av slik infrastruktur. Utvalget ser derfor et behov for en permanent samordningsfunksjon i forvaltningen som kan ivareta strategiske spørsmål ved utvikling implementering og bruk av PKI for sikker kommunikasjon innad i offentlig sektor og med dens brukere.

9.6.1 Innholdet i en samordningsfunksjon for digitale signaturer og PKI

En slik samordningsfunksjon bør dekke både statlig og kommunal forvaltning fordi en infrastruktur av denne art vil være felles for begge. Tilrettelegging av funksjonen bør ta hensyn til dette.

En samordningsfunksjon kan tenkes å omfatte bl.a. følgende oppgaver:

a) Utvikle i samarbeid med sektorer og ulike forvaltningsnivåer detaljerte krav til PKI-løsninger for offentlig sektor herunder utvikle og forvalte de offentlige sertifikatpolicyene basert på PKI-utvalgets anbefalinger

b) Være premissgiver og samarbeide med f.eks. Forvaltningsnettsamarbeidets innkjøpsordning i Statskjøp mht. gjennomføring av anbudsprosesser og inngåelse av relevante rammeavtaler

c) Inngå felles samarbeidsavtaler på vegne av forvaltningen

d) Utvikle et nødvendig standard avtaleverk for bruk av digitale signaturer og PKI i forvaltningen

e) Vedlikeholde felles krav som offentlig sektor ønsker å stille til eksterne leverandører av sertifikater mht. bruk mot offentlig sektor og foreta vurderinger og prekvalifiseringer av slike leverandører

f) Føre oversikter over godkjente leverandører og krav som stilles til dem

g) Koordinere aktiviteter innenfor anvendelse av digitale signaturer og PKI i forvaltningen herunder håndtering av samtrafikkspørsmålet

h) Utrede og håndtere problematikken knyttet til sertifikater fra utlandet

i) Spre informasjon og holde kontakt med andre aktører i samfunnet (f.eks. gjennom et Forum for digitale signaturer) når det gjelder digitale signaturer og PKI.

Kommentarer til de enkelte oppgavene:

a) Utvikling av felles krav innebærer at det i regi av samordningsfunksjonen foregår en prosess med utarbeidelse av relevante dokumenter. Dokumentene bør så sendes på høring i forvaltningen før felleskravene fastsettes endelig. Det kan i denne sammenheng være hensiktsmessig å basere seg på prinsipper for utvikling av forvaltningsstandarder som er nedfelt i AAD-heftet fra 1995.

b) Grunnlaget for anbudsmaterialet for nye rammeavtaler bør ha en grundig forankring i forvaltningens felleskrav på området. Slikt grunnlag kan ikke utarbeides av konsulentmiljøer som ellers er gode samarbeidspartnere når det gjelder standardiserte IT-produkter og -tjenester som PC-er kontorprogramvare osv. Det er derfor naturlig at samordningsfunksjonen med forankring i prosesser beskrevet ovenfor er den som leverer et slikt anbudsgrunnlag.

c) Samordningsfunksjonen vil kunne representere forvaltningen (staten og kommunene) i forhandlinger med markedsaktører som tilbyr sertifikater til enkeltpersoner (jf. valg av modell i punkt 9.3.3). Det er åpenbart at gunstigere vilkår kan oppnås hos slike markedsaktører dersom forvaltningen kan opptre samlet og inngå fellesavtaler framfor at hver sektor eller etat fører forhandlinger selv og inngår avtaler på egen hånd. Videre er sjansene større for at markedsaktørene lettere vil kunne godta forvaltningens krav til tjenester (policy sikkerhetsnivå) dersom forvaltningen bruker sin tyngde som storbruker.

d) Bruk av PKI medfører til dels komplekse ansvarsforhold mellom leverandører og brukere av sertifikattjenester. Det er krevende og vanskelig å utvikle godt avtaleverk som sikrer forvaltningens interesser. Det er derfor nærliggende å prøve å få fram standardavtaler på området som forvaltningen kan få tilbud om å bruke bl.a. for ikke å bli henvist til leverandørenes juridiske løsninger.

e) På lengre sikt når markedet for sertifikattjenester er godt utviklet i Norge kan samordningsfunksjonen istedenfor å inngå felles samarbeidsavtaler med aktører i markedet heller utøve rollen som den som prekvalifiserer (dvs. evaluerer og «godkjenner») leverandører av sertifikattjenester i forhold til felleskrav som forvaltningen vil stille (jf. punkt a). Slik prekvalifisering vil være et tilbud til offentlige virksomheter som blir møtt med krav om å kunne bruke ulike typer sertifikater i markedet.

f) Forutsetningen for at slik prekvalifisering skal kunne fungere er at både kravene evalueringsmetodene og resultatene er bredt tilgjengelige for alle involverte parter.

g) Samordningsfunksjonen bør kunne holde seg orientert om relevante kompetansemiljøer prosjekter og andre aktiviteter når det gjelder digitale signaturer og PKI bl.a. for å kunne legge til rette for erfaringsutveksling knytting av kontakter kompetanseutvikling m.m. I samarbeid med Forum for digitale signaturer samt Post- og teletilsynet bør man også ta initiativ til og følge opp arbeidet med samtrafikkløsninger for sertifikattjenester.

h) Spørsmålet om håndtering av sertifikater fra utlandet er et viktig og komplekst problemområde som må utredes ytterligere både i forhold til forvaltningens behov for sertifikatbruk og behovet for samtrafikk. Et nært samarbeid med Forum for digitale signaturer bør være naturlig. Kontakt med relevante internasjonale samarbeidspartnere og -miljøer vil være viktig.

i) Mange utredninger om digitale signaturer har pekt på behovet for økt kompetanse og kunnskap om området både i forvaltningen og ellers i samfunnet. Samordningsfunksjonen bør derfor spille en viktig rolle. Dette kan innebære kontakt med samarbeidspartnere innen forskning og utvikling samt kontakt med andre kompetente miljøer i forvaltningen og utenfor. Det vil også være naturlig at samordningsfunksjonen har tett kontakt og godt samarbeid med Post- og teletilsynet og Datatilsynet som blir tilsyn for leverandører av sertifikater i medhold av lov om elektronisk signatur.

Utvalget vil presisere at etablering av en slik samordningsfunksjon ikke skal gripe inn i offentlige virksomheters rett og plikt til selv å vurdere de sikkerhetsløsninger som man vil ha behov for i elektronisk samhandling i henhold til eget regelverk. Fellesordninger (som f.eks. rammeavtaler) for digitale signaturer som samordningsfunksjonen vil kunne etablere for forvaltningen må betraktes som et tilbud som bør vurderes på linje med andre tilbud i markedet. Det kan likevel vurderes om offentlige virksomheter som skal gå i gang med digitale signaturer og PKI skal pålegges å vurdere fellestilbudene først før man ev. velger andre løsninger.

9.6.2 Organisering og plassering av samordningsfunksjonen

Utvalget foreslår at samordningsfunksjonen organiseres som et fast samordningsutvalg bestående av representanter fra ulike sektorer og nivåer av forvaltningen (statlig og kommunal) og et sekretariat med fast bemanning.

Størrelse sammensetning og mandat for samordningsutvalget bør vurderes konkret i forbindelse med etableringen. Utvalget mener likevel at alle store/tidlige brukere av digital signatur bør kunne inkluderes at forvaltningsnivåer (særlig kommunene) bør ha tilstrekkelig representasjon og at representanter fra de organer som arbeider med IT-samordning nasjonalt og i forvaltningen bør delta. Samordningsutvalget bør ledes av et av samordningsdepartementene på IT-området enten AAD eller NHD.

I etableringsfasen bør det avklares hvilke fullmakter sekretariatet skal ha i forhold til samordningsutvalget og hvordan forholdet mellom dem skal fungere i praksis.

Utvalget estimerer ressursbehovet for denne funksjonen i en startfase som 1 årsverk til sekretariatsoppgaver og ca. 1–2 månedsverk pr. år fra hvert medlem i utvalget (noe større innsats ca. 4 månedsverk vil måtte forventes fra den som leder et slikt samordningsutvalg). Innsatsen fra medlemmene forutsettes dekket av de respektive forvaltningsorganene ut fra organenes egeninteresse i arbeidet.

Sekretariatet må få et driftsbudsjett som gjør det mulig eventuelt å engasjere noe ekstern bistand. Størrelsen på budsjettet er vanskelig å estimere uten å vite hva slags oppgaver sekretariatet faktisk vil

ivareta men ut fra tidligere erfaringer med Forvaltningsnettsamarbeidet kan det stipuleres til ca. 6 mill. kroner det første driftsåret.

Midlene vil kunne benyttes til utredninger (av f.eks. håndtering av sertifikater fra utlandet) utarbeidelse av grunnlaget for rammeavtaler utvikling av felles sikkerhetskrav og policy evaluering av løsninger i markedet og finansiering av deltakelse i felles erfaringsforum med næringslivet og leverandørene samt ev. bidrag til etableringen av en felles samtrafikktjeneste (jf. punkt 10.10.7).

Ved etablering av sekretariatet bør man ta i betraktning at den virksomheten som får denne funksjonen bør ha tilstrekkelig nærhet til eller kunnskap om den praktiske implementeringen av PKI som pågår i forvaltningen.

Utvalget har drøftet ulike modeller for plassering av sekretariatet:

- Forankring i AAD NHD eller en underliggende virksomhet til disse
- Hos en «største bruker» av sertifikattjenester
- I et annet relevant fagmiljø/eksisterende myndighet f.eks. Post- og teletilsynet eller Datatilsynet.

Plassering av samordningsfunksjonen bør kunne gjøres ut fra visse kriterier f.eks.:

- Nødvendig kompetanse
- Nærhet til sannsynlige brukere
- Evne til å kunne forene ulike interesser i forvaltningen og få fram felles krav
- Ingen fare for rollekonflikter eller habilitetsproblemer overfor forvaltningen og markedet
- Hvor enkelt det er å etablere sekretariatsfunksjonen og komme i gang.

Andre kriterier bør også vurderes.

Utvalget ser det som lite aktuelt å etablere et sekretariat med operative funksjoner internt i et departement. Det strider mot moderne prinsipper for organisering av departementsvirksomhet. En mulig plassering kunne i stedet være i et underliggende organ til AAD som Statskonsult eller Statens forvaltningstjeneste. Begge disse organene har samordningsoppgaver. Plassering under et departementet med samordningsansvar på området og ev. ansvar for å lede utvalget ville gi en «ryddig» styringsstruktur.

Statskonsult ønsker i sin rolle som kompetanseorgan innen forvaltningsutvikling ikke å miste sin uavhengighet og habilitet som evaluatør av statsforvaltningens IT-bruk. Operative driftspregede funksjoner er det derfor ikke ønskelig at Statskonsult skal ivareta ifølge etaten selv. Kommunesektoren er heller ikke noe naturlig nedslagsfelt for Statskonsult. Statskonsult er likevel en viktig aktør som bør kunne delta i samordningsutvalget bl.a. i kraft av sin oppgave som ivaretaker (på vegne av AAD) av rollen som IT-standardiseringssekretariat for forvaltningen.

Statens forvaltningstjeneste (Ft) gjennomfører nå en strategiprosess med tanke på omorganisering og fokusering av virksomheten. Et bærende prinsipp i den nye strategien er at Ft skal fokusere på departementsfellesskapet som målgruppe for sine tjenester. Ressurser skal konsentreres om oppgaver knyttet til departementenes behov for fellestjenester også på IT-området. Dette kan gjøre det vanskelig å plassere et sekretariat som skal utøve samordning for hele forvaltningen inklusive kommunene.

Forvaltningsnettsamarbeidets innkjøpsordning plassert i Ft's avdeling Statskjøp disponerer svært begrensede ressurser samtidig som disse ressursene har kompetanse med hovedtyngde på innkjøpssiden. Øvrige strukturer i Forvaltningsnettsamarbeidet (utenom styringsgruppen som i praksis administrerer innkjøpsordningen) er såpass uavklarte at det ikke er naturlig å plassere en samordningsfunksjon der slik situasjonen er nå. Det pågår også diskusjoner om framtidig organisering av felles innkjøpsfunksjoner for staten og ev. kommunene som kan innvirke på fremtidig organisering av Statskjøp.

I den andre gruppen er Skattedirektoratet og Rikstrygdeverket kandidater som peker seg ut på grunn av sin erfaring med bruk av digital signatur. Begge har noen års erfaring med bruk av digital signatur og PKI

særlig fra elektronisk samhandling med publikum og andre brukere av forvaltningen. Begge etatene besitter kompetanse på området. I tillegg kan både Patentstyret og Brønnøysundregistrene være aktuelle kandidater på noe sikt.

Etablert forvaltningspraksis taler kanskje imot en løsning der en etat i en bestemt sektor tillegges samordningsfunksjoner der ulike behov og hensyn skal ivaretas på vegne av flere virksomheter og forvaltningsnivåer. Samtidig finnes det positive eksempler på at slike virksomheter tillegges fellesfunksjoner for forvaltningen (og resten av samfunnet) f.eks. det sentrale folkeregisteret og arbeidsgiver-/arbeidstaker-registeret.

Et annet moment som taler mot plassering av et sekretariat for en samordningsfunksjon i en sektor kan være behovet for klare styrings- og ansvarslinjer for sekretariatet. Dette behovet kan være vanskelig å forene med forankring av samordningsutvalget i et IT-koordineringsdepartement.

Videre kan plassering av et sekretariat for samordningsfunksjonen i en stor statlig etat føre til bekymring om hvorvidt kommunesektorens interesser vil kunne ivaretas på en tilfredsstillende måte.

Den svenske regjeringen har i sin beslutning av 21.12.2000 lagt forvaltningens samordningssfunksjon for PKI til Riksskatteverket. Begrunnelsen for dette lød:

... inom Riksskatteverket sedan länge finns en omfattande kompetens när det gäller registerhållning för både individer och företag. Genom folkbokföringen är verket huvudansvarigt för de grundläggande individuppgifter som används i samhället. Verket tillhör också de myndigheter som har mest näraliggande planer på omfattande interaktion med medborgare och företag över Internet. Inom verket finns bl.a. av det skälet också den typ av IT-kompetens som krävs. De i utredningen deltagende myndigheterna har också funnit denna lösning lämplig inte minst därför att det för närvarande synes vara den som snabbast kan genomföras.

Plassering av en samordningsfunksjon hos en tilsynsmyndighet som Post- og teletilsynet eller Datatilsynet vil føre til habilitets- og rollekonflikter. Å ivareta tilsyn av aktører i markedet samtidig som man representerer interessene til noen av de største brukerne av digital signatur (forvaltningen) vil innebære en uheldig blanding av roller. I tillegg er en operativ samordningsrolle ikke naturlig for slike virksomheter.

Utvalget mener at det haster med etablering av samordningsfunksjonen og anbefaler derfor at sekretariatet og utvalget etableres som et prosjekt i startfasen. Midler til dette bør kunne omprioriteres innenfor rammen av budsjettet for inneværende år (2001). Det bør drøftes av de relevante departementer hvordan en slik omprioritering konkret kan skje. De relevante departementene er Finansdepartementet Nærings- og handelsdepartementet Arbeids- og administrasjonsdepartementet Sosial- og helsedepartementet og Forsvarsdepartementet. I tillegg må kommunal sektor delta i drøftingene.

En av årsakene til at funksjonen bør komme på plass umiddelbart er hensynet til brukerne av rammeavtalen om digital signatur under Forvaltningsnettsamarbeidet som utløper 1.6.2001. Inngåelse av en ny avtale tar tid og man bør derfor søke å unngå at «gapet» mellom avtalene blir for stort. En annen grunn er behovet for dialog med markedsaktørene med hensyn til å etablere felles standarder på PKI-området.

Organisering og plassering av samordningsfunksjonene bør som nevnt drøftes av berørte departementer berørte underliggende etater (som nevnes her ev. andre i tillegg) og representanter fra kommunesektoren før det endelige valget tas. Utvalget mener at en slik drøftingsprosess bør kunne komme i gang straks.

Utvalget mener at den ordningen man til slutt lander på bør evalueres etter to år med tanke på eventuell alternativ organisering.

9.7 Oppsummering av anbefalinger

Utvalget anbefaler at forvaltningen får et tilbud om sertifikater til sine ansatte gjennom etablering av en ny utvidet rammeavtale om digitale signaturer og sertifikattjenester under Forvaltningsnettsamarbeidets innkjøpsordning. Rammeavtalen skal også tilby produkter og/eller tjenester som gjør det mulig for en offentlig virksomhet selv å kunne utstede sertifikater til sine ansatte. Sertifikater for offentlig forvaltning bør i hovedsak være nivå 3-sertifikater men nivå 2-sertifikater kan ikke utelukkes der behovet tilsier det.

Utvalget anbefaler at det for sertifikater til enkeltpersoner inngås samarbeidsavtaler med minst to aktører i markedet som utsteder eller vil utstede sertifikater til enkeltpersoner i forbindelse med egen bruk av digitale signaturer og PKI. Kostnader ved bruk av slike sertifikater mot offentlig sektor bør ikke belastes enkeltpersoner i startfasen. Sertifikatene bør være minst nivå 2-sertifikater med overgang til nivå 3 når tilsvarende løsninger foreligger i markedet og er bredt tilgjengelige.

Utvalget anser at det bør vinnes flere praktiske erfaringer med bruk av sertifikater i forbindelse med elektronisk samhandling mellom næringslivet og forvaltningen før man foreslår fellestiltak fra forvaltningens side. Utvalget anbefaler at det etableres et eget Forum for digitale signaturer med representanter fra forvaltningen næringslivet og leverandørene for å drøfte felles standarder for digitale signaturer og PKI.

Utvalget anbefaler at det etableres en permanent samordningsfunksjon for bruk av digitale signaturer i og mot forvaltningen. Funksjonen organiseres som et permanent utvalg ledet av et IT-samordningsdepartement enten AAD eller NHD med et sekretariat med eget driftsbudsjett. Organisering og plassering av samordningsfunksjonen bør drøftes snarest av relevante departementer etater og representanter fra kommunesektoren. Utvalget anbefaler at samordningsfunksjonen bør komme på plass allerede i 2001. Denne løsningen bør evalueres etter to år med tanke på en ev. alternativ organisering og plassering.

10 Forvaltningens krav til samtrafikk mellom leverandører av sertifikattjenester

Det eksisterer allerede en rekke sertifikattjenester både i Norge og i et internasjonalt marked. Tjenestene er til dels forskjellige både med hensyn til kvalitetsnivå og bruksaspekter (nedfelt i sertifikatpolicyer) og når det gjelder innhold og format av selve sertifikatene. Mangel på samtrafikk (evnen som et produkt eller et system har til å samarbeide med andre produkter eller systemer) er en av hovedhindringene for å ta i bruk PKI. Utfordringene for forvaltningen er:

- Sørge for avtaleverk og tekniske løsninger som sikrer samtrafikk med henblikk på sertifikattjenester som forvaltningen selv er kunde av eller selv driver
- Stille krav til og bestemme hvilke typer sertifikater og fra hvilke utstedere som skal kunne aksepteres fra privat sektor (enkeltpersoner og næringsliv) ved korrespondanse med forvaltningen
- Vurdere tiltak for å oppnå samtrafikk generelt og ikke bare med hensyn til forvaltningens egne kommunikasjonsbehov
- Ta høyde for internasjonal samtrafikk
- Sørge for tekniske løsninger som kan håndtere forskjellige sertifikatformater og sertifikatutstedere.

10.1 Hva er samtrafikk?

10.1.1 Hva skal samvirke og hvorfor?

Samtrafikk har elementer av både teknologi og tillit. Den teknologiske siden kan deles i tre aspekter:

- Man må kunne behandle sertifikater fra i prinsippet vilkårlige utstedere på en meningsfull måte dvs. gjennomgå sertifikatinnholdet og sjekke utsteders signatur m.m.
- Man må ha sikker kunnskap om utsteders offentlige nøkkel tilsvarende den private som ble brukt til å signere sertifikatet med. Dette er ikke trivielt når utstederen er en annen enn den man selv har fått sertifikater fra.
- Samspill mellom produkter fra ulike leverandører må være mulig. Det er et faktum at to løsninger begge kan være i henhold til en standard men likevel ikke virke sammen.

I tillegg må sertifikatbrukeren kunne bestemme hvor stor tillit det er mulig å ha til sertifikatet det vil si om det er brukbart for det gitte formålet eller ikke.

Samtrafikk er et område som har betydning for alle aktører og der løsninger må finnes ved en kombinasjon og vektlegging langs forskjellige akser:

- Gjennom samarbeid mellom tjenesteleverandører kan man oppnå løsninger som i hvert fall et stykke på vei skjuler samtrafikkproblemer for brukerne.
- I den grad samtrafikk mellom tjenesteleverandører ikke er på plass må man tilrettelegge for at brukerne skal kunne løse samtrafikkproblemene selv.
- Dette kan involvere egne tjenestetilbydere som tar seg av (deler av) behandlingen av sertifikater på vegne av brukerne.

- Tiltak fra myndigheter – nasjonalt og internasjonalt – kan være nødvendig for å muliggjøre samtrafikk enten som regulerende tiltak eller i form av tilrettelegging og økonomiske og andre incentiver. Standardiseringsarbeid er også et viktig bidrag.

10.1.2 Status for samtrafikk

Status i dag er at samtrafikkavtaler mellom sertifikatutstedere er lite utbredt men at man ser enkelte slike samarbeidsstrukturer. Eksempler i Norge er kryssertifiseringsavtalen for Forvaltningsnettsamarbeidet og arbeidet med et felles system BankID for sertifikattjenester for norske banker.

Internasjonal samtrafikk er lite utbredt men noen eksempler finnes. Postverkene i Norge Sverige Finland og Irland har samarbeidet om sine tjenester med tanke på kryssertifisering. Det danner grunnlag for arbeid i Den internasjonale postunionen med tanke på et mer eller mindre verdensomspennende system for sertifikattjenester. Innen banksektoren er IDENTRUS[24]et meget viktig initiativ.

Samtrafikk på leverandørnivå oppnås gjennom tillitsstrukturer (se punkt 10.2) og felles spesifikasjoner. Men i dag og i hvert fall en del år framover vil samtrafikk i hovedsak være overlatt til brukerne. Egne tjenester for samtrafikk finnes ikke i dag men er likevel også på relativt kort sikt et mulig alternativ.

Myndighetsrollen er i støpeskjeen gjennom utredningsarbeid som denne NOU-en og annet arbeid som oppsummert i kapittel 4.

Standarder for sertifikattjenester er i hovedsak på plass men standardene inneholder ofte alternativer og må presiseres ytterligere gjennom profiler. Spesielt gjelder dette selve sertifikatene. Disse er standardisert gjennom X.509 v3-spesifikasjonen [37] men sertifikater fra forskjellige utstedere bruker til dels vidt forskjellige profiler. Forskjeller i tekniske løsninger er relatert både til sertifikatutstedere og til leverandører av utstyr og programvare til utstedere og til brukere.

De juridiske aspektene ved samtrafikk er meget komplekse. Samtrafikk over landegrensene vil i tillegg kreve forståelse for og hensyn til særegenheter i andre lands lover og rettspraksis.

10.1.3 Behandling av sertifikater

Behandling av sertifikater består av:

Gjennomgang av sertifikatinnholdet[25]for å sjekke at det har korrekt format. Her skal det ikke være noen problemer med hensyn til samtrafikk dersom: 1) alle sertifikater som utstedes følger samme standard (X.509 v3) og 2) programvaren hos sertifikatbruker kan lese alle mulige elementer i et X.509 v3-sertifikat. Disse kravene bør være oppfylt av alle utstedere og all vanlig programvare. Men praktisk erfaring viser at det kan finnes forbehold spesielt knyttet til private utvidelser som X.509 v3 gir muligheter for og som

---

24

http://www.identrus.com

25

Dvs. sjekk av at sertifikatet har korrekt format i henhold til X.509 v3-standarden. Dette innebærer ikke noen vurdering av om *verdier* av felter attributter og utvidelser kan tolkes og er fornuftige bare at de kan leses.

brukes av enkelte spesifikasjoner. Siden X.509 v3 er en omfattende standard med mange valgmuligheter er det også en viss risiko for at produkter har feil mangler eller unøyaktigheter.

- Sjekk av utsteders signatur på sertifikatet. Dette betinger sikker tilgang på utsteders offentlige nøkkel.
- Sjekk av gyldighetsperiode for sertifikatet. Dette skal ikke medføre problemer med hensyn til samtrafikk så lenge tidsangivelser er angitt på en måte som kan tolkes av sertifikatbrukerens programvare og dette skal normalt være oppfylt. Det forutsettes også at aktørene har noenlunde korrekte klokker (det er ingen strenge krav til klokkesynkronisering).
- En del andre tester av sertifikatinnholdet bl.a. om bruken er i samsvar med det som er angitt i sertifikatet. Dette skal normalt håndteres riktig av alle implementasjoner. Merk at man også trenger støtte for de kryptoalgoritmene som brukes for sertifikatet både signeringsalgoritmen for utsteder og den algoritmen som offentlig nøkkel i sertifikatet tilhører.
- Sjekk av tilbaketrukket sertifikat – dette betinger tilgang på utsteders tilbaketrekkingsliste eller tilgang til andre tjenester for å sjekke sertifikatets status. En tilbaketrekkingsliste vil ha en veldefinert struktur som skal kunne behandles hos enhver sertifikatbruker. Dersom man er i stand til å sjekke utsteders signatur på et sertifikat er man også i stand til å sjekke dennes signatur på tilbaketrekkingslisten.
- Tolkning av innholdet i sertifikatet (felter attributter og utvidelser) med tanke på videre behandling av informasjonen.

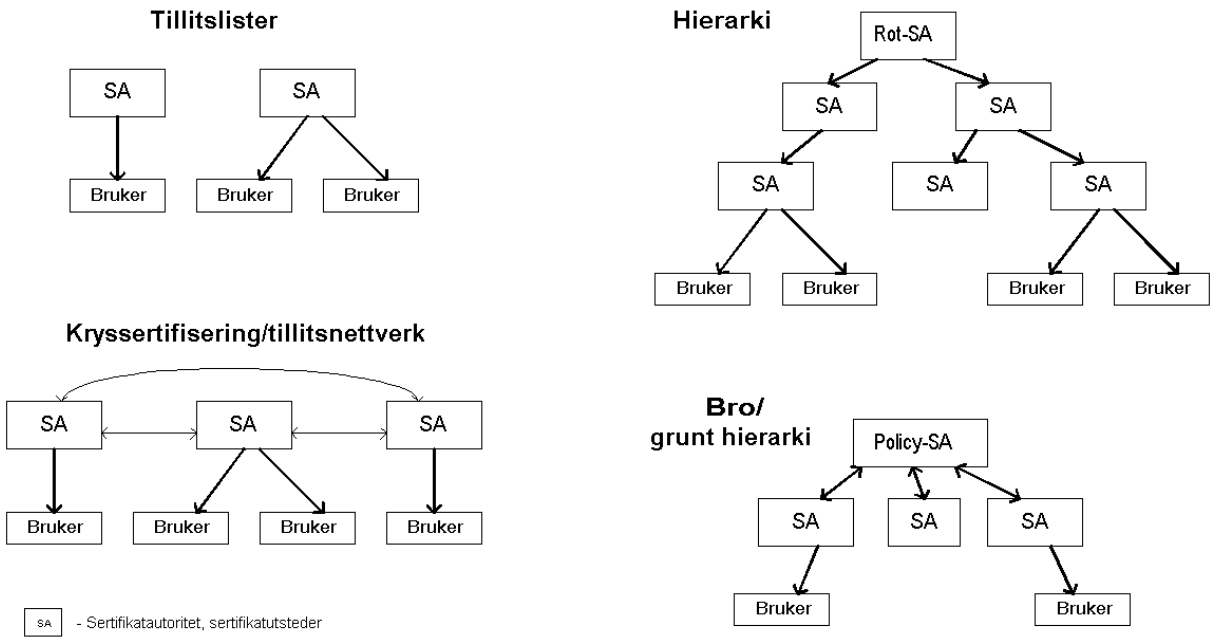
Dagens løsninger forutsetter at sertifikatbrukerens programvare er i stand til å ta seg av denne prosesseringen eventuelt med assistanse fra brukeren selv. Kompleksiteten i dette øker sterkt med antallet forskjellige sertifikatprofiler og utstedere som man må forholde seg til. Det må være et mål å unngå at brukerne blir eksponert for disse problemstillingene.

Spesielle krav er knyttet til tolkning av informasjonen i sertifikatene i de tilfellene der brukeren er en tjeneste dvs. at sertifikater må behandles helt automatisk og uten menneskelig medvirkning. Her må programvaren være i stand til å trekke ut den nødvendige informasjonen fra (forskjellige) sertifikatformater og eventuelt avlede annen informasjon fra dette. Enten må programvaren ta hånd om dette selv eller det må finnes egne tjenester som kan brukes.

10.2 Tillitsstrukturer og samtrafikk mellom utstedere

10.2.1 Tillitsstrukturer

Samtrafikk mellom sertifikatutstedere innebærer at tillit til en sertifikatutsteder (i figur 10.1 kalt SA) medfører at man også kan ha tillit til andre utstedere. Dette oppnås ved at utstederne inngår avtaler som regulerer forholdet dem imellom og formaliserer dette ved å danne en tillitsstruktur.



Figur 10.1 Tillitsstrukturer

Tillitsstrukturer kan kategoriseres slik:

- Tillitsliste. Det dreier seg om helt separate utstedere og sertifikatbrukere må vedlikeholde en egen liste over utstedere brukeren stoler på.
- Hierarki der utstedere har sertifikater utstedt av PKI-tjenester på høyere nivå opp til en felles rot. Hierarkier kan i prinsippet være «dype» men det vanlige i dag er to-nivå (grunne)-hierarkier med bare ett nivå under roten.
- Tillitsnettverk (web of trust) som realiseres ved kryssertifisering mellom PKI-tjenestene. Kryssertifisering gjøres ved at utstederne gjensidig utsteder sertifikater for hverandres offentlige nøkler (enveis kryssertifisering er mulig men svært uvanlig). Dette er vanlige X.509 v3-sertifikater men de skal være merket som kryssertifikater og kravet til innhold er noe forskjellig fra sertifikater for brukere eller sertifikater utstedt i et hierarki.
- Broer som realiseres ved kryssertifisering mellom utstederne og en felles broutsteder. Tillitsmessig er dette det samme som et grunt hierarki men implementasjonen er en annen.
- Hybride modeller med kryssertifisering kombinert med hierarkier. Dette kan være krysssertifisering mellom utstedere internt i ett hierarki mellom hierarkier på rot-nivå eller generelt mellom en utsteder i ett hierarki og en annen tjeneste. Dette er ikke vist i figuren.

Dagens situasjon er i stor grad basert på tillitslister dvs. at utstederne opererer helt separate tjenester uten noen form for gjensidig samarbeid eller godkjenning. Man ser allerede nå at dette skaper problemer fordi antallet utstedere særlig i internasjonal sammenheng begynner å bli stort.

Hierarkier og tillitsnettverk tillater at sertifikater utstedt av en eller annen tjeneste i denne strukturen kan gjenkjennes overalt ellers i strukturen (dvs. av sertifikatbrukere som har et tillitsforhold til en eller annen av tjenestene). Man kan konstruere en sertifikatkjede (også kalt tillitskjede) mellom vilkårlige brukere innen strukturen. Det er ikke nødvendigvis lett å finne riktig sertifikatkjede.

10.2.2 Konsistent kvalitetsnivå for tillitsstrukturer

I utgangspunktet betyr ikke tillitsstrukturer noe mer enn en forenkling når det gjelder å gjenkjenne sertifikater. Det betyr ikke at alle tjenestene er på samme kvalitetsnivå. Sertifikatbrukere må altså definere tillit til hver enkelt tjeneste separat akkurat som i tilfellet tillitslister.

Det er imidlertid vanlig å legge på ekstra betingelser som garanterer at tjenestene er på samme kvalitetsnivå. I et hierarki gjøres dette ved at roten setter betingelser som en utsteder må oppfylle før roten er villig til å utstede et sertifikat. Utstederen må gjøre betingelsene gjeldende for eventuelle underordnede utstedere dersom hierarkiet har mer enn to nivåer. Dette kan gjøres ved at roten setter en sertifikatpolicy som skal følges av alle tjenestene men det kan også gjøres ved en evaluering av de sertifikatpolicyene som tilbys opp mot et kvalitetsnivå. Dette er indikert for eksempelet «grunt hierarki» i figur 10.1 ved at roten har fått navnet «Policy-SA» (SertifikatAutoritet). Det er en betegnelse som av og til brukes og som henspiller på at roten bestemmer sertifikatpolicyer for hele strukturen.

For kryssertifisering bruker man begrepet «policy mapping» for å indikere at tjenestene er på samme kvalitetsnivå. Policy mapping angis i krysssertifikater ved at man lister opp de sertifikatpolicyene som er involvert. Også for kryssertifisering er det mulig å bruke samme sertifikatpolicy for alle utstedere slik det gjøres i Forvaltningsnettsamarbeidet.

10.2.3 Broer

En brostruktur (anvendt av føderale myndigheter i USA [26]) er tillitsmessig det samme som et grunt hierarki der broutstederen fungerer som rot. Broutstederen definerer et sett av rammepolicyer som angir definerte kvalitetsnivåer. De enkelte utstederne kryssertifiserer så mot broutstederen med «policy mapping» mot den rammepolicyen som tilsvarer utstederens sertifikatpolicy. Man vil da alltid kunne gå til broutstederen og få tak i dennes (kryss-)sertifikat for en gitt utsteder og man vil også gjennom dette kunne bestemme nivået på utstederens sertifikater gjennom kjennskap til den tilsvarende rammepolicyens nivå.

10.2.4 Dybde av hierarkier

Hierarkier med mange nivåer (dype) anbefales ikke. Det kan medføre lange sertifikatkjeder. Lange kjeder svekker tilliten siden det alltid er en liten mulighet for feil i et ledd i kjeden og behandling av sertifikatkjedene kan bli meget ressurskrevende siden det kan være mange sertifikater som skal behandles. På nasjonalt nivå (i Norge og i andre land) ser vi at trenden heller er to-nivå-hierarkier som f.eks. BankID. For internasjonal samtrafikk vil slike nasjonale to-nivå-hierarkier enten trenge ett nivå til over de nasjonale røttene eller man kan bruke kryssertifisering mellom nasjonale systemer.

10.2.5 Hvor mye bidrar tillitsstrukturer til samtrafikk?

Man vil aldri få en situasjon der en tillitsstruktur omfatter alle aktuelle utstedere. Det offentlige kan stille krav (som i Forvaltningsnettsamarbeidet) til strukturer mellom utstedere som det offentlige selv skal bruke. Men for totalbildet spesielt med et internasjonalt perspektiv vil ikke dette kunne dekke alt. Strukturering av tjenester i hierarkier eller ved kryssertifisering forenkler likevel bildet for samtrafikk sterkt.

Eksempler:

- Forvaltningsnettsamarbeidets rammeavtaler med kryssertifisering garanterer at sertifikatbrukere innen dette systemet bare trenger å forholde seg til sin egen utsteder
- Det er klart mye enklere å forholde seg til én felles BankID-løsning enn til forskjellige løsninger for forskjellige banker.

Man vil alltid stå igjen med en tillitsliste der man individuelt må bestemme tillit til enkelttjenester eller til hele tillitsstrukturer. Tillitslister forenkler situasjonen i den grad man kan gå fra lange til korte lister som stort sett angir tillit til et fåtall strukturer. Innen visse anvendelsesområder vil man bare trenge å forholde seg til et visst utvalg av alle mulige utstedere (f.eks. alle kommersielle i Norge) og strukturering av dette utvalget vil da kunne ha stor betydning.

10.2.6 Tiltrodde samtrafikktjenester

Som et supplement eller kanskje som et alternativ til tillitsstrukturer kan man tenke seg tiltrodde tjenester som behandler sertifikater fra «vilkårlige» utstedere på vegne av sertifikatbrukerne. En sertifikatbruker kan sende et mottatt sertifikat til en slik tjeneste og som minimum få som svar om sertifikatet er gyldig suspendert eller tilbaketrukket. Man kan tenke seg at tjenesten kan gi tilleggsinformasjon f.eks. hvilket kvalitetsnivå et sertifikat har (ut fra sertifikatpolicy) eller informasjon som er avledet av innholdet i sertifikatet f.eks. fødselsnummer. Slike tjenester kalles *samtrafikktjenester*.

Samtrafikktjenester kan tilbys:

- Som kommersielle tjenester i et åpent marked
- Internt i en virksomhet for å sentralisere (policy for) sertifikathåndtering
- I samarbeid mellom virksomheter f.eks. felles for flere forvaltningsorganer.

Samtrafikktjenester beskrives nærmere i punkt 10.10.7.

10.3 Sertifikatpolicy og kvalitetsnivåer

10.3.1 Tillit og kvalitet

Selv om de tekniske problemstillingene blir løst vil det ikke være noen garanti for at et sertifikat er godt nok for det formålet man skal bruke det til. Hva som er godt nok avgjøres av den sikkerhetspolicyen som gjelder for den aktuelle anvendelsen. Sertifikattjenester har varierende kvalitet når det gjelder prosedyrer for utstedelse og krav til sikkerhetsnivå for sertifikateierens omgivelser (f.eks. smartkort eller ikke). I tillegg kan det være gitt begrensninger på hvilke anvendelser sertifikatet er tillatt brukt for (f.eks. bare for banktjenester – tenkt eksempel) og utstederen kan i større eller mindre grad ha fraskrevet seg ansvaret for feilsituasjoner spesielt i forhold til andre anvendelser enn tiltenkt.

Tillit til et sertifikat – om det skal aksepteres eller ikke – vil bli bestemt av kombinasjonen av utsteder og sertifikatpolicy. Denne avgjørelsen kan tas fra gang til gang når man mottar et sertifikat eller regler for slike avgjørelser kan plasseres i sertifikatbrukernes systemer f.eks. ved at lister av godkjente utstedere og sertifikatpolicyer settes i nettlesere eller e-postsystemer. Det finnes lite støtte for å plassere denne typen godkjenningsinformasjon på organisasjonsnivå utover å sørge for at nettlesere og e-post hos alle sertifikatbrukere får en standardisert og godkjent konfigurasjon. Men man kan anta at støtte for slik organisasjonsmessig konfigurering vil komme relativt snart implementert i e-posttjenere web-tjenere brannmurer og andre komponenter på en virksomhets grensesnitt mot eksterne nettverk. En annen idé som ikke er realisert foreløpig er at brukerne kaller en samtrafikktjeneste (internt eller eksternt for organisasjonen) og får returnert et «ja» bare dersom både utsteder og sertifikatpolicy for det aktuelle sertifikatet er akseptable i henhold til virksomhetens sikkerhetspolicy.

Evaluering av sertifikatpolicyer i forhold til kvalitetskrav for et spesifikt formål er vanskelig. Dette bunner bl.a. i at sertifikatpolicyer er kompliserte tekniske og til dels juridiske dokumenter. Det kan i hvert fall ikke forventes at den enkelte sertifikatbruker kan gjøre de nødvendige vurderinger.

Internasjonalt er en evaluering enda mer komplisert siden sertifikatpolicyer kan være skrevet på et fremmed språk ha henvisninger til fremmede lands lover og regelverk og ellers være innholdsmessig og «kulturelt» fremmede.

10.3.2 Varemerker for sertifikater

En sertifikatpolicy definerer det kvalitetsnivået utstederen påberoper seg med hensyn til sertifikatene. En sertifikatbruker trenger tillit til at utstederen faktisk arbeider i henhold til sin sertifikatpolicy altså at utsteder ikke jukser. Tillit til utsteder knyttes bl.a. til utstederens gode navn og rykte. Det man ser er at utstedere prøver å bygge varemerker f.eks. «VeriSign»[26]«BankID»[27]«Postens EID»[28]eller «ZebSign»[29] Varemerker har flere formål men et av de viktigste er å oppnå tillit ikke bare hos egne kunder men også hos andre som må forholde seg til merket. Det er imidlertid et langt stykke igjen før varemerker for sertifikater er innarbeidet. Det virker kompliserende at et varemerke ikke behøver å være entydig. Sertifikatbrukere kan godt ha et forhold til VeriSign men vil kanskje ha vanskeligheter med å skjønne at denne tjenesten har flere nivåer og at de svakeste nivåene kanskje ikke burde godkjennes for sertifikatbrukerens spesifikke formål.

«Varemerke» kan eksemplifiseres ved en sertifikatbruker som ikke selv har noen BankID men som velger å stole på BankID-sertifikater fordi sertifikatbrukeren vet hva dette er og stoler på bankene. Internasjonalt vil dette bety at bare noen få globale strukturer vil kunne få allmenn aksept. I dagens marked er det etablert noen slike varemerker hvor det mest kjente er VeriSign.

Begrepet «kvalifisert sertifikat» kan betraktes ut fra samme tankegang. Dette er ikke et varemerke knyttet til en enkelt leverandør men en annen form for et innarbeidet begrep som impliserer tillit. Analogier kan være merking som «Godt norsk» eller former for miljømerking av varer.

10.4 Sjekk av sertifikater

Det å sjekke et sertifikat er samme prosess enten man behandler et sertifikat fra egen utsteder eller fra en annen og potensielt ukjent utsteder. Men prosessen kompliseres når man ikke «kjenner» sertifikatformat og utsteder. Da kan man trenge hjelp til prosessen.

26

http://www.verisign.com

27

BankID skal bli et varemerke (à la BankAxept) for en felles sertifikatstruktur for alle norske banker. Bankene skal selv være utstedere av sertifikater og systemet skal struktureres i et to-nivå-hierarki med en felles rot over bankene.

28

Se http://peid.sds.no for mer informasjon. Dette er en sertifikattjeneste primært for privatpersoner. Posten er utsteder og tjenesten drives av ErgoGroup.

29

ZebSign er Telenors kommende varemerke for sertifikater.

.

10.4.1 Tilbaketrekkingsinformasjon

Sjekking av om et sertifikat er trukket tilbake er en operasjon som i dagens praksis er anbefalt men som man ofte hopper over. Strengt tatt løper man i henhold til de fleste sertifikatpolicyer en stor risiko ved å la være å sjekke utstederens tilbaketrekkingsinformasjon fordi dette skyver mer ansvar over på sertifikatbrukeren. Innen forvaltningen vil det være et krav at tilbaketrekking skal sjekkes før et sertifikat godtas og det må legges til rette for at dette kan gjøres på en enkel måte for brukerne. Helst skal denne sjekken være helt usynlig for brukerne.

Tilbaketrekkingsinformasjon for en gitt utsteder kan man finne gjennom en peker i sertifikatet (CRL Distribution Point-utvidelsen) eller på annen måte. «Annen måte» betyr at sted for henting av tilbaketrekkingsinformasjon på forhånd må være satt inn i systemet hos sertifikatbrukeren eller at en menneskelig bruker eksplisitt utfører operasjonene. Automatisert tolkning av og bruk av CRL Distribution Point-utvidelsen i sertifikater støttes av en god del men ikke all programvare. Man er også avhengig av at utsteder faktisk legger denne informasjonen i sertifikatene og det er langt fra alltid tilfelle. Et tilleggsproblem for sjekk av tilbaketrekking er at dette ofte er en tidkrevende operasjon fordi:

- Prosessering av sertifikatkjeder er meget ressurskrevende.
- Sjekking av tilbaketrekkingslister kan være meget ressurskrevende fordi lengden på listen kan bli svært stor. Disse listene skal som oftest hentes over nettverket og prosesseres lokalt.

Et alternativ til tilbaketrekkingslister er tilgang til en OCSP-tjeneste[30] [55]. OCSP kan gi vesentlig raskere svar angående tilbaketrekking fordi det bare er en kort forespørsel online med et kort svar. Men det må være en tiltrodd tjeneste hvilket medfører noe ekstra kompleksitet.

10.4.2 Tolkning av meningsinnholdet i sertifikater fra forskjellige utstedere

Problemene knyttet til samtrafikk kan oppsummeres slik: Kan sertifikatbrukeren trekke den nødvendige informasjonen ut av sertifikatet i en forståelig form? Dette har to underpunkter: Finnes informasjonen i sertifikatet (dvs. i sertifikatprofilen) og kan sertifikatbrukeren tolke informasjonen i den formen den er kodet i sertifikatet?

Noen deler av informasjonsinnholdet i sertifikater er standardiserte og obligatoriske slik som algoritmeidentifikasjoner serienummer og den offentlige nøkkelen selv. Disse skaper ikke problemer men kryptoalgoritmene som brukes (både for signering av sertifikatet selv og for den offentlige nøkkelen i sertifikatet) må finnes hos sertifikatbrukeren.

Andre elementer i sertifikater er mer eller mindre obligatoriske i den forstand at alle «normale» sertifikatprofiler vil ha dem med og kodingen er veldefinert. Key Usage og Certificate Policies-utvidelsene er to eksempler her.

Navn finnes alltid i sertifikater men hva som inngår i navnene og hvordan denne informasjonen er kodet (f.eks. hvilke attributter) vil variere fra profil til profil. En menneskelig mottaker vil vanligvis kunne gi meningsinnhold til navn uavhengig av f.eks. om personnavn er kodet i Given Name- og Surname-attributtene eller i Common Name-attributtet. Men når mottaker er en applikasjon som skal trekke ut informasjon og viderebehandle den er slike forskjeller svært kompliserende. I praksis må alle profiler «kodes inn» i applikasjonen.

Navn som skal være egnet for automatisert viderebehandling bør inneholde ett unikt element – en unik identifikator – som applikasjonene kan ta tak i. Dette bør være tilstrekkelig til identifikasjon uten at andre

---

30 On-line Certificate Status Protocol.

deler av navnet behandles. Slike identifikatorer inngår i mange profiler men hvilke felt de er kodet i og hva de faktisk betyr varierer fra tilfelle til tilfelle. Spesielt for internasjonal samtrafikk vil det kunne være vanskelig å forstå hva en identifikator egentlig representerer.

Forskjellige sertifikatformater kan raskt bli et problem spesielt for applikasjoner og systemer. Også for menneskelige sertifikatbrukere som skal bruke sertifikater fra ulike tjenester kan situasjonen bli forvirrende. I et internasjonalt perspektiv kan man i tillegg få problemer knyttet til hvilket språk som er brukt.

Anbefalte sertifikatprofiler der man har spesifisert minimumskrav til innhold og koding for sertifikater av forskjellige typer (ansattsertifikat personsertifikat virksomhetssertifikat osv.) er et viktig tiltak for samtrafikk. Andre deler av sertifikatinnholdet kan være opp til hver enkelt utsteder.

10.5 Tilgang til utstederes offentlige nøkler

Sjekk av et sertifikat forutsetter at man har sikker tilgang til utstederens offentlige nøkkel. Denne kunnskapen kan man ha ved at utstederens offentlige nøkkel er verifisert og lagt inn i sertifikatbrukerens systemer på forhånd eller ved at den hentes f.eks. fra utstederens web-sider ved behov. Man kan også få tak i utstederens offentlige nøkkel ved at utstederen har et sertifikat utstedt av en annen utsteder – enten i et hierarki eller ved kryssertifisering. Det siste alternativet fører til et tilbakevendende problem: Man må ha sikker tilgang til denne utstederens offentlige nøkkel osv. I siste instans må man også her stole på en offentlig nøkkel som er lagt inn på forhånd eller som hentes når behovet oppstår.

Av dette resonnementet følger det at man til slutt må hente og stole på en offentlig nøkkel som ikke er sertifisert av en utenforstående part. Utstedere må derfor publisere sine offentlige nøkler på en måte som gjør at brukere kan ha tillit til dem og nøklene må beskyttes mot manipulering. Det siste gjøres ved at utstedere (i hvert fall de som ikke har noe sertifikat fra andre utstedere) publiserer sine offentlige nøkler gjennom egensignerte sertifikater. Dette gir ikke ordentlig autentisering av utstederen men det gir integritetsbeskyttelse av nøklene og autentisering dersom man stoler på at det egensignerte sertifikatet faktisk er fra utstederen.

Ved utstedelse av sertifikater vil alle utstedere sørge for at deres egne offentlige nøkler blir installert hos sertifikateieren. For smartkort o.l. vil utstederens offentlige nøkkel ligge i smartkortet mens den for programvareløsninger vil bli installert i sertifikateierens system. Men med tanke på samtrafikk er spørsmålet hvordan man kan få tak i offentlige nøkler for andre utstedere enn dem man selv har et kundeforhold til.

I langt de fleste tilfellene er man avhengig av at alle utstederes offentlige nøkler må være tilgjengelige lokalt hos sertifikatbrukeren. Mange internasjonale sertifikatutstedere har sørget for å få sine offentlige nøkler med i standarddistribusjonen av nettlesere (som Microsoft Internet Explorer og Netscape Navigator) og etter hvert i systemer som Microsofts Windows 2000. Dette utgjør nå ca. 140 offentlige nøkler. Sertifikater fra disse utstederne kan prosesseres uten videre. Ingen norske utstedere er med i denne listen.

For sertifikater utstedt av andre tjenester f.eks. av de norske aktørene innen området er man avhengig av at tjenestenes offentlige nøkler eksplisitt installeres hos brukerne. Når dette er på plass har man sørget for at sertifikater utstedt av disse tjenestene kan behandles og verifiseres.

Tillitsstrukturer forenkler situasjonen ved at offentlig nøkkel for én utsteder (roten i et hierarki eller en som har utstedt kryssertifikater) vil gi tilgang til andre utstederes offentlige nøkler gjennom sertifikater. Hos brukerne trenger man da i prinsippet ikke å installere offentlig nøkkel for mer enn én utsteder innenfor tillitsstrukturen men av effektivitetshensyn kan det likevel lønne seg å legge inn nøkler for flere utstedere. Da slipper man prosessering av sertifikatkjeder.

Det er også mulig å la utstedere «nedover» i et hierarki (kryss-)sertifisere roten slik at man kan starte med offentlig nøkkel for en vilkårlig utsteder i systemet (f.eks. den som har utstedt ens egne sertifikater) og få tak i roten gjennom et sertifikat. Dette er en løsning som har begrenset produktstøtte.

Det er ikke uvanlig at en sertifikateier oppgir (f.eks. legger ved en signert melding) alle sertifikater i en kjede fra seg selv og sin egen utsteder opp til roten men det er mer vanlig at man bare legger ved sitt eget sertifikat og overlater til sertifikatbrukeren å hente resten av sertifikatene i kjeden. I dette tilfellet må sertifikatbrukeren kunne gjøre katalogoppslag eller på annen måte kunne finne sertifikatene.

I et kryssertifiseringsregime er det ikke hensiktsmessig for sertifikateieren å oppgi mer enn sitt eget sertifikat. Sertifikatbrukeren må da finne et kryssertifikat utstedt av en utsteder som brukeren stoler på. Det enkleste tilfellet er der brukerens egen utsteder har en direkte kryssertifisering. Da kan sertifikatbrukeren greit finne kryssertifikatet fra egen utsteder som brukeren jo stoler på.

I hybride systemer med kombinasjon av krysssertifisering og hierarki er det generelt meget vanskelig å finne en sertifikatkjede som kan brukes til å etablere tillit. Det er rimelig klart at med et stort antall utstedere vil en hierarkisk struktur være desidert enklest.

En av de største fordelene med samtrafikktjenester er at de er i stand til å håndtere denne kompleksiteten på vegne av brukerne. Offentlige nøkler for et stort antall utstedere kan legges inn i tjenesten på en sikker måte slik at brukerne ikke behøver å forholde seg til sertifikatkjeder og tillitsstrukturer.

10.6 Distribusjonstjenester og kataloger

10.6.1 Behov for kataloger

Alle sertifikatutstedere vedlikeholder kataloger over egne utstedte sertifikater. En katalog kan være «intern» dvs. tilgjengelig bare for utstederen selv og kanskje et antall «kjernebrukere» – som alle banker for BankID. Slike kataloger vil inneholde alle sertifikater fra den spesifikke utstederen.

Andre kataloger kan være åpent tilgjengelige f.eks. på Internett eller tilgjengelige bare for en mer eller mindre lukket gruppe f.eks. gjennom abonnement. Sertifikateiere må som et minimum kunne reservere seg mot innlegging i åpne kataloger. Det kan tenkes at det i enkelte tilfeller vil være nødvendig med et aktivt samtykke. Sertifikater kan også eksporteres til andre kataloger enn dem utstederen selv kontrollerer f.eks. bedriftsinterne kataloger der dette ikke hindres av personvernhensyn.

Når det gjelder samtrafikk ligger problemene i at en sertifikatbruker ikke uten videre kan vite hvilken utsteders katalog som inneholder det sertifikatet brukeren er ute etter og det er heller ikke sikkert at brukeren har tilgang til den aktuelle katalogen (f.eks. fordi den bare er for abonnenter). Hvis man ikke vet hvem som har utstedt sertifikatet kan et søk over alle mulige utstedere være svært tidkrevende. Dersom søket skal implementeres i en automatisert prosess står man overfor en meget vanskelig oppgave.

Betydningen av katalogtjenester for sertifikater skal ikke overvurderes. Ved autentisering og signering vil sertifikateieren vanligvis legge ved sertifikatet (eller hele sertifikatkjeden om ønskelig) slik at sertifikatbrukeren ikke behøver å hente det selv. Sertifikater for en kommunikasjonspartner vil man normalt bare hente dersom man skal kryptere en melding til en mottaker og ikke har dennes sertifikat for dette formålet. Selv dette trenger ikke å involvere et avansert katalogsystem. Lokale kataloger med sertifikater for dem man vanligvis kommuniserer med oppslag på web-sider for informasjon om mottakeren eller rett og slett en e-post med spørsmål er høyst aktuelle metoder.

10.6.2 Kopling av kataloger

Direkte samspill mellom katalogsystemer er meget vanskelig. Forvaltningsnettsamarbeidet stilte krav til leverandørene om et system der sertifikatbrukerne bare trenger å forholde seg til sin egen utsteder. Utsteders katalogsystem skal videreformidle søk til andre utstederes kataloger. Dette viste seg å være en meget kompleks problemstilling og det var meget tidkrevende å få en løsning på plass. Kompleksiteten tilsier at slik kopling av katalogsystemer ikke vil være noen generell løsning på samtrafikk relatert til kataloger. Direkte kopling mellom kataloger krever i praksis at alle er basert på X.500-standarden.

Et alternativ til kopling er at kataloger ikke videreformidler søk men returnerer et «hint». Dette kan støttes av LDAP[31] [75] som nå er den klart anbefalte protokollen for katalogtilgang selv for

31

kataloger som er basert på X.500. Dette krever at utstedernes katalogsystemer inneholder mye informasjon om hvordan hint skal gis og at sertifikatbrukernes programvare (LDAP) kan behandle hint.

BankID har i praksis en felles katalogstruktur der alle sertifikater legges i samme katalog som så kan kopieres ut til den enkelte bank etter behov. Man kan tenke seg samme løsning som BankID altså en felles katalog som inneholder alt eller i hvert fall det meste av sertifikater fra norske utstedere. Realismen i dette er kanskje ikke så stor og gitt at katalogenes betydning ikke skal overvurderes er det antakelig heller ikke nødvendig med en felles katalog.

10.6.3 Metakatalog

En enklere variant av en felleskatalog er en «metakatalog» som inneholder informasjon om andre kataloger. Sertifikatbrukere kan da søke via metakatalogen som enten kan returnere hint om hvilken katalog som bør prøves eller som kan utføre søket på vegne av sertifikatbrukeren.

En metakatalog kan gjerne inneholde alle sertifikater for utstedere og alle kryssertifikater slik at sertifikatbrukere kan gå ett sted for å få fatt i dem.

10.6.4 Hvordan gjøre tilbaketrekkingsinformasjon tilgjengelig?

En sertifikatutsteder må gjøre tilbaketrekkingsinformasjon tilgjengelig. Det trengs ikke noe katalogsystem for dette men en velkjent Internett-adresse (URL) der informasjonen kan hentes. Det er sterkt anbefalt at denne adressen legges i sertifikatene i CRL Distribution-Point utvidelsen.

Alle utstedere i dag støtter tilbaketrekkingslister (CRL) som må hentes og prosesseres av sertifikatbrukeren og som er «selvbeskyttende» slik at distribusjonstjenesten ikke trenger å være tiltrodd. Dette skyver mye prosessering og mye ansvar over på sertifikatbrukeren.

Utstederen kan også velge å operere en tjeneste basert på OCSP [55]. I sin enkleste form gir dette et ja/nei-svar på om et sertifikat er gyldig basert på et spørsmål fra sertifikatbrukeren. En OCSP-tjeneste må være tiltrodd. Det betyr at tjenesten alltid må autentiseres overfor sertifikatbrukeren. For OCSP gjøres dette ved at svaret er signert men man kan også tenke seg bruk av en autentisert sikker kommunikasjonskanal for spørsmål og svar.

En samtrafikktjeneste kan erstatte OCSP-tjenester drevet av utstederne selv. Her kan brukerne tilbys ett punkt for sjekk av gyldighet av sertifikater fra flere utstedere.

10.7 Implementasjon og produktmessige aspekter

10.7.1 Implementasjon av tjenester som skal bruke sertifikater

Mulighetene for å bruke sertifikater fra forskjellige utstedere mot en gitt tjeneste bør prinsipielt bare være begrenset av hva tjenestetilbyderen ønsker å akseptere ut fra et organisatorisk og sikkerhetsmessig synspunkt. Dette forutsetter at tjenesten (applikasjonen) er implementert på en måte som muliggjør samtrafikk.

Samtidig finnes det et uttalt ønske om å slippe individuelle tilpasninger for hver enkelt sertifikattype som skal aksepteres. Dette kan oftest løses ved å isolere sertifikatbehandlingen i egne moduler eller ved bruk av samtrafikktjenester.

Lightweight Directory Access Protocol er en Internett-standard for aksess til katalogsystemer.

10.7.2 Krav til brukersiden for tjenester som skal bruke sertifikater

En tjeneste som krever digitale signaturer kan i dag ikke basere seg bare på standard programvare hos brukerne. Funksjonalitet for digitale signaturer støttes ennå ikke på en tilfredsstillende måte f.eks. av standard nettlesere.

Tjenesten kan da stille visse krav til hva brukerne skal ha på plass. De fleste leverandører av sertifikater vil levere tilleggsprogramvare for bruk av sertifikater og nøkler sammen med f.eks. nettlesere. Kravene vil være knyttet til karakteristikker for slik programvare hos brukerne f.eks. evnen til å kunne produsere visse dokumentformater.

Alternativt kan tjenestetilbyderen selv tilby brukerprogramvare som tar seg av de ønskede funksjonene men for samtrafikk er man avhengig av at programvaren som tilbys kan støtte sertifikater fra forskjellige utstedere.

Enda et alternativ er å tilby funksjonaliteten i form av programbiter som overføres integrert med web-sider (script Java applets Microsoft ActiveX Controller). Dette er i dag meget vanskelig sett fra et sikkerhetsmessig synspunkt og kan heller ikke gjøres på en enkel måte hvis man skal ta hensyn til samtrafikk – se [30].

Standardiseringsnivået for sertifikatprodukter med smartkort er ennå ikke på et slikt nivå at man kan unngå installering av spesielle komponenter for å kommunisere med smartkortet. Men disse spesialkomponentene kan i hvert fall i stor grad tilby standard programmeringsgrensesnitt. Dette er først og fremst et problem for mobilitet – det er enda et stykke igjen før en sertifikateier kan bruke sitt smartkort i en «vilkårlig» maskin.

10.7.3 Samspill mellom forskjellige produkter

Standarder innen PKI (selve X.509 v3 relaterte PKIX[32]spesifikasjoner og annet) gir i likhet med svært mange andre standarder rikelig rom for tilpasninger. Man kan lett havne i en situasjon der produkter fra to leverandører begge tilbyr profiler i overensstemmelse med standardene men som likevel ikke kan virke sammen.

I prinsippet bør produkter være fleksible med hensyn til profiler slik at tjenester har størst mulig fleksibilitet innen rammene av standardene. I praksis vil alle produkter ha visse begrensninger. Dette kan dreie seg om kryptoalgoritmer eller programmeringsgrensesnitt som ikke støttes visse felter attributter og utvidelser som ikke støttes i sertifikater osv. Til en viss grad er dette forståelig og det er rimelig at leverandørene ikke bruker mye ressurser på å støtte relativt «eksotiske» varianter.

I en del tilfeller kan det være at produktene nærmest blir skreddersydde til visse profiler og dermed kan det oppstå problemer i de tilfellene hvor en tjeneste eller en kunde ønsker å bruke noe annet. Ett eksempel på dette er muligheter for å prosessere kjeder av sertifikater som bør være et absolutt krav men som ikke har full støtte i alle produkter.

Et viktigere eksempel er knyttet konkret til Entrust[33]som er verdens største leverandør av PKI-produkter. Entrust har laget egne PKI-profiler og publisert disse. Entrusts produkter støtter

---

32

Public Key Infrastructure for X.509 er en arbeidsgruppe under IETF (Internet Engineering Task Force) som er ansvarlig for tekniske spesifikasjoner for Internett.

-

33

http://www.entrust.com

bare disse profilene med noen variasjoner og det finnes en rekke tredjepartsleverandører som har lagt opp sine produkter etter de samme spesifikasjonene (Entrust-Ready-produkter). Fordelen med denne tilnærmingen er at man har fått på plass et godt utvalg av produkter særlig på klientsiden som virker sammen uten store problemer ved at man har strammet tilstrekkelig inn på i utgangspunktet underspesifiserte standarder. Ulempen er at der Entrusts profiler ikke helt passer i forhold til kravene har man valget mellom å tilpasse kravene eller å stenge Entrust-Ready-produkter ute.

Det første alternativet å tilpasse seg Entrusts profiler kan bety dårligere tilpassede løsninger og det betyr at man lar profiler bestemt av én leverandør være utslagsgivende. Innen forvaltningen er det klart at man ikke bør legge spesifikasjoner fra enkeltprodusenter – selv om spesifikasjonene er åpne – til grunn for kravspesifikasjoner. Selv om de fleste andre leverandører kan tilpasse seg Entrust er dette klart konkurransevridende.

Med tanke på samtrafikk er det også uheldig å spesifisere en tjeneste på en måte som gjør at klienters sertifikater fra verdens største leverandør (med partnere) ikke kan brukes mot tjenesten.

10.8 Juridiske aspekter ved samtrafikk

10.8.1 Avtaleverk

En sertifikatutsteder vil ha avtaleforhold med flere andre parter:

- Egne kunder (sertifikateiere)
- Andre utstedere gjennom kryssertifisering eller i hierarkier
- Registreringsautoriteter (ikke spesielt relevant rolle for samtrafikk og derfor ikke berørt i dette kapitlet)

Sertifikatprodusent (datasentral med høy sikkerhet) der denne er forskjellig fra utsteder (som er den som er navngitt som utsteder i sertifikatene) – eksempelvis vil BBS[34]produsere sertifikater for BankID men bankene er utstedere

- Smartkortprodusent som også kan ha ansvaret for produksjon av nøkler
- Enkelte sertifikatbrukere spesielt tjenester (private eller offentlige) som ønsker å akseptere sertifikatene for adgang til tjenester
- Andre tiltrodde aktører som enten trengs for sertifikatutstedelse (f.eks. offentlige registre) eller som tilbyr tilleggsfunksjonalitet (f.eks. en samtrafikktjeneste).

Alle tillitsstrukturer forutsetter avtalemessige forhold. Man bør ikke kryssertifisere uten en gjensidig avtale mellom utstederne. I et hierarki kan det avtalemessige løses gjennom en sertifikatpolicy som brukes for å utstede sertifikater for underliggende utstedere men det er vanlig at man også her inngår eksplisitte avtaler (jf. interbankavtalen for BankID). Avtaler bør regulere ansvarsmessige forhold men avtaleinnhold kan variere sterkt fra ett tilfelle til et annet.

34

Bankenes betalingssentral http://www.bbsas.no

Med hensyn til samtrafikk er det likevel klart at ikke alle aktører vil ha eksplisitte avtaler med en gitt utsteder. Dette gjelder først og fremst mange sertifikatbrukere men det vil også gjelde utstedere som ikke deltar i noen felles tillitsstruktur.

Utstederen må gjøre klart sitt ansvar sine ansvarsbetingelser og ansvarsbegrensninger. Dette kan gå ut på at sertifikateieren er ansvarlig for visse sikkerhetsforanstaltninger at utstederen bare tar ansvar for bruk for bestemte formål begrensninger i erstatningsbeløp osv. Lovgivning rettsvalg og spesifikasjon av tvistemålshåndtering vil også normalt være med. De fleste slike forhold vil være regulert i en sertifikatpolicy. Aktører (særlig sertifikatbrukere) uten egen avtale med utstederen må da studere sertifikatpolicyen for å finne ut noe om den ansvarsmessige risikoen ved å akseptere et sertifikat.

10.8.2 Ansvarsforhold

For tjenester som ikke inngår i noen felles tillitsstruktur vil det normalt ikke eksistere noe avtaleforhold som regulerer ansvaret mellom utstedere. Med henblikk på ansvarsforhold må man vurdere hver tjeneste for seg.

Ved hierarkier eller kryssertifisering vil det normalt eksistere avtaler som regulerer ansvarsforholdene og slike forhold kan i tillegg være regulert i sertifikatpolicyer. Slike avtaler bør dekke opp forhold der en sertifikatbruker er kunde hos én utsteder og der brukeren kan stole på et sertifikat utstedt av en av de andre utstederne i tillitsstrukturen. Som regel vil dette bli gjort ved at en sertifikatbruker bare trenger å forholde seg til sin egen utsteder ved feilsituasjoner. Denne utstederen vil så ta seg av forhold mot den utstederen som faktisk er ansvarlig for feilen (jf. BankID og Forvaltningsnettsamarbeidet).

For hierarkiske strukturer er det knyttet et spesielt problem til hvilket ansvar roten tar på seg og hvilken aktør som skal ha dette ansvaret. I hvor stor grad er roten ansvarlig for (sine vurderinger av) egnetheten til utstedere lenger nede i hierarkiet? Finnes det noen aktør som naturlig bør ta ansvaret for roten og har denne aktøren i tilfelle styrke til dette? For BankID tar bransjeforeningene (Sparebankforeningen og Finansnæringens Hovedorganisasjon) ansvaret sammen og dette betyr i siste instans at deres medlemmer er solidarisk ansvarlige. Men hierarkier som binder sammen utstedere uten noen felles tilknytting gjennom bransjeforeninger eller på annen måte vil ikke ha noen naturlig rotaktør. I andre tilfeller vil f.eks. en bransjeforening ikke ha tilstrekkelig styrke til å ta på seg reelt ansvar av betydning.

10.9 Oppsummering av problemområder

For samtrafikk kan man oppsummere de viktigste problemområdene relatert til elementene i en PKI slik:

- Forskjellige profiler av standardene kan føre til samtrafikkproblemer mellom produkter fra forskjellige leverandører og enkelte produkter er tett knyttet til bruk av visse profiler (f.eks. Entrust-Ready). På noen områder mangler det standarder.
- Tillitsstrukturer løser langt på vei samtrafikk mellom utstedere som har valgt å inngå avtaleforhold og delta i en tillitsstruktur (hierarki eller kryssertifisering). Men man vil aldri få tillitsstrukturer som omfatter alle utstedere derfor vil en sertifikatbruker uansett være nødt til å forholde seg til «utenforstående» utstedere.
- Tillitsstrukturer fordrer prosessering av sertifikatkjeder. Dette er ressurskrevende og kompliserende og støttes ikke av alle produkter.
- Avtaleverk regulerer forholdene mellom aktører (utstedere og sertifikateiere/andre utstedere/enkelte sertifikatbrukere) men man vil alltid kunne få situasjoner der en sertifikatbruker ikke har noen eksplisitt avtale verken med den aktuelle utstederen eller sertifikateieren.
- Sertifikatpolicy og sertifikatpraksis angir kvalitetsnivå på tjenestene og regulerer ansvar m.m. men det er vanskelig å sammenlikne tjenester fordi de i dag ikke

kategoriseres i nivåer (bortsett fra etter hvert kvalifisert nivå). Sertifikatpolicyer (og -praksiser) er dokumenter som er vanskelig tilgjengelige selv for eksperter. Metoder for karakterisering av tjenester i et begrenset antall diskrete kvalitetsnivåer trengs.

- Sertifikatformater fra forskjellige utstedere vil variere og dette skaper problemer spesielt for automatisk viderebehandling basert på sertifikatinnholdet. Det er behov for basis sertifikatprofiler som kan sikre at viktig informasjon er med i alle sertifikater og kan finnes på samme sted i sertifikatene.
- Distribusjonstjenester for sertifikater er et vanskelig område for samtrafikk fordi samspill mellom flere uavhengige kataloger er vanskelig og sertifikatbrukere kan ikke uten videre vite hvilken katalog det er riktig å søke i. Metakataloger som kan hente informasjon fra andre kataloger eller returnere fornuftige hint om hvor man skal søke kan være en løsning.

10.10 Forvaltningens behov for samtrafikk

Forvaltningen kan vanskelig rette krav relatert til samtrafikk direkte til sertifikateierne men kravene kan søkes oppfylt gjennom tiltak i forhold til utstederne.

10.10.1 Behov for tillitsstrukturer

Det er naturlig for forvaltningen å kreve etablering av tillitsstrukturer for de PKI-tjenestene som forvaltningen selv benytter som utstedere. Krysssertifisering – som Forvaltningsnettsamarbeidet – virker som den mest hensiktsmessige løsningen så lenge antallet utstedere forvaltningen har avtale med er relativt lite. Forvaltningen bør stille krav til innholdet i kryssertifiseringsavtaler på samme måte som det er gjort for Forvaltningsnettsamarbeidet.

Med tanke på grenseflaten mellom offentlig og privat sektor bør forvaltningen aktivt arbeide for etablering av tillitsstrukturer f.eks. BankID men det er vanskelig å se at det finnes noen «maktmidler» som er hensiktsmessige. For rent privat sektor gjelder den samme anbefalingen om aktivt arbeid for å få tillitsstrukturer på plass.

10.10.2 Forvaltningens behov for sertifikatkataloger

Forvaltningen vil ønske seg god tilgang til alle sertifikater for ansatte i offentlig sektor f.eks. gjennom en videreføring av katalogstrukturen fra Forvaltningsnettsamarbeidet. Det er viktig å lage regelverk som sikrer at alle utstedere sørger for det nødvendige «bokholderiet» knyttet til tjenestene. Men forvaltningen kan vanskelig kreve avanserte katalogtjenester fra alle utstederne og i hvert fall ikke at kataloger generelt skal kunne virke sammen. Løsninger med metakataloger er mulig men utvalget anbefaler ikke å sette i gang noen større aktiviteter rundt sertifikatkataloger. Dersom prosjekter rundt generelle kataloger startes anbefales det å få med sertifikater som ett element i dette arbeidet.

10.10.3 Løsninger for tekniske problemstillinger

Bruk av standardiserte profiler

I Norge vil felles profiler forenkle samtrafikk. Både for offentlig og for privat sektor anbefaler utvalget derfor at det brukes mest mulig felles profiler.

Tilgjengelige produkter

Ettersom man stort sett er prisgitt de store internasjonale leverandørene når det gjelder hva som er tilgjengelig av produkter er det begrenset hvor mye påvirkning man kan få til fra Norge. Det er uheldig å

stille krav etter en enkelt leverandørs spesifikasjoner men det er også uheldig spesielt med tanke på samtrafikk å lage spesifikasjoner som har lite støtte i produkter. Utover det at man alltid må holde seg innenfor standardene er det eneste rådet utvalget kan gi i denne omgangen å stille de kravene man mener bør oppfylles og så justere dem etter hva det er mulig å få til med dagens produkter. Et nært samarbeid med leverandørene i spesifikasjonsfasen viste seg å være nyttig for Forvaltningsnettsamarbeidet.

Objektive og ikke-diskriminerende krav ved valg av standarder

Det bør stilles krav til at relevante standarder (og profiler) følges ved kommunikasjon med offentlig sektor. Disse skal i størst mulig grad være harmoniserte offentliggjorte og tilgjengelige. Dersom slike ikke finnes fra internasjonale standardiseringsorganer kan forvaltningen selv definere krav til standarder og profiler.

Allment tilgjengelige tjenester

Konkurranse i telemarkedet er et virkemiddel for å nå de telepolitiske målene bl.a. at alle husholdninger og bedrifter over hele landet skal ha tilgang til grunnleggende teletjenester av høy kvalitet til lavest mulig pris. Forvaltningen har behov for å sikre at dette også skal gjelde for sertifikattjenester.

10.10.4 Avtalemessige forhold

De største avtalemessige problemene ved bruk av PKI ligger i håndtering av ansvar når sertifikatbrukeren ikke har noe som helst avtaleforhold med utstederen og heller ikke med noen annen utsteder innenfor en tillitsstruktur som utstederen er med i.

For forvaltningen er det viktig at avtalemessige forhold er på plass og det er sannsynlig at offentlige virksomheter vil ønske å inngå eksplisitte avtaler med utstederne de aksepterer sertifikater fra på grenseflaten mot privat sektor – også der utstederen ikke har egen avtale om levering av sertifikater til det offentlige. Subsidiært må offentlige virksomheter sjekke sertifikatpolicy/sertifikatpraksis for å avgjøre om det er f.eks. ansvarsmessige forhold som ikke er akseptable.

For rent privat sektor er det viktig med en viss lovmessig regulering av det ansvaret en utsteder må ta på seg spesielt med hensyn til forbrukervern.

Dersom man ender opp med en strukturering av sertifikattjenester i et hierarkisk system kan det tenkes at det er nødvendig for det offentlige å ta ansvar for å unngå at gode intensjoner ikke blir realisert fordi ingen kan eller vil ta ansvaret for roten.

Alle til alle-kommunikasjon

I telemarkedet fokuserer regelverket på at det er de sterke operatørene (som har mer enn 25 % av det relevante markedet) som pålegges å inngå avtale om samtrafikk. I praksis betyr det at Telenor fungerer som navet i et hjul og sikrer at alle telekunder kan kommunisere med hverandre. Også Telenor Mobil og NetCom er pålagt å inngå samtrafikkavtaler med andre når disse etterspør det.

Dette systemet vil ikke direkte kunne overføres til sertifikattjenester i form av pålegg om kryssertifisering eller et felles hierarki. Men et parallelt system kan implementeres ved hjelp av en samtrafikktjeneste. Dersom alle utstedere har en avtale med samtrafikktjenesten og utleverer nødvendig informasjon f.eks. om tilbaketrekkinger vil sertifikatbrukere kunne forespørre samtrafikktjenesten om gyldigheten av sertifikater fra «vilkårlige» utstedere. I prinsippet kan en samtrafikktjeneste faktisk også tilby sjekk av sertifikater fra andre utstedere enn de den har eksplisitte avtaler med men dette vil ansvarsmessig medføre en meget uklar situasjon.

Dersom en samtrafikktjeneste skal ha en så sentral rolle som et «nav» for samtrafikk ved bruk av sertifikater må det utredes nærmere hvilke krav – og eventuelt hvilket ansvar – forvaltningen skal stille til tjenesten. Dersom man ikke pålegger en samtrafikktjeneste en slik «obligatorisk» rolle kan samtrafikktjenester tilbys i markedet til aktører som har behov for det.

En samtrafikktjeneste vil likevel ikke fjerne behovet for tillitsstrukturer som kryssertifisering. Tillitsstrukturer regulerer avtalemessige forhold direkte mellom utstederne og vil på denne måten være tryggere for brukerne. En gjennomgående kryssertifisering eller et hierarki sikrer også alle til alle-

kommunikasjon for et gitt sikkerhetsnivå uten at man er avhengig av enten en samtrafikktjeneste eller av å stole på et stort antall utstedere.

For å sikre alle til alle-kommunikasjon hva gjelder kommunikasjon med offentlige virksomheter kan man tenke seg et system der det overlates til markedet å organisere ordninger for kryssertifisering men at staten stiller som krav at de som skal utstede sertifikater til aktører innen forvaltningen skal kryssertifiseres med hverandre slik det er gjort for Forvaltningsnettsamarbeidet.

Prising

På teleområdet er prisen for samtrafikk den største kilden til konflikt. Operatører med sterk markedsstilling er forpliktet til å ta kostnadsorienterte samtrafikkpriser men de mindre operatørene er ofte av den oppfatning at prisene gir en avkastning for de store som er høyere enn «rimelig avkastning av anvendt kapital» (det regulatoriske kravet).

For en samtrafikktjeneste for elektroniske sertifikater kan man tenke seg flere løsninger. Den ene ytterligheten er at alle operatører dekker sine egne kostnader og at det ikke finnes felles katalog eller tjenester. I den andre enden av skalaen kan man se for seg at man oppretter en felles samtrafikktjeneste (database) som drives som et selvstendig selskap og der operatørene betaler for bruk av den felles ressursen.

Det er på nåværende tidspunkt vanskelig å se om noen av alternativene peker seg ut som mest ønskelige. Valg av løsning kan også overlates til markedet med mindre det er spesielle forhold knyttet til kommunikasjon med det offentlige som bør ivaretas.

10.10.5 Forvaltningens behov for tilsyn med samtrafikken

Samtrafikk er en del av premissene for å få PKI til å fungere på samfunnsnivå. Hvis forvaltningen stiller krav til at samtrafikk skal være mulig og eventuelt hvordan den skal foregå vil det være behov for å påse at kravene blir fulgt. Det kan gjøres på flere måter og spørsmålet er hva som vil være et fornuftig rettslig virkemiddel. Forvaltningen kan kreve at aktører som forvaltningen vil benytte forplikter seg til gode samtrafikktjenester. Forvaltningen bør sammen med relevante tilsynsmyndigheter og markedsaktører arbeide for etablering av slike tjenester.

Dersom samtrafikk realiseres (delvis) gjennom en separat samtrafikktjeneste kan det være nødvendig å stille egne krav til (tilsyn med) denne tjenesten – se nedenfor.

Det er Forsvarets/totalforsvarets og Direktoratet for sivil beredskaps oppgave å sørge for at en PKI fungerer i krise- og krigssituasjoner. Forvaltningen bør selv kunne definere sine behov og hvilke tiltak som må settes i verk i slike situasjoner.

10.10.6 Forvaltningens behov for internasjonal samtrafikk

Det er foreløpig gjort lite for å kartlegge hvilke behov forvaltningen har for elektronisk kommunikasjon over landegrensene. Det er klart at det til en viss grad vil være behov for kommunikasjon med andre lands forvaltninger og også med organer som EU FN og andre. Behov for kommunikasjon med utenlandske virksomheter kan oppstå f.eks. i forbindelse med internasjonale anbudsforespørsler og kommunikasjon med borgere som er bosatt i utlandet kan oppstå f.eks. ved søknader om arbeids- og oppholdstillatelse og i forbindelse med trygd. I det siste tilfellet har Rikstrygdeverket identifisert et klart behov knyttet til internasjonal samtrafikk med tanke på sine ca. 16 000 utenlandske «kunder».

Det viktigste virkemiddelet i dag er at forvaltningen deltar i internasjonalt arbeid innen relevante områder og at spesifikasjoner i Norge legges så tett som mulig opp mot det som er vanlig i våre nærmeste samarbeidsland. Oppfølging av arbeid i EU kan ha spesiell betydning.

Merk at krav om tilgang til fødselsnummer kan virke ekskluderende i forhold til utenlandske sertifikattjenester. Sertifikattjenesten må verifisere et oppgitt fødselsnummer mot folkeregisteret før sertifikatutstedelsen for å kunne produsere en korrekt tabell og det er tvilsomt om slik adgang vil kunne gis til utstedere utenfor Norge.

10.10.7 En separat samtrafikktjeneste

Hva oppnår man med en samtrafikktjeneste?

En samtrafikktjeneste er en separat tjeneste som kan svare på forespørsler om i prinsippet vilkårlige sertifikater. En samtrafikktjeneste kan innhente informasjon om en rekke sertifikatutstedere og effektivisere sjekking av sertifikater utstedt av disse. Bruk av en samtrafikktjeneste kan være fordelaktig fordi:

- Tilbaketrekkingslister kan hentes regelmessig slik at samtrafikktjenesten ikke trenger å gjøre dette for hver enkelt forespørsel. Tjenesten kan bygge en tabell over tilbaketrukkete sertifikater og bare sjekke mot denne.
- Tjenesten kan ta seg av kompleksiteten knyttet til prosessering av forskjellige sertifikatprofiler på vegne av brukerne.
- Tjenesten kan holde styr på et stort antall offentlige nøkler for utstedere.
- Sertifikatkjeder kan behandles på forhånd slik at sjekk av sertifikater normalt vil kunne gjøres bare i forhold til utstederen uten ekstra prosessering knyttet til hierarkier kryssertifisering etc.
- Samtrafikktjenesten kan gjøre vurderinger av sertifikatpolicy og eventuelt annen informasjon med tanke på å kategorisere tjenester f.eks. i kvalitetsnivåer.
- Samtrafikktjenesten kan trekke ut eller avlede tilleggsinformasjon fra sertifikater f. eks. «oversette» unik identifikator til fødselsnummer basert på den aktuelle utstederens tabell for dette.

Den viktigste ulempen knyttet til bruk av samtrafikktjenester er at dette er enda en tjeneste som man må stole på og som må være tilgjengelig. Tjenesten vil kunne «sitte på» mye sensitiv informasjon både knyttet til sertifikatene selv og til logging av hvilke forespørsler som kommer fra forskjellige kunder.

Juridiske aspekter for samtrafikktjenester

En samtrafikktjeneste som tilbys store (institusjonelle) brukersteder vil kunne ha et klart regulert forhold både til eierskap (til informasjon) bruksområder for tjenesten og tjenestetilbudet (kvalitet).

En samtrafikktjeneste som tilbyr policyavklaringer/policymapping f.eks. gjennom kategorisering i forhold til kvalitetsnivåer kan ha et stort ansvar i og med at dette vil være en tjeneste utover det som tilbys fra hver enkelt sertifikatutsteder.

Eierskap til sertifikat og tilleggsinformasjon vil være viktig. Hvem eier hvilken informasjon og hvordan kan denne informasjonen brukes? Tilleggsinformasjon vil ofte bare kunne utleveres til autoriserte brukere for autoriserte anvendelser og med sikkerhetstiltak som oppfyller f.eks. Datatilsynets regler.

En samtrafikktjeneste vil stå ansvarlig for det som sendes ut av svar på henvendelser. Et slikt ansvar vil samtrafikktjenesten kun ønske å påta seg dersom det eksisterer avtaler mot sertifikatutsteder.

Anbefalinger om samtrafikktjeneste

Gitt kompleksiteten i samtrafikkproblemene antar utvalget at samtrafikktjenester på sikt kan være den mest tiltalende løsningen. Men det finnes ikke slike tjenester i Norge i dag og det finnes få produkter for å realisere slike tjenester.

En samtrafikktjeneste for forvaltningen kan etableres i markedet i samarbeid med andre aktører som trenger en slik tjeneste. Forvaltningen kan da bidra i utviklingen av tjenesten også økonomisk for å få en tjeneste som er tilpasset forvaltningens krav.

Det antas at dette er en bedre løsning enn å etablere en sentral samtrafikktjeneste kun for forvaltningen eller separate samtrafikktjenester for hver enkelt offentlig virksomhet som måtte ha behov for det (eksempler kan være Skattedirektoratet Rikstrygdeverket). Det er vanskelig å tenke seg noe annet enn at samtrafikktjenester for privat sektor blir tilbudt på et markedsmessig grunnlag.

Det vil være naturlig at flere aktører tilbyr samtrafikktjenester i markedet. Tjenestene kan som et utgangspunkt være knyttet opp mot spesielle tillitsstrukturer eller systemer (f.eks. BankID) men må kunne svare for utstedere utenfor disse systemene.

10.11 Anbefalinger for forvaltningens strategi

Dette mandatpunktet viser at det er mye som er uavklart i forbindelse med samtrafikk. Bl.a. er det forskjellige profiler for standardene som brukes og det mangler en del standarder. Det finnes liten kompetanse på området. Tillitsstrukturer vil bare løse deler av utfordringene knyttet til samtrafikk og avtaler mellom aktører er bare delvis på plass. Samtrafikk er fortsatt et ferskt felt der få kan vise til praksis.

Utvalget anser det som riktig å stille krav som man mener bør oppfylles for deretter å justere dem etter hva det er mulig å få til. Utvalget har følgende anbefalinger:

a) Forvaltningen bør arbeide for etablering av tillitsstrukturer (kryssertifisering eller hierarki). Forvaltningen bør kreve denne typen strukturer for utstedere det offentlige har avtaler med. I øyeblikket antas det at det ikke er nødvendig at det offentlige oppretter en egen rot eller bro slik man har gjort i en del andre land. Men dersom dette framstår som den naturlige løsningen bør det offentlige være villig til å ta initiativer jf. problemene rundt ansvarsavklaringer og tilgjengelighet av en «naturlig aktør» med ansvar for roten av tillitsstrukturer.

b) Det anbefales ikke å sette i gang initiativer eksplisitt for sertifikatkataloger bortsett fra at man bør opprettholde kravene fra Forvaltningsnettsamarbeidet om «gode» kataloger og helst også samspill mellom disse internt i offentlig sektor. På sikt kan man vurdere etablering av en tjeneste for metakatalog med kopling mot (offentlige) kataloger for forskjellige utstedere.

c) Utvalget anbefaler at forvaltningen ved samordningsfunksjonen tar initiativ til etablering av samtrafikktjenester som kan motta sertifikater fra «vilkårlige» utstedere og returnere informasjon om sertifikatet og eventuelt utlede informasjon fra innholdet. En samtrafikktjeneste bør implementeres gjennom et samarbeid mellom forvaltningen og private aktører og tjenesten bør tilbys av kommersielle tilbydere. Det kan være aktuelt for forvaltningen å delfinansiere etableringen av tjenesten som deretter må kunne operere på kommersielle vilkår.

d) Det bør utredes om forvaltningen har felles krav til verifikasjonsinformasjon i forbindelse med behandling av sertifikater.

Del IV
Forslag til regulering av elektronisk kommunikasjon med og i forvaltningen

11 Forslag til regulering av bruk av digitale signaturer og dokumentkryptering i forvaltningen

11.1 Bakgrunn

Dette kapitlet inneholder diskusjon og skisse til et mulig *regelverk* for hvordan digitale signaturer og kryptering kan tas i bruk med og i forvaltningen. Verken den nye loven om elektronisk signatur eller eRegel-prosjektet dekker de behovene og kravene til konkret regulering som det presenteres forslag til. Det gjør heller ikke andre deler av utvalgets anbefalinger. I dette kapitlet fremmes det imidlertid forslag til hvordan forvaltningen mer konkret kan ta i bruk de anbefalte løsningene for digitale signaturer og kryptering.

Utvalget mener det er behov for et felles grunnlag for å ta løsningene i bruk. Dels vil dette være til hjelp for den enkelte virksomhet dels vil man unngå helt ulike framgangsmåter.

Utvalget mener de reglene som foreslås og oppsummeres i dette kapitlet generelt bør sees i sammenheng med regler for elektronisk saksbehandling. På området for sikring av taushetsplikt finnes beskyttelsesinstruksen jf. omtale i punkt 1.2 siste avsnitt og utvalget mener at elektronisk behandling av opplysninger gradert etter beskyttelsesinstruksen bør sees i sammenheng med de reglene utvalget foreslår i dette kapitlet. Både beskyttelsesinstruksen og (forhåpentligvis) skissen til regler vil være gjenstand for videre arbeid fra de ansvarlige regelverksforvalterne og utvalget mener dette vil være en god anledning til å se utviklingen av disse regelområdene i sammenheng.

I punkt 11.2 behandles spørsmålet om regler for signering og autentisering i punkt 11.3 regler for innholdskryptering. Under punkt 11.4 følger noen overordnede synspunkter på etablering av sikkerhetstjenester for forvaltningen. I punkt 11.5 diskuterer vi om det er lurt med veiledning (retningslinjer) eller bindende regler i form av lov eller forskrift. I punkt 11.6 gir utvalget en samlet oversikt over anbefalingene.

eRegel-prosjektet (Kartleggingsprosjektet [47]) påpeker at hvorvidt man kan/bør åpne for elektronisk kommunikasjon i en bestemmelse må vurderes ut fra den aktuelle bestemmelsen sammen med andre relevante bestemmelser.

Saksbehandlere som skal ta i bruk digitale signaturer og kryptering i saksarbeidet kan trenge regler for når teknikkene kan brukes og hvordan de skal brukes i ulike sammenhenger [62]. Bruken vil variere fra institusjon til institusjon og ligger til dels utenfor utvalgets mandat.

Utvalgets anbefalinger er ment som grunnlag for videre arbeid og diskusjon omkring frambringelsen av nødvendige regler. Anbefalingene er ikke og er heller ikke ment å være et ferdig bearbeidet forslag til regler. Det er heller ikke meningen å utelukke andre løsninger enn de skisserte. Enkelte av forslagene er med hensikt spissformulert i håp om å stimulere diskusjonen.

11.1.1 Aktuelle problemstillinger

Anbefalingene gir åpning for å benytte flere sikkerhetsnivåer og ulike modeller for implementering av sertifikattjenester mv. De gir rom for å la det enkelte forvaltningsorgan velge å benytte andre sikkerhetstjenester enn digitale signaturer. Dersom det fattes beslutning om å tilby offentlige personsertifikater vil det være naturlig at forvaltningen bygger sine løsninger rundt disse. Ettersom det foreløpig ikke er fattet noen slik beslutning må de foreslåtte reglene forsøke å favne også andre løsninger.

Bruk av digitale signaturer og kryptering berører den generelle saksbehandlingen. I anbefalingene er det derfor gjort forsøk på å behandle grenseflatene mot og gi forslag til utfylling av regelverk som berøres av bruk av digitale signaturer og kryptering. Dette gjelder f.eks. generelle regler for elektronisk saksbehandling og arkiv.

Den interne organiseringen av departementer og etater med hensyn til hvem som har kompetanse til å underskrive eller avgi uttalelse i ulike sammenhenger hvem underskriver hva er spørsmål som i alle fall i prinsippet er uavhengige av bruk av moderne kommunikasjonsteknologi. På den andre siden vil en økende

grad av automatisering og «selvbetjening» i forvaltningen samt endringer i arbeidsflyt ved innføring av elektronisk saksbehandling skape nye muligheter og utfordringer. Dette prøver utvalget å ta hensyn til.

Kjernen i regler om bruk av digitale signaturer og kryptering vil være bestemmelser som retter seg mot brukerne – både internt i forvaltningen og mot enkeltpersoner når disse kommuniserer med forvaltningen.

Det kan gjennomføres et systematisk skille mellom 1) regler for bruk av digitale signaturer og 2) regler for kryptering. Behovet for henholdsvis signering og kryptering utløses av ulike bestemmelser og oppfølgingen følger også forskjellige linjer.

F.eks. vil spørsmål om valg av metode for å «underskrive» en klage over et forvaltningsvedtak og den etterfølgende vurdering av om klagen skal tas under behandling eller avvises følge forvaltningslovens regler om klage. Samtidig kan henvendelsen være underlagt taushetsplikt etter forvaltningsloven. Det er ikke de samme hensynene som gjør seg gjeldende i disse to tilfellene. Det er heller ingen sammenheng mellom sanksjoner ved overtredelse.

Henvendelsen kan også være underlagt krav til sikring av personopplysninger etter personopplysningsloven. Disse bestemmelsene spenner antakelig over begge de nevnte regelsett idet man etter omstendighetene skal sikre både datakvalitet integritet konfidensialitet og tilgjengelighet.

Det kan også være behov for samordning med reglene om behandling av dokumenter/informasjon gradert etter beskyttelsesinstruksen. Utvalgets arbeid er begrenset til sivil sektor utenfor sikkerhetslovens[35]virkeområde. Hvilke krav som vil bli stilt til elektronisk behandling av dokumenter gradert etter beskyttelsesinstruksen etter at datasikkerhetsdirektivet blir opphevet er foreløpig uklart for oss. Det bør imidlertid vurderes om det er mulig å samordne kravene for graden «Fortrolig» i beskyttelsesinstruksen med krav som følger f.eks. av taushetsplikt og sikring av sensitive personopplysninger.

Man kan tenke seg at det blir innført generelle krav til bruk av sikkerhetstjenester for nærmere angitte anvendelser. Det er f.eks. mulig at krav til bruk av signaturteknologi kan knyttes til den aktuelle meldings «rettslige status» f.eks. til om meldingen vil utgjøre et saksdokument i arkivlovens forstand eventuelt kombinert med spørsmålet om det utløser rettigheter eller plikter for noen involverte eller om meldingen vil være underlagt krav etter økonomireglementet. Det kan tenkes at meldinger som *verken* er saksdokument *eller* relevant som dokumentasjon etter økonomireglementet skal være helt unntatt fra retningslinjene om bruk av autentiseringstjenester eller signeringsteknologi. Slike meldinger kan ha behov for integritets- og/eller autentisitetstjenester.

Selv om en melding er unntatt fra krav til autentiseringstjenester og signeringsteknologi kan den likevel være underlagt krav til innholdskryptering. F.eks. kan meldingen være knyttet til utvalgsarbeid og inneholde opplysninger som ikke er offentlige men likevel ikke være et saksdokument for det aktuelle organet.

Fordi behovene for sikkerhetstjenester kan variere mellom forvaltningsorganene og den enkelte anvendelse er det i anbefalingene lagt opp til en viss grad av frihet for organene til selv å velge den løsningen de finner tilfredsstillende og hensiktsmessig eventuelt innenfor rammen av alternativer trukket opp av et koordinerende organ for forvaltningen.

Etatenes anskaffelse av verktøy/system/løsning for digitale signaturer og kryptering omfattes ikke av retningslinjene. Dette er interne prosesser som ikke behøver låses fast i retningslinjer som retter seg mot andre. Det gir større fleksibilitet med hensyn til å utnytte mulighetene som ligger i framtidig utvikling av sikkerhetstjenestene i markedet. Retningslinjer for bruk må derimot forankres i regelverk som er bindende også for andre enn forvaltningen selv.

35

Lov om forebyggende sikkerhetstjeneste av 20. mars 1998 nr. 10 med tilhørende forskrifter (ikke i kraft).

11.1.2 Forholdet til lov om elektronisk signatur

Lov om elektronisk signatur [52] implementerer Direktiv 1999/93/EF og behandler først og fremst spørsmål knyttet til sertifikatutsteders virksomhet og funksjonelle krav til og rettsvirkningene av såkalte «kvalifiserte elektroniske signaturer». Loven berører i liten grad reglene for bruk av elektroniske signaturer og den behandler ikke spørsmålet om innholdskryptering.

Dersom forvaltningen velger å bygge sine løsninger på annet enn kvalifiserte sertifikater og såkalte sikre signaturframstillingssystemer gir loven liten veiledning. Utvalget forutsetter at det kan velges andre løsninger i tillegg derfor er det nødvendig å berøre enkelte spørsmål som også er behandlet i loven.

11.1.3 Forholdet til eRegel-prosjektet

Spørsmålet om hvilke av de ulike form- og prosedyrekravene i lovgivningen som kan oppfylles med elektronisk kommunikasjon og elektronisk signatur og eventuelle endringer i lovens krav er ikke noe hovedanliggende for utvalget. De spørsmålene er til vurdering i det enkelte departement som et ledd i eRegel-prosjektet. Som del av den prosessen må man blant annet vurdere hensynene bak det enkelte form- og prosedyrekrav. I denne utredningen forutsettes det at de nødvendige tilpasningene blir gjennomført.

Det regelverket som anbefales utviklet på grunnlag av forslagene i dette kapitlet vil derimot utgjøre et rammeverk som regelverksforvaltere kan støtte seg på når man skal vurdere å tillate elektronisk kommunikasjon og velge løsninger for hvordan dette kan skje på det enkelte området.

Selv om det ikke finnes form- eller prosedyrekrav i lovgivningen som er til hinder for elektronisk kommunikasjon eller stiller krav til bruk av sikkerhetstjenester kan det være f.eks. bevismessige forhold eller risikovurderinger som gjør det hensiktsmessig eller nødvendig å ta i bruk slike tjenester.

11.1.4 Språk og begreper i dette kapitlet

Skissen til regelverk har ikke gjennomgått noen separat språklig eller regelteknisk bearbeiding. Etter formålet har det ikke vært nødvendig og med den tid og de ressurser som har vært tilgjengelig ville det heller ikke vært mulig.

Det er ikke utarbeidet entydige definisjoner men en beskrivelse av hvordan noen sentrale begreper benyttes i dette kapitlet kan være på sin plass ettersom kapitlet ender med en skisse til noe utvalget mener bør bli et regelverk. Begreper som «melding» «henvendelse» «dokument» og «materiale» kan være synonymer avhengig av sammenhengen. Det skilles ikke konsekvent mellom begreper som «data» og «informasjon». Derimot benyttes begrepet «opplysning» som en nøytral form som kan dekke begge betydninger. Begreper som «forvaltningsorganet» «organet» «etaten» og «virksomheten» kan være brukt om hverandre uten at det er noen tilsiktet realitetsforskjell. Begrepene «borger» «den enkelte» «enkeltpersoner» og liknende benyttes om den som kommuniserer med forvaltningen i annen egenskap enn som ansatt i forvaltningen.

Begrepene «elektronisk signatur» og «digital signatur» brukes slik de for tiden vanligvis benyttes på området.[36] Begrepene «signeringsnøkler» og «krypteringsnøkler» brukes om data som benyttes i forbindelse med henholdsvis digitale signaturer[37]og innholdskryptering.

36

Med «digital signatur» menes her anvendelse av systemer for offentlignøkkel-kryptering og sertifikater utstedt og administrert innenfor en offentlignøkkel-infrastruktur (PKI). Med «offentlignøkkel» siktes det til at nøkkelen er offentlig tilgjengelig – ikke at den nødvendigvis har noen tilknytning til det offentlige. Med «elektronisk signatur» menes den videre anvendelse av autentiseringsteknikker som definert i lov om elektronisk signatur jf. § 3 nr. 1.

Det er imidlertid et problem at en del av reglene skal gjelde både for digitale signaturer med tilhørende sertifikater og for andre signerings- og autentiseringsteknikker f.eks. PIN-koder og passord hvis forvaltningsorganet benytter slike løsninger. I noen sammenhenger vil man kunne fellesbehandle PIN-koder/passord («autentiseringsdata») og offentlige nøkler («signaturverifiseringsdata») f.eks. ved krav til autentisering av melding eller verifisering av signatur. I andre sammenhenger er det autentiseringsdata og signeringsnøkkel/privat nøkkel («signaturfremstillingsdata») som fellesbehandles f.eks. ved krav til forsvarlig oppbevaring og bruk av nøkler eller PIN-koder/passord.

Signaturverifiseringsdata kan etter omstendighetene refereres til som «sertifikat» i den forstand at sertifikatet representerer den knytting mellom signaturverifiseringsdata og det kjennetegn eller den egenskap ved sertifikatinnehaveren som man er ute etter å få bekreftet. Av og til kan det være fristende å gjøre noen grove forenklinger og snakke om bruk av koder og sertifikater også i situasjoner der det er anvendelse av signeringsnøkkel man tenker på. Det ville imidlertid bygge opp under en del av de misforståelser som eksisterer med hensyn til hva sertifikater er og hvordan de brukes. Inntil videre ser utvalget derfor ikke noen vei utenom de tunge begrepene autentiseringsdata og henholdsvis signaturfremstillingsdata og signaturverifiseringsdata knyttet til den skissen til regelverk som her foreslås.

11.2 Signering og autentisering

11.2.1 Behovet for koordinering og ønsket om fleksibilitet

Det er i alle fall tilsynelatende en iboende motsetning mellom behovet for koordinering og ønsket om fleksibilitet med hensyn til kommunikasjonsform og sikkerhetstjenester for ulike typer henvendelser.

På den ene siden kan det enkelte forvaltningsorgan og den enkelte borger ha et ønske om selv å kunne velge det man mener er en hensiktsmessig og tilfredsstillende sikkerhetstjeneste.

På den andre siden ligger det åpenbart en utfordring i å administrere et stort antall ulike løsninger internt i forvaltningen og for den enkelte i å måtte forholde seg til mange ulike løsninger.

En mulighet er å åpne for at forvaltningsorganene velger ulike løsninger f.eks. digitale signaturer og PenOp[38]men med krav om samvirke på tvers av forvaltningsorganer. Det er antakelig vanskelig å oppnå noe effektivt samvirke mellom så ulike typer løsninger i ulike organer. Derimot er det kanskje mulig å oppnå slike effekter hvis organene anvender ulike implementeringer av digitale signaturer.

En annen mulighet er å redusere antall sikkerhetsnivåer til et minimum og la mest mulig kommunikasjon med forvaltningen gå uten sikkerhetsløsning eller basert på løsninger som leveres med standard nettlesere (f.eks. SSL). Til gjengjeld kan man kreve et høyere sikkerhetsnivå der kravet til

---

37

Det skilles ikke her mellom privat nøkkel benyttet for signering (ikke-benekting i tekniske termer) og autentisering (som kalles «digital signatur» i sertifikatsammenheng når det «signeres» over en hash-verdi for autentiseringsformål uten at man mener å «binde seg» til innholdet i det datagrunnlag hash-verdien er utledet av). Dersom det benyttes ulike nøkler for disse formålene og det er å foretrekke vil det fremgå av nøkkelsertifikatene hvilken funksjon den enkelte nøkkel har.

38

Kryptering av en visuell underskrift på et dokument. htttp://www.penop.com

sikkerhet først slår inn. Man må ikke tape av syne at mye av kommunikasjonen mellom enkeltpersoner og forvaltning er trivielle henvendelser som ikke stiller høye krav til sikkerhet og som det ikke er hensiktsmessig å regulere. Dette bør være tilgjengelig ved elektroniske hjelpemidler også for parter som ikke ønsker å delta i «full elektronisk saksbehandling og kommunikasjon». Man bør med andre ord ikke stille andre krav enn det en hvilken som helst nettilknyttet PC med «state of the art»-programvare kan tilfredsstille – med mindre det er helt nødvendig å stille høyere krav.

Skal det først stilles krav utover «gjennomsnittsmaskinens» standardkonfigurasjon er det mindre betenkelig å heve kravene til et nivå som kan tilfredsstille flere behov. Bruk av digitale signaturer basert på såkalte kvalifiserte sertifikater er åpenbart ett mulig nivå.

I Sverige har Statskontoret gått ut med en anbefaling om tre sikkerhetsnivåer se punkt 6.1. Det forventes ikke at det laveste nivået vil få samordnede løsninger mellom forvaltningsorganer. Og det er antatt at «middels høyt» nivå vil være tilstrekkelig for de fleste anvendelser[39]

11.2.2 Forholdet til elektronisk saksbehandling

Bruken av digitale signaturer kryptering og andre elektroniske sikkerhetstjenester henger nært sammen med elektronisk saksbehandling i sin alminnelighet.

Regler og prosedyrer for mottak og håndtering av henvendelser for journalføring og arkivering for intern saksflyt og meddelelse til den saken gjelder om utfallet av saksbehandlingen vil ha betydning for hvilke sikkerhetstiltak som er tjenlige og nødvendige. For eksempel vil prosedyrer for å sikre at krypteringsnøkler ikke går tapt slik at data blir utilgjengelige kunne være annerledes dersom all dekryptering skjer i sentralt postmottak eller arkiv enn om det skjer hos den enkelte saksbehandler. Beskyttelse av data internt i etatens eget system kan skje med andre midler enn overfor omverdenen fordi det er kjente deltakere og forvaltningsorganet definerer selv «reglene» for tilgang til og bruk av systemet.

Utkastet til nye retningslinjer for elektronisk post i statsforvaltningen kan være ett utgangspunkt for vurdering av sikkerhetstjenester brukt i forbindelse med visse sider ved den elektroniske saksbehandlingen.

Elektronisk post er imidlertid ikke den eneste formen for elektronisk kommunikasjon man kan forvente at forvaltningen vil benytte. Det ser tvert imot ut til at en stor del av saksbehandlingen på sikt vil være lagt opp rundt bruk av web-steder eller liknende løsninger. I mange tilfeller vil det være i form av helt eller delvis automatiserte tjenester. Dette gir andre og bedre muligheter for å styre informasjonsflyten mellom enkeltpersoner og forvaltningen. Forvaltningen kan i større grad kontrollere hvilken informasjon enkeltpersoner har tilgang til på forhånd hvor i mottaksapparatet meldinger dukker opp hvilke meldingsformater som benyttes hvilke kontroller som kreves osv. Det åpner for helt andre muligheter når det gjelder fortløpende kontroll med om nødvendige opplysninger er avgitt og for umiddelbar tilbakemelding til brukeren. Forvaltningsorganet har mindre kontroll med disse forholdene ved bruk av alminnelige e-postsystemer.

Videre kan løsninger som kontrolleres av forvaltningsorganet legge til rette for bruk av sikkerhetstjenester på en annen måte enn e-postløsninger. Særlig løsninger basert på autentisering med PIN-koder eller passord av ulike slag kan etableres i forvaltningsorganets informasjonssystem uten behov for endringer i brukerens lokale nettleser. Det er også mulig å legge opp lenker til veiledninger og relevante kataloger mv. på en måte som gjør det enklere for brukeren enn ved tradisjonell e-post.

Den forutberegneligheten som ligger i en slik struktur vil antakelig gi en stabil ramme for bruk av digitale signaturer o.l. Dette utelukker ikke bruk av e-post der forvaltningsorganet finner at *det* er hensiktsmessig.

39

Jf. Statskontoret *Elektroniska signaturer och elektronisk identifiering för myndigheters e-tjänster* 25. august 2000.

.

11.2.3 Rutiner for og krav til elektronisk kommunikasjon med forvaltningen

Omtalen av de følgende punktene må sees i relasjon til forvaltningslovens alminnelige bestemmelser om informasjonsutvekslingen mellom enkeltpersoner og forvaltning. Utvalgets anbefalinger se punkt 11.6 er ikke ment å skulle gripe inn i forvaltningslovens regulering av den tradisjonelle informasjonsflyten men snarere være et supplement som regulerer de særlige forholdene som gjør seg gjeldende når man benytter elektronisk kommunikasjon.

11.2.3.1 Adressat for henvendelser til forvaltningen

Det vil formodentlig være en fordel for et forvaltningsorgan om alle innkommende henvendelser som gjelder forvaltningsorganet og dets virksomhet blir «sluset gjennom» forhåndsdefinerte kanaler med ansvar for registrering/journalføring og videreformidling av henvendelsen til rette sted i organisasjonen. En eventuell (første) verifisering av signaturer eller kontroll med andre autentiseringsmekanismer og sikkerhetsløsninger som måtte være benyttet kan skje der. En del av funksjonene kan gjennomføres automatisk av behandlende informasjonssystem. Dette gjelder i mindre grad for elektronisk post.

Det bør derfor være mulig for forvaltningsorganet å angi med bindende virkning hvilke adresser eller hjelpemiddel/system som skal benyttes ved henvendelse til forvaltningsorganet i elektronisk form. For å gjennomføre dette bør det også være mulig for forvaltningsorganet å returnere/avvise en henvendelse som ikke er i henhold til anvisningene sammen med opplysning om hva som er korrekt framgangsmåte.

Samtidig bør forvaltningsorganet ha anledning til å åpne for adressering av meldinger direkte til saksbehandler dersom organets interne rutiner er tilrettelagt for dette. Det at den enkelte saksbehandler har en e-postadresse bør imidlertid ikke være tilstrekkelig.

Direkte adressering forutsetter andre interne rutiner bl.a. for saksdeling journalføring og arkivering. Organet bør ha lagt til rette for dette før det åpnes for direkte adressering i saksbehandlingen. Man kan tenke seg at også direkte adressert innkommende post enten går direkte til postmottaket eller «avleverer kopi» til postmottaket på sin vei fra postserver til adressaten. Dette vil imidlertid føre til at også personlig post blir avlagt i postmottaket. Og dersom meldingen gjelder forvaltningsorganets virksomhet men er adressert til feil person vil det kunne påføre postmottaket eller saksfordeler unødig ekstraarbeid ved at man må «tilbakekalle» den direktesendte meddelelsen samtidig som man fordeler meldingen til riktig saksbehandler.

Det er også andre ulemper knyttet til direkte adressering f.eks. oppfølging dersom vedkommende er fraværende har sluttet e.l. Feiladressering kan av flere grunner føre til at ting tar lengre tid eller på andre måter virker uheldig for avsender f.eks. fordi kunnskapen om håndtering av feilsendte meldinger og hvilken informasjon avsender har krav på og behov for kan være mindre hos den enkelte saksbehandler enn hos postmottaket. Direkte adressering bør derfor være forbeholdt tilfeller eller typer av saksbehandling der det enten er særskilt behov for det eller det i alle fall er på det rene at det ikke har spesielle ulemper.

For å unngå usikkerhet bør regelen antakelig være at hvis forvaltningsorganet ønsker å åpne for direkte adressering bør dette gjøres uttrykkelig. For eksempel kan det gjøres ved veiledning på organets web-sider eller gjennom peker fra meldinger som sendes ut fra organet. Dette vil øke forutberegneligheten for brukerne ved innføring av elektronisk kommunikasjon og saksbehandling.

Før det åpnes for adressering direkte til saksbehandler må det være lagt til rette for sikring av meldingers konfidensialitet. Dette forutsetter at man enten åpner for kryptering med saksbehandlers offentlige krypteringsnøkkel eller at det legges til rette for en totrinnsprosess der meldingen formidles kryptert til organets postmottak e.l. og videreformidles direkte derfra under organets interne sikringsrutiner. Valg av løsning kan bl.a. avhenge av hvilken type informasjon det er tale om å overføre.

Det kan være særskilte behov for direkte kommunikasjon mellom ansatte i forvaltningsorganer. Det vil si at informasjonsutveksling mellom ansatte i samme eller ulike organer i første omgang går utenom arkiv eller postmottak slik det skjer f.eks. ved bruk av telefon eller telefaks. Dette kan bl.a. være begrunnet i hensyn til effektivitet eller behov for å kunne kommunisere skriftlig når postmottaket ikke er bemannet. Også disse tilfellene forutsetter at de interne rutinene er lagt til rette bl.a. når det gjelder krav til journalføring. Dersom foreløpig behandling og videresending fra postmottak skjer automatisk når postmottaket ikke er bemannet burde behovet for direkte adressering være begrenset men kan naturligvis være til stede i enkelte tilfeller. Det er heller ikke alle de samme innvendingene som gjør seg gjeldende her som ved henvendelser «utenfra». Blant annet vil kommunikasjon direkte mellom saksbehandlere ofte være

basert på mer sikker kunnskap om hvem som er rette adressat enn når det gjelder f.eks. henvendelser fra privatpersoner. Videre vil enkelte forvaltningsorganer være tilsluttet nett som sikrer meldinger mot innsyn fra utenforstående uten bruk av krypteringsnøkler knyttet til den enkelte mottaker.

Likevel bør man tenke gjennom om det virkelig er grunn til å behandle i alle fall meldinger som vil være «saksdokumenter» i forvaltningslovens forstand ulikt avhengig av om de kommer fra borgerne eller fra et annet forvaltningsorgan. Det enkelte forvaltningsorgan bør ta stilling til om de ønsker én løsning for innkommende meldinger eller om de vil legge til rette for alternativer. I og med at hensynene kan variere i de ulike tilfellene bør det kanskje være adgang til å åpne for direkte adressering bare fra andre forvaltningsorganer.

- Henvendelser i elektronisk form til et forvaltningsorgan skal rettes til den adressen forvaltningsorganet har oppgitt for slike henvendelser.
- Hvis forvaltningsorganet har tilrettelagt for henvendelser eller visse typer av henvendelser via eget nettsted/hjemmeside skal henvendelser i elektronisk form skje på den måten det er tilrettelagt for.

Henvendelse i elektronisk form direkte til saksbehandler av meldinger som angår forvaltningsorganet skal kun skje hvis forvaltningsorganet har lagt til rette for det og uttrykkelig tillatt slik direkte kommunikasjon generelt eller i det enkelte tilfelle[40]

- Forvaltningsorganet kan avvise henvendelser som har en annen form eller er avgitt til annen adresse eller på en annen måte enn foreskrevet eller tilrettelagt for. Forvaltningsorganet skal samtidig opplyse om hva som er korrekt adresse form eller framgangsmåte. Slike opplysninger kan gis i form av henvisning til eller utsending av veiledning om forholdet.
- Forvaltningsorganet kan bestemme at adressering direkte til saksbehandler av meldinger som angår forvaltningsorganet bare kan skje når meldingen sendes fra annet forvaltningsorgan.

11.2.3.2 Henvendelser som utløser veiledningsplikt – formfrie henvendelser

Henvendelser til forvaltningen er mangeartete. Det kan være uforpliktende informasjonsinnsamling forespørsel som utløser veiledningsplikt henvendelse som utløser saksbehandling men som ikke er underlagt spesielle formkrav informasjonsutveksling som etter loven skal skje i bestemte former og utveksling av følsom informasjon av ulike slag. Krav og rutiner må tilpasses dette.

I punkt 11.2.1 anbefaler utvalget at man ikke bør kreve bruk av sikkerhetsløsninger i andre sammenhenger enn der det ansees nødvendig. Det kan imidlertid være vanskelig å gi helt presise beskrivelser på forhånd av når det er behov for f.eks. rimelig sikker identifisering. For å unngå at man for «sikkerhets skyld» krever sikkerhetsløsninger bør det være mulig for forvaltningsorganet å søke tilleggsopplysninger eller kreve bruk av sikkerhetsløsninger i individuelle tilfeller der det er nødvendig.

40

Dette innebærer ingen restriksjoner på forvaltningsorganets adgang til å åpne for elektronisk kommunikasjon direkte til saksbehandler men medfører blant annet at organet først bør ta uttrykkelig stilling til om de interne rutiner er tilfredsstillende jf. drøftelsen ovenfor. En klar angivelse av hvilke kommunikasjonskanaler organet støtter vil også bidra til å øke forutberegneligheten for brukerne ved innføring av elektronisk kommunikasjon og saksbehandling.

.

Det bør også være anledning til å fastsette generelle krav for visse typer av henvendelser f.eks. krav om å benytte digitale signaturer og/eller innholdskryptering.

Hvis forvaltningsorganet stiller slike krav bør det samtidig tilby eller gi anvisning på sikkerhetstjenester som oppfyller de kravene som er stilt. Det kan ikke kreves at den enkelte selv skal finne fram til egnede tjenester. Anvisning kan gis f.eks. ved lenke eller relevant kontaktinformasjon til sertifikatutstedere som forvaltningsorganet aksepterer eller ved at organet selv organiserer og tilbyr eventuelt med tredjemanns hjelp bruk av f.eks. passord og PIN-koder for autentisering mot forvaltningsorganets informasjonstjenester.

- Henvendelser til forvaltningen som ikke er underlagt særskilte formkrav og som ikke utløser saksbehandling kan skje i elektronisk form uten bruk av sikkerhetstjenester.
- Forvaltningsorganet kan i det enkelte tilfelle be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av henvendelsen.

11.2.3.3 Søknader og andre henvendelser som utløser saksbehandling

Adgangen til å kreve «bekreftelse av identitet eller fullmakter» blir antakelig for svakt i en del tilfeller. Det må også være adgang til å kreve mulighet for autentisering ikke-benekting og eventuelt konfidensialitet. Dette kan f.eks. skje ved å kreve bruk av særlige sikkerhetstjenester som digitale signaturer og kryptering.

- Henvendelser som utløser saksbehandling men som ikke er underlagt særskilte formkrav kan skje uten bruk av sikkerhetstjenester.
- Forvaltningsorganet kan i det enkelte tilfelle be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av henvendelsen. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
- Forvaltningsorganet kan fastsette at slike krav skal gjelde generelt for nærmere angitte typer av henvendelser.
- Forvaltningsorganet skal tilby eller gi anvisning på tjenester som gjør det mulig å oppfylle kravet til bekreftelse av identitet eller fullmakter eller øvrige krav forvaltningsorganet har stilt.

11.2.3.4 Henvendelser som er underlagt formkrav

Henvendelser som er underlagt formkrav kan trenge mekanismer for å sikre både dataintegritet og mulighet for å sikre bekreftelser av avsenders identitet eller fullmakter.

- For henvendelser som er underlagt særskilte formkrav kan forvaltningsorganet gi anvisning på hvilke virkemidler som må benyttes for at henvendelse kan skje i elektronisk form herunder krav til virkemidler for sikker bekreftelse av avsenders identitet eller fullmakter. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
- Forvaltningsorganet skal tilby eller gi anvisning på tjenester som gjør det mulig å oppfylle kravet til bekreftelse av identitet eller fullmakter eller øvrige krav forvaltningsorganet har stilt.

11.2.3.5 Henvendelser som ikke tilfredsstiller aktuelle krav

Anbefalinger på dette området er tenkt å omfatte både tilfeller der nødvendig sikkerhetstjeneste ikke er brukt og tilfeller der aktuelt sertifikat e.l. er trukket tilbake eller signaturen av annen grunn ikke kan verifiseres.

Et forvaltningsorgan som mottar henvendelse i elektronisk form som ikke tilfredsstiller de aktuelle kravene til slik henvendelse skal uten ugrunnet opphold gi avsender melding om dette samt gi veiledning om hvilke tiltak som må iverksettes for at henvendelsen skal kunne tas under behandling[41]

- Slik veiledning kan gis ved henvisning til forvaltningsorganets offentliggjorte regler for håndtering av den aktuelle typen henvendelse.
- Forvaltningsorganet skal registrere tidspunkt for når slik melding er sendt og til hvem.
- Dersom feilen er av en slik art at det ikke er mulig å identifisere avsender og varsel ikke kan sendes skal det registreres.
- Forvaltningslovens alminnelige regler om avvisning og oppreisning kommer til anvendelse på de nevnte forholdene.

11.2.3.6 Underretning om vedtak

For å få mest mulig effektivitet ut av den elektroniske saksbehandlingen bør det også være mulig å gi underretning om enkeltvedtak i elektronisk form. Dette må skje på en slik måte at de(n) vedtaket retter seg mot ikke kommer i en situasjon hvor det er større risiko for å lide rettstap f.eks. ved oversitting av klagefrister enn for dagens underretning på papir.

Dette innebærer for det første at man må forsikre seg om at vedkommende er oppmerksom på at underretning vil skje i elektronisk form f.eks. ved å innhente vedkommendes samtykke. For det andre er det viktig å sikre at vedtaket bare gjøres tilgjengelig for rette vedkommende. For det tredje bør man søke å fastlegge et klart skjæringspunkt for når underretning ansees å ha skjedd og klagefrister begynt å løpe.

Fordi vi mangler tradisjon og erfaring med denne formen for underretning er behovet for et klart skjæringspunkt antakelig større enn for papirbasert underretning. Manglende tradisjon og erfaring gjør det nødvendig å opprettholde en reserveløsning. Den innebærer at de som til tross for samtykket til elektronisk underretning av en eller annen grunn ikke får tilgang til vedtaket får dette tilsendt på tradisjonell måte og etter en bestemt tid.

- Underretning om enkeltvedtak kan skje i elektronisk form dersom den vedtaket gjelder/den som har krav på underretning har samtykket i dette.
- Underretning om vedtak skal gjøres tilgjengelig fra dertil egnet informasjonssystem.
- Den vedtaket gjelder skal få melding om at vedtak er fattet og om hvor og hvordan vedkommende kan skaffe seg kunnskap om innholdet samt en frist for når dette senest må skje.

---

41 Dette er tenkt å omfatte både tilfeller der nødvendig sikkerhetstjeneste ikke er brukt og tilfeller der aktuelt sertifikat e.l. er trukket tilbake eller signaturen av annen grunn ikke kan verifiseres.

.

- Vedtakets innhold skal gjøres tilgjengelig for parten når vedkommende bekrefter sin tilknytning til saken overfor informasjonssystemet der vedtaket er lagt ut (autentisering).
- Informasjonssystemet registrerer tidspunktet for når parten har skaffet seg tilgang til vedtaket samt data som bekrefter vedkommendes tilknytning til saken.
- Underretning ansees å ha skjedd på det tidspunktet parten skaffet seg tilgang til vedtaket.
- Dersom parten ikke har skaffet seg tilgang til vedtaket innen 7 dager fra det tidspunkt det ble sendt melding om vedtaket eller vedtaket ble gjort tilgjengelig skal underretning skje i henhold til de reglene som gjelder for underretning om enkeltvedtak på det aktuelle området når det ikke er gitt samtykke til elektronisk kommunikasjon.

11.2.3.7 Klage

Hvis saksbehandlingen ellers foregår i elektronisk form eller det er lagt særskilt til rette for det bør klage over forvaltningens vedtak kunne formidles elektronisk. Det problematiseres ikke her hva som skal til for å oppfylle forvaltningslovens krav om at klage skal undertegnes jf. forvaltningsloven § 32 bokstav b).[42]

- Klage over enkeltvedtak kan sendes i elektronisk form dersom forvaltningsorganet har tilrettelagt for det eller underretning om vedtaket er skjedd i elektronisk form.
- Forvaltningsorganet kan be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er nødvendig for håndtering av klagen. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
- Forvaltningsorganet skal tilby eller gi anvisning på tjenester som gjør det mulig å oppfylle kravet til bekreftelse av identitet eller fullmakter eller de øvrige kravene forvaltningsorganet har stilt.

I forvaltningsloven finnes det regler om hva som skal til for å avbryte en klagefrist. Klage framsatt ved hjelp av «brukerstyrt» elektronisk kommunikasjon som f.eks. vanlig e-post omfattes imidlertid neppe av spesialregelen for klage avgitt til post eller telegrafstasjon. Det bør vurderes om det skal utvikles spesialregler for fristavbrudd ved elektronisk formidling av klage f.eks. når klage leveres over dedikert informasjonstjeneste tilrettelagt av forvaltningsorganet.

Det kan også vurderes en løsning basert på at forvaltningsorganet alltid skal kvittere for mottatt klage. Klager kan i så fall ikke forutsette at klagen er mottatt før han har fått kvittering.

Det er imidlertid ikke uten videre riktig å overføre risikoen for formidlingsfeil eller forsinkelse på klager når forvaltningsorganet har åpnet for elektronisk kommunikasjon i forbindelse med klager.

En mulig løsning kan være å knytte fristavbrudd til det tidspunkt klager initierte sending av den elektroniske meldingen til forvaltningsorganet men med plikt til å følge opp kvittering for mottak og sende

---

42

Se ev. rapport fra Kartleggingsprosjektet om dette. Formålet med retningslinjene her er å gi anvisning på framgangsmåte som kan/skal benyttes dersom loven ellers åpner for elektronisk kommunikasjon. Det forutsettes at de nødvendige lovendringer vurderes i den nåværende fase av Kartleggingsprosjektet/eRegel-prosjektet.

klagen på nytt dersom kvittering ikke er mottatt innen f.eks. 24 timer. Dette vil imidlertid legge nye byrder på klageren med hensyn til oppfølging etter at klage er sendt. Det åpner også for mulighet til å hevde at det ikke foreligger fristoversittelse ved å påberope at klage er sendt like før fristen gikk ut men ikke kommet fram. Med en knapp frist for kontroll av kvittering og eventuell ny klage vil dette likevel neppe få stor betydning fordi fristoversittelsen under en slik regel ikke kan overstige f.eks. de nevnte 24 timer. Innvendingen at klage er sendt men ikke mottatt har man for øvrig heller ingen mulighet for å etterprøve i dag for klager sendt med posten.

Ved fristoversittelse bør alminnelige regler om oppreisning komme til anvendelse.

Et alternativ er at klager alltid leveres over dedikert informasjonstjeneste slik at formidling av klage og kvittering for mottak skjer «i en operasjon». Dette bør antakelig være hovedregelen supplert med bestemmelser om håndtering av klager sendt på annen måte.

- Hvis det skal framsettes klage i elektronisk form og forvaltningsorganet har lagt til rette for klage ved bruk av sitt informasjonssystem skal denne framgangsmåten benyttes.
- Et forvaltningsorgan som mottar klage i elektronisk form skal straks sende kvittering til avsender for mottatt klage.

Klager har plikt til å kontrollere at han mottar kvittering for innsendt klage[43] Dersom slik kvittering ikke er mottatt innen 24 timer skal klager sende klagen på nytt med angivelse av når den ble sendt første gang.

11.2.3.8 Innsyn i opplysninger og dokumenter i elektronisk form

Det bør være adgang til innsyn i elektronisk arkiv. Dette vil kunne innebære en vesentlig styrking av innsynsretten ettersom terskelen for den enkeltes innsyn senkes. Man antar for det første at det er enklere å begjære innsyn direkte fra egen maskin enn via brev eller telefon forutsatt at innsynsarkivet er hensiktsmessig organisert. For det andre slipper vedkommende å vente på brev fra organet eller møte opp personlig. Innsyn via skjerm kan i mange tilfelle oppnås umiddelbart etter at begjæring er sendt[44]

Dersom det begjæres partsinnsyn og dokumentet ikke kan utleveres etter offentlighetsloven er det viktig å sikre at begjæringen kommer fra parten selv og at opplysningene ikke blir gjort tilgjengelige for uvedkommende i forbindelse med utleveringen. Etter personopplysningsloven kan begjæring om innsyn sendes i elektronisk form og den behandlingsansvarlige kan kreve at den registrerte (den opplysningene gjelder og som ber om innsyn) identifiserer seg på en sikker måte f.eks. ved hjelp av en digital signatur[45]

43

I et dedikert system vil kvittering bli sendt umiddelbart slik at ingen ekstra kontroll er nødvendig. Regelen om særskilt kontroll vil først og fremst gjelde alminnelig e-post. Bruk av e-post for klage bør begrenses.

.

44

Se nærmere om dette f.eks. i Statskonsults rapport 1998:13: *Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering.*

.

45

Jf. personopplysningsloven § 24 jf. § 18. I § 24 heter det at den behandlingsansvarlige kan kreve en skriftlig og undertegnet begjæring for å sikre at det er den registrerte og ingen

Innsyn kan som nevnt skje f.eks. ved autentisering direkte mot «innsynsarkiv» (speiling av dokumenter for innsynsformål) eller ved overføring av dokumenter i kryptert form. Dette kan skje ved bruk av en digital signatur i forbindelse med innsynsbegjæring og ved at dokumenter sendes ut i kryptert form eller gjøres tilgjengelige på dedikert informasjonssystem på samme måte som ved underretning om vedtak jf. punkt 11.2.3.6.

- Begjæring om innsyn i dokumenter eller opplysninger i en sak kan sendes forvaltningsorganet i elektronisk form.
- Forvaltningsorganet kan i det enkelte tilfelle be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av henvendelsen. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
- Dersom forvaltningsorganet fører elektronisk arkiv kan innsyn gis i elektronisk form.
- Med mindre innsyn kan kreves etter offentlighetsloven gis innsyn i elektronisk form bare under forutsetning av at det kan gjennomføres tilfredsstillende bekreftelse av vedkommendes tilknytning til saken og sikkerhet for at dokumentene kun gjøres tilgjengelige for denne.

11.2.3.9 Høring og kommentar til høring av forskrifter o.l.

Det vil utvilsomt være hensiktsmessig for forvaltningsorganet om materiale som skal på høring kan legges ut på dertil egnet tjenermaskin i stedet for å bli massedistribuert i form av brevpost.

Det er imidlertid av betydning at berørte personer og instanser får oppfordring til å sette seg inn i det materiale høringen gjelder. Dette kan skje enten ved at vedkommende gjøres aktivt oppmerksom på høringen slik høringsbrevet fungerer i dag eller at det på annen måte gjøres alminnelig kjent hvor høringsmateriale til enhver tid gjøres tilgjengelig slik ordningen er for enkelte typer av kunngjøringer.

Aktiv varsling kan skje ved hjelp av elektronisk post. For at dette skal ha samme effekt som dagens høringsbrev er det en forutsetning at mottaker har tilfredsstillende rutiner for håndtering av e-post. Dette er særlig viktig i forhold til høringer som direkte berører borgernes rettigheter eller plikter.

Man kunne kanskje tenke seg løsninger av liknende type som for underretning om enkeltvedtak (jf. ovenfor) altså at det blir sendt ut et tradisjonelt høringsbrev dersom høringsinstansen ikke skaffer seg tilgang til det aktuelle materialet innen en viss tid. Dette kan imidlertid være mer problematisk enn i underretningstilfellene fordi høringen ikke er basert på direkte forhåndskontakt mellom forvaltningsorganet og parten med innhenting av samtykke til elektronisk kommunikasjon men er en «én til mange»-kommunikasjon initiert av forvaltningen selv.

For høring av forskrifter etter forvaltningsloven er det forvaltningsorganet selv som bestemmer på hvilken måte varsling skal foregå jf. forvaltningsloven § 37. Kravet til sakens opplysning og at de berørte skal gis (reell) anledning til å uttale seg innebærer imidlertid visse minstekrav til den framgangsmåten forvaltningsorganet velger.

Dersom det skal gjennomføres endringer i dagens rutiner for høringer f.eks. i forhold til når det skal varsles individuelt bør det først foretas en grundigere utredning av konsekvensene.

---

annen som får tilgang til opplysningene. I spesialmotivene til bestemmelsen Ot.prp. nr. 92 (1998-1999) s. 122 framgår det imidlertid at begjæring kan skje i elektronisk form forutsatt at den registrerte identifiserer seg på sikker måte f.eks. ved hjelp av digital signatur.

.

Kommentarer til høringsdokument bør kunne formidles i elektronisk form. Skriftlighetskravet i forvaltningsloven § 37 (vedr. forskrifter) er neppe til hinder for dette. Fordi det kan være av betydning hvem som har avgitt høringsuttalelsen og for å utelukke muligheten for at det uriktig avgis uttalelse i andres navn må forvaltningsorganet kunne innhente nødvendige opplysninger for verifisering av avgivers identitet eller fullmakter eller stille krav til sikkerhetsløsninger. Hvor sterkt behovet er vil være avhengig av hva høringen gjelder.

- Høringsbrev til adressater med eget/sentralt e-postmottak kan sendes i elektronisk form. I stedet for fullstendig høringsbrev kan det sendes melding om hvor høringsbrevet er gjort tilgjengelig med oppfordring om å skaffe seg tilgang innen et nærmere angitt tidspunkt. Dersom vedkommende ikke har skaffet seg tilgang til høringsbrevet innen angitt frist bør høringsbrevet sendes i papirbasert form med mindre forvaltningsorganet har bestemt noe annet for den aktuelle høringen.
- Uttalelser til høringen kan avgis i elektronisk form. Slik uttalelse avgis til den e-postadressen forvaltningsorganet har angitt for den aktuelle høringen eller på annen måte som forvaltningsorganet har gitt anvisning på.
- Forvaltningsorganet kan be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av uttalelsen. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
- Forvaltningsorganet skal tilby eller gi anvisning på tjenester som gjør det mulig å oppfylle kravet til bekreftelse av identitet eller fullmakter eller de øvrige kravene forvaltningsorganet har stilt.

11.2.4 Arkiv og langtidslagring

Etter arkivforskriftens § 5-2 kan arkivmateriale avleveres til Det statlige arkivverk (Riksarkivet og statsarkivene) etter 25–30 år. Ved avlevering overtar mottakende institusjon ansvaret for å opprettholde tilgjengeligheten for dokumentene. I henhold til § 5-8 «fastset Riksarkivaren spesifiserte krav til materiale som skal avleverast til Arkivverket». Kravene omfatter bl.a. ordning dokumentasjon merking type og format.

Spørsmål knyttet til arkivformat for elektroniske meldinger utstyrt med elektronisk signatur er til en viss grad beskrevet i Noark-4 [57] (godkjent standard for elektronisk arkivsystem etter arkivloven og forskriftene). Hensynet til lagring over lengre tid av signerte elektroniske meldinger er også grunnlaget for en del av kravene i foreliggende europeisk standard for (utvidede) signaturformater (ETSI ES 201 733). Det foreligger også forslag til standard uten krav til tidsstempling (ETSI TS 101 733) som ble forventet vedtatt i løpet av år 2000.

De nevnte standardene representerer *mulige alternativer* for lagring av signerte dokumenter ikke bindende krav. Man bør derfor vurdere om det bør stilles noen overordnede funksjonelle krav til lagring som blant annet de nevnte standardene vil oppfylle.

Lagring av elektroniske dokumenter over lengre tid[46]innebærer problemer og utfordringer vi ikke kjenner eller som i alle fall er mindre påtrengende enn ved bruk av papir som

---

46

Med oppbevaring over lengre tid menes her oppbevaring utover den tid saken er til behandling ikke nødvendigvis «langtidslagring» i arkivets forstand.

lagringsmedium. I framtiden trenger man å kunne arkivere f.eks. bilder tegninger og lyd sammen med de øvrige dokumentene. Vår definisjon av «dokument» som en avgrenset informasjonsmengde kan bli utfordret av elektroniske dokumenter med hyperlenker til andre elektroniske dokumenter. En annen utfordring er at et dokument kan se annerledes ut når det presenteres via en nyere versjon av tekstbehandlingssystemet enn den det ble skrevet i. Dette kan medføre endringer i (sentral)arkivets funksjon og arkivfunksjonen vil trolig bli enda viktigere enn før. For det første kan det være behov for særskilt utstyr og kompetanse for å bevare elektroniske meldingers integritet over tid. For det andre kan det tenkes at forvaltningens arkiv også må betjene enkeltpersoner i noe større grad enn tilfellet er i dag jf. punkt 11.2.7.7.

Det vil antakelig finnes en del tilfeller eller typer anvendelse av elektronisk kommunikasjon der det bare vil være aktuelt å verifisere meldinger i forholdsvis kort tid etter at den aktuelle transaksjonen eller informasjonsutvekslingen fant sted. I så fall er det antakelig tilstrekkelig å kreve at man har tilgjengelig de verifiseringsdataene som er nødvendige for å verifisere meldingen så lenge den er lagret. Dette bør være et minimumskrav for meldinger som etter arkivloven eller annet regelverk skal arkiveres og kan hensiktsmessig framstå som hovedregelen.

Det er imidlertid flere særskilte problemer knyttet til arkivering og oppbevaring av meldinger med digitale signaturer. For det første har sertifikatene en begrenset gyldighetsperiode (gjerne to til tre år fra det tidspunkt de er utstedt). Etter at sertifikatet er løpt ut kan man ikke lenger basere seg på sertifikatet alene ved verifisering av signaturen. For det andre kan sertifikatet være trukket tilbake etter at signaturen ble verifisert. Dersom det ikke er truffet tiltak som gjør det mulig å tidfeste når signaturen ble påført og når den ble verifisert kan man ikke uten videre bygge på signaturen etter at sertifikatet er trukket tilbake. I tillegg svekkes sikkerheten med tiden. Ved arkivering bør det derfor oppbevares tilstrekkelige opplysninger til at man i ettertid kan sannsynliggjøre at signaturen ble tilfredsstillende verifisert på relevant tidspunkt.

Dette kan f.eks. skje ved at meldingen arkiveres sammen med ulike «tidsstempel» og øvrige relevante opplysninger som definert i ETSI ES 201 733 Electronic Signature Formats (f.eks. komplett kjede av sertifikater og tilbaketrekkingsdata eller referanse til disse). For langtidslagring kan i tillegg et såkalt «arkiv-tidsstempel» påføres.

Alternativt kan arkivfunksjonen innhente nødvendige opplysninger og gjennomføre nødvendige verifiseringer. Deretter arkiveres meldingen sammen med arkivets bekreftelse på at korrekt verifisering fant sted på et bestemt tidspunkt. Tilliten er i dette tilfellet ikke basert på muligheten for å gjenta verifiseringsprosessen med sikkert resultat. Idéen er derimot at tilliten til arkivfunksjonen og arkivets rutiner skal etablere den nødvendige bekreftelse på at knyttingen mellom meldingen og sertifikatet var i orden ved mottak eller at det på annen måte ble gjennomført tilfredsstillende autentisering og at arkivet deretter har sikret meldingens integritet[47] Denne framgangsmåten kan være aktuell blant annet dersom den signerte meldingen blir konvertert til nytt format. Den opprinnelige signaturen kan bare verifiseres i forhold til formatet meldingen hadde da signaturen ble generert.

Melding som er signert med en digital signatur og som blir arkivert [48]skal arkiveres sammen med sertifikat som bekrefter signaturen og øvrige opplysninger som er

---

47

ETSI TS 101 733 Electronic Signature Formats (v 1.2.2 (2000-10)) åpner for en slik modell jf. pkt. 4.2 siste avsnitt siste setning.

.

48

Presiseringen er gjort for å vise at det ikke er meningen å pålegge arkiveringsplikt for meldinger *alene av den grunn* at de er signert med digitale signaturer.

nødvendige for å verifisere signaturen herunder bekreftelse på at sertifikatet ikke var trukket tilbake da verifisering fant sted[49]

For meldinger der sertifikatets gyldighetsperiode er kortere enn tiden det kan ta å bekrefte meldingens innhold og for meldinger som ved arkivering eller i løpet av oppbevaringstiden skal konverteres til annet format skal arkivet ved mottak verifisere signaturen og deretter på hensiktsmessig måte bekrefte knyttingen mellom meldingen meldingens signatur og aktuelt sertifikat sammen med opplysning om tidspunktet for bekreftelsen. Arkivet skal sikre integriteten til meldingene og bekreftelsen av de nevnte forholdene i oppbevaringsperioden.[50] Arkivet kan beslutte at denne framgangsmåten skal benyttes også for andre meldinger (enn de som er nevnt i første setning).

Dersom arkivet ikke lykkes i å verifisere signaturen skal det lagres opplysning om det om mulig sammen med opplysning om årsaken til at verifisering ikke lyktes. [51]

Melding eller resultatet av en automatisert databehandling (f.eks. fra automatisert tjeneste med web-grensesnitt) som er bekreftet med annen autentiseringsteknikk enn digital signatur skal lagres sammen med opplysninger om at korrekt autentisering har funnet sted og om mulig hvilken teknikk som ble benyttet.[52]

49

Bekreftelse på at sertifikatet ikke var trukket tilbake på det tidspunkt verifisering fant sted kan være i form av tidsstemplet bekreftelse fra tilbaketrekkingsliste tidsstemplet bekreftelse fra sertifikat-statustjeneste (OCSP) eller liknende.

.

50

Dette kan som nevnt ovenfor skje enten ved påføring av et «arkiv-tidsstempel» som definert i f.eks. ES 201 733 Electronic Signature Formats eller ved at arkivet på annen måte sikrer meldingens integritet og på tilfredsstillende måte dokumenterer knyttingen mellom meldingen og de forholdene sertifikatet representerer.

51

Selv om det ikke er mulig å verifisere signaturen ved arkivering kan det ikke utelukkes at meldingen er relevant. For det første kan det tenkes at signatur strengt tatt ikke er påkrevet i det aktuelle tilfellet jf. det som er sagt i «Krav til kontroll av sertifikater og tilbaketrekkingslister» under punkt <!fldrslt>11.2.6.10 om hvilken betydning manglende verifisering har for den videre behandlingen av meldingen. For det andre kan man tenke seg at de forholdene meldingen omhandler støttes av andre opplysninger i saken som derved bidrar til å sannsynliggjøre at meldingens integritet er i behold.

52

11.2.5 Signering og verifisering av signatur – bruk av helt eller delvis automatiserte systemer

11.2.5.1 Signering av meldinger som behandles manuelt

Signering av meddelelser med digital signatur bør antakelig følge de samme reglene som til enhver tid gjelder for tilsvarende meddelelse sendt på papir – i hvert fall når det gjelder det innholdsmessige.

Man kunne imidlertid tenke seg en ordning med bruk av digitale signaturer for «forsegling» av meldinger der «seglet» identifiserer etaten som utsteder (kildeautentisering). Et slikt «segl» kan være bærer av funksjoner som likner den tillitbyggende effekten man oppnår ved bruk av forvaltningsorganets trykte brevark og konvolutter. Forsegling ved hjelp av en digital signatur gir også dataintegritet.

Dersom etaten eller virksomheten kan identifiseres gjennom et slikt «segl» «digitalt stempel» eller hva man nå vil kalle det er det antakelig ikke nødvendig at mottaker kan identifisere saksbehandler gjennom signaturen. Hvis det er av betydning at mottaker av meldingen kjenner saksbehandlers identitet kan den framgå av selve meldingen. Slik er situasjonen i dag. De færreste av oss er i stand til å identifisere avsender basert på signaturen. De nødvendige opplysningene finner vi i klartekst andre steder i dokumentet.

Signering som gjøres av saksbehandler og evt. overordnede blir en intern prosess som sikrer innholdet og at etaten innestår eller hefter for dette. Saksbehandlingssystemet bør sikre at meldinger ikke formidles til «forsegling» og utsending før kravene til den interne saksbehandling er ivaretatt. F.eks. kan det sikre at riktig antall personer eller person på rette nivå i organet har godkjent meldingen for utsending eller at de relevante operasjonene for den aktuelle sakstypen er registrert gjennomført mv.

«Seglet» som blir påført ved utsending eller når meddelelsen gjøres tilgjengelig på annen måte bør være en bekreftelse på at de interne prosessene er ivaretatt – og derved det eneste mottaker behøver å forholde seg til.

Framgangsmåten vil innebære en kanalisering av all etatsrelatert informasjonsutveksling via en eller flere «meldingssentraler». Dette vil antakelig legge til rette for effektiv journalføring gjennomføring av innsynsrett mv.

Den sentraliserte oppgaven med forsegling mv. bør være en automatisert funksjon slik at meldingen kan sendes ut eller gjøres tilgjengelig på aktuelt informasjonssystem uavhengig av om arkiv/postmottak er bemannet.

Det må være mulighet for kommunikasjon direkte mellom saksbehandlere i ulike forvaltningsorganer. Dette kan være aktuelt bl.a. i forbindelse med forvaltningsinternt arbeid med budsjetter e.l. som både skal holdes konfidensielt og som må kunne kommuniseres mellom saksbehandlere uavhengig av om arkiv eller postmottak er bemannet.

11.2.5.2 Verifisering av signaturer ved mottak

En sentralisert funksjon kan også være aktuelt når etaten er mottaker. Det vil si at ikke bare mottak og evt. dekryptering men også verifisering av signaturer og sertifikater foregår sentralt – slik at saksbehandler kan forholde seg til meldingens innhold slik det framstår for ham.

Dette *kan* lette både teknologiinnføring opplæring og informasjon i etatene ved at en del oppgaver ivaretas uten at den enkelte saksbehandler behøver å involvere seg.

Dette innebærer antakelig krav til arkivering av aktivitetslogger e.l. Det bør ikke stilles krav om lagring av autentiseringsdata som sådanne. I kode/passord-systemer kan dette innebære en sikkerhetsrisiko. Eventuelle alternativer er lagring av autentiseringsdata i kryptert form eller lagring av engangspassord. Det siste stiller krav til bevaring av samtlige benyttede engangspassord hos forvaltningsorganet og register over når de ble benyttet og er neppe særlig praktisk.

Foreliggende ETSI-standard for signaturformat (ES 201 733) forutsetter at nødvendige opplysninger og behandlingsregler på sikt kan representeres og distribueres i maskinlesbar form som en del av signaturen i form av referanse til en signaturpolicy slik at mottakende system kan behandle henvendelsen automatisk[53] En signaturpolicy er primært tenkt knyttet til spesifiserte typer.

Inntil videre må imidlertid en del av disse spørsmålene løses enten lokalt i det enkelte informasjonssystemet gjennom kryssertifisering og liknende tiltak eller vurderes av den enkelte saksbehandler. Så langt det er mulig bør man unngå å basere seg på manuell behandling hos den enkelte saksbehandler når det gjelder elektroniske signaturer. Med mulig unntak av det å vurdere koplingen mellom sertifikateier og den aktuelle saken som etter omstendighetene kan forutsette konkret kunnskap om saken eller parten bør tiltak knyttet til verifisering av signaturen skje enten automatisk eller sentralt i organet. Det kan ikke og bør ikke kreves eller forventes at den enkelte saksbehandler skal kunne vurdere f.eks. om en gitt sertifikatpolicy eller signaturpolicy er tilfredsstillende for formålet[54]

11.2.5.3 Henvendelser som behandles automatisk

I en del tilfeller vil henvendelser til forvaltningen bli behandlet automatisk. Dette spenner over et bredt register fra å gjøre opplysninger og søknadsskjemaer eller liknende tilgjengelig til behandling av standardiserte meldinger og til den automatiserte avgjørelsesprosessen.

I slike sammenhenger blir personrelaterte sertifikater i det mottakende systemet uten reell betydning. Det gir ikke mening å utstyre et informasjonssystem med sertifikater som peker til en person som har de nødvendige fullmakter til å gjennomføre den aktuelle transaksjonen når behandlingen i sin helhet gjennomføres av informasjonssystemet.

Det hensiktsmessige må være at systemet «signerer» direkte på vegne av etaten for de transaksjonene systemet er «autorisert» for å behandle. Med andre ord når forvaltningsorganet har innrettet seg slik at behandlingen i systemet er avgjørende for resultatet og resultatet formidles i elektronisk form direkte til den det gjelder bør det framgå at meldingen er avgitt av organet som sådant og mottakeren bør kunne innrette seg i forhold til dette. Man bør ikke opprettholde noen fiksjon om at en person med fullmakt står bak avgjørelsen.

Det må finnes rutiner for kvalitetssikring av slike systemer og for godkjenning av dem. Rutinene må blant annet sikre at relevant regelverk er representert i systemet på korrekt måte og at behandlingen kan gjennomføres lovlig uten manuell behandling. Gjennomføring av slik kvalitetssikring og godkjenning må være et absolutt og ufravikelig krav og kan ikke være forhandlingstema ved inngåelse av avtale om utvikling eller levering av slikt informasjonssystem.

Når man mister siste rest av manuell saksbehandling på et område glipper også taket i forestillingen om saksbehandleren som fatter en veloverveid beslutning. Vår forvaltningslov bygger nok på denne forutsetningen.

Det skjer utvilsomt en betydelig grad av automatisering på enkelte forvaltningsområder allerede i dag. Inntil nå har imidlertid dette til en viss grad vært «skjult» bak de rutinene for formidling av informasjon på

53

Jf. f.eks. ETSI ES 201 733 *Electronic Signature Formats* og GlobalSign/ICRI *Signature Policies* 28 August 2000.

.

54

Derimot kan man tenke seg at brukerens lokale system i forbindelse med verifisering av signaturen sjekker den anvendte policyen f.eks. ved å gjøre oppslag mot liste over aksepterte policyer.

.

papir som har funnet sted uavhengig av behandlingsform. Når vi nå er på vei over i stadig mer omfattende elektronisk saksbehandling og elektronisk kommunikasjon blir også dette kjennetegnet ved tradisjonell saksbehandling borte. Det kan derfor være på tide å vurdere om forvaltningsloven uttrykkelig bør åpne for helt automatiserte beslutningsprosesser og samtidig synliggjøre kravene til slike systemer ved å stille opp eller gi hjemmel for utarbeiding av krav til kvalitetssikring og godkjenning.

11.2.5.4 Utstedelse og bruk av sertifikater for informasjonssystemer

Avsnittene over gir bakgrunnen for følgende forslag:

- Informasjonssystemer som benyttes i forbindelse med helt eller delvis automatiserte behandlinger og som i sitt resultat er eller framstår som avgjørelser i forvaltningslovens forstand skal utstyres med sertifikat som identifiserer den etaten som informasjonssystemet behandler meldinger for.

Sertifikatet skal inneholde opplysninger som overfor mottakeren av sertifikatet bekrefter knyttingen mellom en behandling utført av informasjonssystemet og den aktuelle etat.[55]

Mottaker av meldinger knyttet til slike sertifikater kan forholde seg til meldingen som om den var signert av en person i forvaltningen med fullmakt til å avgi eller signere nevnte melding eller avgjørelse med mindre vedkommende visste eller måtte vite at meldingen eller avgjørelsen var blitt til ved en feil.[56]

- Søknad om utstedelse av sertifikat som knytter signaturverifiseringsdata (offentlig nøkkel) til et informasjonssystem og en offentlig etat og som skal brukes ved

---

55

Dette kan f.eks. skje ved at sertifikatet inneholder opplysninger som ved visning på skjerm hos mottaker ved bruk av vanlig programvare framstår som etatens alminnelig kjente navn. Dersom etaten benytter flere informasjonssystemer bør hvert enkelt system utstyres med egne sett med nøkler og sertifikat.

56

Det er ikke meningen at dette skal gripe inn i den adgang som ellers finnes til å sette til side eller omgjøre vedtak som er beheftet med feil – kun det forhold at vedtaket ikke er fattet av rette person innenfor det aktuelle organ. I prinsippet kan man også tenke seg sertifikater til forvaltningsansatte som ikke inneholder den ansattes navn men derimot navnet på forvaltningsorganet sammen med et ansattnummer eller annen identifikator som gjør det mulig for organet å identifisere saksbehandleren. Med mindre saksbehandlers navn framgår av meldingen ellers vil saksbehandler være anonym i forhold til mottakeren. Man kan da tenke seg at den samme rettslige virkning inntrådte som ved meldinger «forseglet» av organets informasjonssystem. Det er imidlertid ikke her noen automatisert behandling eller andre forhold som begrunner en særlig flytting av risiko for feil over på forvaltningsorganet. Det synes derfor ikke å være grunn til å behandle bruken av eventuelle «anonyme ansattsertifikater» på annen måte enn der saksbehandler underskriver med fullt navn.

behandlinger som kan resultere i avgjørelser etter forvaltningsloven skal godkjennes av den som er bemyndiget til å tildele fullmakter på etatens vegne.

11.2.5.5 Sårbarhetsbetraktninger – sikring av nøkler for informasjonssystemer

De av forvaltningens systemer som måtte bli utstyrt med egne sertifikater for signering/forsegling må stort sett antas å være virksomhetskritiske systemer. Stans i eller et «angrep» på et slikt system vil kunne lamme virksomheten i en periode.

Hvis nøkkelsertifikatet til et slikt system trekkes tilbake vil systemet i praksis bli satt ut av drift fordi det ikke lenger er mulig å verifisere meldinger fra systemet. For enkeltpersoner vil det neppe være et uoverstigelig problem å vente en dag eller to på nye nøkler og sertifikat dersom signeringsnøkkelen skulle bli kompromittert. For en større virksomhet som et forvaltningsorgan kan selv noen timers stans være kritisk. Med mindre generering av nye nøkler og utstedelse av nytt sertifikat kan skje meget raskt bør det derfor etableres rutiner for at slike informasjonssystemer utstyres med minst ett ekstra sett med signeringsnøkler som raskt kan tas i bruk dersom et sertifikat blir trukket tilbake eller en signeringsnøkkel går tapt f.eks. som følge av teknisk svikt.

Konsekvensene av stans i systemet utgjør også en særlig utfordring i forhold til sårbarheten som ligger i muligheten for kompromittering av den nøkkelen sertifikatutsteder benytter for signering av sertifikater. Dersom denne nøkkelen kompromitteres rykkes grunnlaget for tilliten bort for alle sertifikater utstedt av denne sertifikatutstederen med den aktuelle nøkkelen.

I sistnevnte tilfelle vil det ikke hjelpe å ha flere nøkler fra samme utsteder ettersom alle vil være utsatt for samme tillitssvikt. Det bør derfor vurderes om ikke informasjonssystemer for forvaltningsorganet skal utstyres med nøkler (signaturgenereringsdata) fra minst to uavhengige sertifikatutstedere.

Signeringsnøkler som benyttes i automatiserte systemer må være installert slik at de kan benyttes direkte av systemet uten noen menneskelig mellomkomst. Dette stiller krav til sikring av informasjonssystemet for å unngå misbruk av og angrep på de aktuelle nøklene. Ettersom sikringstiltakene ikke kan bygges rundt enkeltpersoners godkjenning av hver enkelt «signeringshandling» jf. det som er sagt om forvaltningsansattes bruk i note 27 nedenfor må tiltakene i stedet være knyttet til fysisk og logisk sikring av informasjonssystemet og det miljøet det opererer i.

- For et informasjonssystem som er utstyrt med sertifikat for forvaltningsorganet skal det være lagt opp rutiner som sikrer at systemet raskt kan settes i drift med nye signaturgenereringsdata og nytt sertifikat dersom det sertifikatet som er i bruk blir trukket tilbake eller signaturgenereringsdata går tapt.
- Det bør vurderes om informasjonssystemet skal være utstyrt med signaturgenereringsdata og sertifikat fra mer enn én sertifikatutsteder.
- Signaturgenereringsdata skal være sikret mot misbruk etter anerkjente prinsipper for informasjonssystemers sikkerhet.

11.2.6 Forvaltningsansattes bruk av elektronisk signatur

11.2.6.1 Anskaffelse av nøkler koder og sertifikat

For å kunne iverksette elektronisk saksbehandling i større skala må arbeidsgiver kunne pålegge den forvaltningsansatte å ta i bruk de sikkerhetstjenester som forvaltningsorganet har valgt å benytte i sin saksbehandling. På hvilken måte tildeling av nøkler koder og sertifikater skal skje og hvor den enkelte må henvende seg for registrering e.l. vil være avhengig av hvilke(n) tjeneste(r) som er valgt. Arbeidsgiver må derfor gi den forvaltningsansatte anvisning om hvorledes vedkommende skal forholde seg.

Av koordineringshensyn og for å sikre best mulig effektivitet i de interne kommunikasjonsprosessene i forvaltningen bør sertifikater som skal benyttes av forvaltningsansatte under tjeneste for arbeidsgiver kun utstedes av sertifikatutstedere som forvaltningsorganet eller koordinerende organ for forvaltningen har

utpekt/godkjent og eventuelt inngått rammeavtale med[57] Dette gjør det mulig bl.a. å sikre interoperabilitet og tilgang til nødvendige sertifikatkataloger at alle forvaltningsansatte har tilgang til de sertifikatene[58]som er nødvendige for å verifisere andre tjenestemenns sertifikater og kontroll med at tjenestene holder et tilfredsstillende sikkerhetsnivå. Dersom det er nødvendig av koordineringshensyn eller fordi det enkelte forvaltningsorgan mangler kompetanse på området kan det være hensiktsmessig å begrense valgmulighetene til sertifikatutstedere man har inngått rammeavtale med. Det forutsettes at ordningen med rammeavtaler innrettes i henhold til reglene for offentlige anskaffelser.

- Et forvaltningsorgan kan gi sine ansatte anvisning om hvilke sikkerhetstjenester de skal benytte under tjeneste for organet og hvor de skal henvende seg eller gå fram for å anskaffe nødvendige nøkler koder sertifikater mv.
- Forvaltningsansatte skal under tjeneste for arbeidsgiver kun benytte sertifikater utstedt av sertifikatutsteder som er godkjent av arbeidsgiver eller av et forvaltningsorgan som har koordineringsansvar for forvaltningens virksomhet.
- Koordinerende forvaltningsorganer kan bestemme at det under tjeneste for forvaltningsorganer kun skal benyttes sertifikater fra sertifikatutsteder som har inngått rammeavtale om levering av slike tjenester til forvaltningen.
- Dersom rammeavtalen løper ut og ikke blir fornyet i løpet av sertifikatets gyldighetsperiode skal sertifikatet likevel kunne benyttes i resten av gyldighetsperioden med mindre sertifikatutsteders sertifikat blir trukket tilbake eller nødvendige katalogtjenester mv. ikke lenger er tilgjengelige.

Koordinerende forvaltningsorganer kan bestemme at slikt sertifikat likevel ikke skal benyttes etter at rammeavtalen er løpt ut.[59]

11.2.6.2 Hva må dokumenteres ved anskaffelse av sertifikat?

Hvilke forhold som skal dokumenteres ved anskaffelse av nøkler koder eller sertifikat mv. vil avhenge av hvilken sikkerhetsløsning som er valgt. For et ansattsertifikat vil det normalt være tilstrekkelig å få dokumentert brukers identitet og ansettelsesforhold. For andre typer av sertifikater kan det i tillegg være nødvendig med opplysning om vedkommendes fullmakter profesjonstilknytting e.l.

57

Det bør søkes en løsning som gjør det mulig å koordinere både statlig og kommunal forvaltning.

.

58

De aktuelle sertifikatutstederes sertifikater.

59

Dersom det ikke er sikret mulighet for full støtte til sertifikater fram til de løper ut må det være adgang til å pålegge å avbryte bruken i gyldighetsperioden.

Prosedyrer og krav til dokumentasjon i forbindelse med anskaffelse av sertifikat vil framgå av den sertifikat- eller signaturpolicy forvaltningsorganet har valgt og som det skal utstedes sertifikat i henhold til.

11.2.6.3 Innsamling av opplysninger og samtykke til utlevering av sertifikat mv.

I henhold til forslaget til lov om elektronisk signatur [52] kan opplysninger som skal benyttes i sertifikater bare innhentes direkte fra den opplysningen gjelder eller med dennes uttrykkelige samtykke jf. § 7.

Videre kan sertifikatutsteder ikke utlevere sertifikat til andre uten sertifikateiers samtykke jf. (forutsetningsvis) lov om elektronisk signatur § 14 annet ledd bokstav b). Dersom det skal være åpning for at forvaltningsansatte selv signerer utgående meddelelser må det innhentes samtykke til utlevering av sertifikat.

Det er neppe praktisk eller holdbart at mottaker av en melding signert av en forvaltningsansatt i tjeneste ikke skal få tilgang til det aktuelle sertifikatet. Dersom slikt samtykke ikke blir gitt bør konsekvensen være at den ansatte ikke kan drive utadrettet saksbehandling i elektronisk form.

I normaltilfellene vil relevant sertifikat være vedlagt meldingen slik at utlevering fra sertifikatutsteder ikke er nødvendig. Man bør imidlertid ikke utelukke muligheten for å hente sertifikat direkte fra utsteder (eller eventuelt forvaltningsorganets hjemmeside) og følgelig bør samtykke innhentes rutinemessig. Sertifikat som skal benyttes i forbindelse med kryptering (ved hjelp av mottakers offentlige nøkkel) må hentes hos sertifikatutsteder hvis ikke avsender er kjent med sertifikatet fra før. Slikt sertifikat omfattes imidlertid ikke av lov om elektronisk signatur.

- Innsamling av opplysninger som skal benyttes i sertifikat skal skje direkte fra den opplysningen gjelder eller med dennes uttrykkelige samtykke jf. lov om elektronisk signatur § 7 [52].
- I forbindelse med søknad fra forvaltningsansatt om sertifikat til bruk i tjenesten skal sertifikatutsteder be om den ansattes samtykke til utlevering av sertifikatet til andre jf. (forutsetningsvis) lov om elektronisk signatur § 14 annet ledd bokstav b).

Man bør samtidig søke samtykke til utlevering av opplysninger om den ansattes arbeidsområde eller fullmakter i tjenesten når disse opplysningene er lagret i tilknyttet katalog og ikke direkte i det aktuelle sertifikatet forutsatt at opplysningene kan forventes å ha betydning for anvendelsen av sertifikatet. Slike opplysninger skal kun utleveres i forbindelse med verifisering av det aktuelle sertifikatet.[60]

11.2.6.4 Veiledning av den ansatte

Fordi bruken av elektroniske signaturer mv. er lite kjent er det viktig at det gis tilstrekkelig og hensiktsmessig informasjon til brukeren før teknikkene tas i bruk.

Ved anskaffelse av nøkler koder og sertifikat skal den ansatte få opplysning/veiledning om:

- Ansvar og plikter i forbindelse med oppbevaring og bruk av nøkler koder og sertifikat mv.

60

Ideen er at det ikke skal være mulig å «surfe» på katalogen for å kartlegge de enkeltes fullmakter men kun å få verifisert om vedkommende har de nødvendige rettigheter eller er tilknyttet relevant område for anvendelsen av sertifikatet.

Aktuell sertifikatpolicy og -praksis (i form av en tilpasset brukerversjon) [61]

- Egen og andres mulighet til å sperre eller suspendere sertifikatet
- Utløp av sertifikatet
- Sertifikatutsteders oppbevaring av personopplysninger oppbevaringsperioden og hvem sertifikatet kan utleveres til mv. jf. personopplysningsloven § 19
- Sertifikatutsteders ansvar og plikter
- Registreringsenhetens ansvar og plikter
- Restriksjoner på bruk av sertifikatet.

11.2.6.5 Påbud om bruk av nøkler koder og sertifikat

Det bør vurderes om forvaltningsorganet og forvaltningsansatte skal ha plikt til å benytte digitale signaturer eller liknende i enkelte sammenhenger.

Når forvaltningsorganet skal utarbeide kriterier for når saksbehandler skal benytte digitale signaturer e.l. bør kriteriene så langt som mulig knyttes til vurderinger som saksbehandler skal gjøre uansett f.eks. vurdering av om den aktuelle meldingen skal arkiveres etter arkivloven er omfattet av økonomireglementet eller om det dreier seg om et *vedtak* i forvaltningslovens forstand. Dette kan gjelde både vedtak om materielle spørsmål og prosessuelle avgjørelser f.eks. om å avvise en klage eller avvisning av en henvendelse som ellers vil innebære at en sak blir initiert. Man bør så langt det er mulig unngå å innføre nye vurderingstemaer for den enkelte saksbehandler.

Dersom man velger å benytte løsning med sentral «forsegling» av meldinger og underretning om vedtak over dedikert informasjonssystem vil behovet for å pålegge den enkelte saksbehandler plikter med hensyn til signering bli vesentlig mindre.

11.2.6.6 Annen bruk av nøkler koder og sertifikat

Utenom de tilfellene der det er plikt til å benytte digitale signaturer eller sende meldingen via meldingssentral bør saksbehandler selv kunne velge å benytte digitale signaturer under utøving av tjenesten der vedkommende finner det hensiktsmessig eller hvis mottaker krever det.

11.2.6.7 Restriksjoner på bruk av nøkler koder og sertifikat

For å unngå sammenblanding av roller har utvalget funnet det mest hensiktsmessig at personlig sertifikat (ansattsertifikat) som inneholder peker til et forvaltningsorgan som arbeidsgiver ikke skal benyttes for andre formål enn i tjeneste for arbeidsgiver. For private formål må den enkelte anskaffe personsertifikat.

- Autentiseringsdata eller sertifikat (f.eks. ansattsertifikat) som inneholder peker til et forvaltningsorgan som arbeidsgiver skal kun benyttes i tjeneste for arbeidsgiver.
- Personlige (private) sertifikater skal ikke benyttes i tjeneste for arbeidsgiver.

61

Det er viktig at denne informasjonen gis i en form som brukeren kan forstå. Det kan ikke forventes at den enkelte skal kunne forholde seg direkte til den aktuelle sertifikatpolicy og sertifiseringspraksis. Se f.eks. *Model PKI Disclosure Statement*(PDS) i ETSI TS 101 456 *Policy Requirements for Certification Authorities Issuing Qualified Certificates Annex B.*

11.2.6.8 Krav til forsvarlig bruk og oppbevaring av nøkler/nøkkelbærende medium

Uansett hvilken løsning som velges for den enkelte anvendelse må det stilles krav til den enkeltes omgang med og bruk av signaturframstillingsdata (signeringsnøkler) eller autentiseringsdata (passord/PIN-koder). Dette er en forutsetning for at man kan ha tillit til løsningen.

Dette innebærer for det første å sikre at andre ikke får tilgang til koder og nøkler for det andre at koder og nøkler bare benyttes til det formålet de er utstedt for. For det tredje må eier aldri forlate datamaskinen usikret i en slik status at andre kan fortsette en aktiv sesjon eller sende meldinger på andres vegne.

I tillegg er det behov for å sikre at signaturframstillingsdata og de dataene som skal signeres ikke «angripes» eller «misbrukes» av det informasjonssystemet de benyttes i f.eks. som følge av virus e.l. Dette stiller krav til signaturframstillingssystemet brukerens øvrige systemkonfigurasjon det omkringliggende miljøet («brannmurer» o.l.) og PC-er som sådanne. Slike krav må i første omgang ivaretas av den enhet som står for anskaffelse og drift av informasjonssystemene i virksomheten jf. punkt 11.4. I neste omgang må det stilles krav til brukeren om ikke å foreta handlinger som kan true sikkerheten i systemet som ukritisk nedlasting eller installering av ikke godkjent programvare e.l. I praksis må dette antakelig løses ved at arbeidsgiver gir instrukser om bruk av virksomhetens informasjonssystem.

- Eieren av signaturframstillingsdata skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre.
- Signaturframstillingsdata skal kun benyttes til de formålene de er utstedt for.

Eieren skal aldri forlate arbeidsstasjon terminal eller annen enhet som benyttes for autentisering eller signaturgenerering uten å sikre at signaturframstillingsdata ikke lenger er tilgjengelige på/i enheten at den aktuelle sesjon er avsluttet eller at enheten på annen måte er sikret mot uvedkommendes misbruk.[62]

- Eieren av signaturframstillingsdata skal ikke overlate disse til andre eller gi andre tilgang til dem heller ikke når andre skal handle på hans vegne. Dersom noen skal handle på vegne av en annen (etter fullmakt) skal dette skje med fullmektigens egne signaturframstillingsdata under henvisning til at meldingen er avgitt på vegne av en annen. (Den man opptrer på vegne av kan utstede rollesertifikat til sin fullmektig (når dette blir tilgjengelig).)
- Bestemmelsene om signaturframstillingsdata gjelder tilsvarende for bruk av autentiseringsdata (passord/PIN-koder).
- Den ansatte skal ellers følge instruksene arbeidsgiver har fastsatt om bruk og sikring av virksomhetens informasjonssystem herunder om kontroll med materiale som skal lastes ned eller installeres i informasjonssystemet.

11.2.6.9 Varslingsplikter ved tap av nøkler mistanke om misbruk mv.

Et ledd i forsvarlig bruk av koder passord nøkler og nøkkelbærende medier er omgående varsling dersom det oppstår mistanke om at nøkler er tapt kommet på avveie eller på annen måte blir eller kan bli misbrukt.

62

En del problemer løses dersom passord for tilgang til signeringsnøkler må oppgis hver gang signeringsnøkkelen skal benyttes slik det er foreslått i Sverige. Men med mindre signering foregår i aktive kort e.l. vil dette antakelig være avhengig av den enkeltes lokale konfigurasjon.

- Eieren av signaturframstillingsdata eller autentiseringsdata skal straks varsle sertifikatutsteder eller den som ellers er utpekt til å motta varsel dersom det oppstår mistanke om at signaturframstillingsdata eller autentiseringsdata er tapt kommet på avveie eller på annen måte blir eller kan bli misbrukt.

11.2.6.10 Krav til kontroll av sertifikater og tilbaketrekkingslister

Ved mottak av melding utstyrt med signatur må det blant annet kontrolleres om signaturen kan verifiseres om de relevante sertifikater fortsatt er gyldige og tilfredsstillende for den aktuelle anvendelsen om sertifikatet tilhører rett person mv. Hvilke kontroller som skal gjennomføres og hvilken tilleggsinformasjon som skal innhentes vil avhenge av hvilken tjeneste som benyttes og hvor kritisk den enkelte anvendelse er. Kravene kan defineres gjennom en signaturpolicy[63]

Spørsmålet om i hvilken grad saksbehandler skal gjennomføre de aktuelle kontrollene er avhengig av hvilke tjenester som finnes sentralt i organet og hvilke funksjoner som løses automatisk i den enkeltes lokale arbeidsstasjon jf. om verifisering av signaturer ved mottak under punkt 11.2.5. Dette er imidlertid oppgaver som i størst mulig grad bør løses automatisk. Hvis verifisering derimot ikke lykkes og dette innebærer at videre behandling av meldingen ikke kan skje må saksbehandler initiere melding til avsender i henhold til reglene om meldinger som ikke tilfredsstiller kravene under punkt 11.3.5.[64]

- Dersom melding som er utstyrt med elektronisk signatur ikke kan verifiseres i henhold til reglene som gjelder for den aktuelle meldingstypen og dette har betydning for behandling av meldingen i forvaltningsorganet skal det sendes melding til avsender i henhold til reglene under punkt 11.2.3.

11.2.6.11 Krav til/anbefaling om lokal oppbevaring av sertifikater mv.

Opplysninger som er nødvendige for å verifisere en signatur bør oppbevares sammen med meldingen eller gjennom vedlikehold av lokal sertifikatdatabase og sperreliste mv. og med referanse til den enkelte melding. Slike opplysninger kan i tillegg til de relevante sertifikatene f.eks. være bekreftelse på kontroll av tilbaketrekkingsliste e.l. Slike opplysninger bør i størst mulig grad oppbevares av arkivet eventuelt erstattes med arkivets bekreftelse på de forhold som er verifisert jf. det som er sagt om arkiv og langtidslagring i punkt 11.2.4. Dersom meldingen i en periode oppbevares annet sted enn i sentralt arkiv må organet eller saksbehandlers lokale system ivareta denne oppgaven.

- Kopi av relevant(e) sertifikat(er) og øvrige opplysninger som er nødvendig for verifisering av signaturer over tid bør oppbevares av arkivet.
- Dersom meldingen i en periode lagres lokalt hos brukeren uten å være oversendt arkivet bør opplysningene lagres lokalt sammen med meldingen.

63

Jf. f.eks. ETSI ES 201 733 Electronic Signature Formats og GlobalSign/ICRI *Signature Policies* 28 August 2000.

.

64

Det er ikke sikkert at manglende verifisering bestandig vil ha betydning for behandling av meldingen. Det kan f.eks. tenkes at meldingen gjelder begjæring om innsyn i dokument som kan utleveres etter offentlighetsloven eller anmodning om å få tilsendt søknadsskjema eller andre forhold der vedkommendes identitet mv. er uten betydning.

11.2.7 Privatpersoners bruk av elektronisk signatur

Forvaltningen har en åpenbar interesse i og behov for å ha klare regler for håndtering av elektroniske meldinger som mottas av behandles i og sendes fra forvaltningsorganer. Derimot bør det antakelig vises tilbakeholdenhet med å pålegge borgerne plikter med hensyn til hvorledes de skal håndtere meldinger i sitt eget informasjonssystem. Med unntak av de tiltak som har betydning for forvaltningens kommunikasjon med den enkelte bør nok retningslinjene som er rettet mot borgerne snarere ha form av veiledende retningslinjer enn av bindende regler.

Meldingsbehandlingen hos forvaltning og borger vil ha en del fellestrekk og det vil langt på vei være de samme spørsmålene som skal behandles. Løsningene kan imidlertid variere blant annet fordi den enkelte normalt ikke har tilgang til noen meldingssentral som verifiserer signaturer eller arkivfunksjon som kan vareta langtidslagring av elektroniske meldinger på en tilfredsstillende måte. Det er mulig at enkeltpersoner bør kunne basere seg på forvaltningens arkiv for langtidslagring av meldinger som er utvekslet med et forvaltningsorgan.

11.2.7.1 Valg av sikkerhetstjeneste

Det bør i utgangspunktet ikke være begrensninger i borgernes adgang til fritt å velge hvilken sertifikattjenestetilbyder de vil benytte så lenge tjenesten tilfredsstiller de krav forvaltningsorganet stiller. Det kan imidlertid være hensiktsmessig for den som ikke allerede har anskaffet nøkler og sertifikat mv. å benytte en sertifikatutsteder som er utpekt eller drives av det aktuelle forvaltningsorgan eller koordinerende organ for forvaltningen. Brukeren behøver da ikke gjøre noen selvstendig vurdering av om tjenesten holder tilfredsstillende nivå men kan basere seg på de vurderinger som allerede er gjort av forvaltningen.

Frihet med hensyn til valg av sertifikatutsteder gjør det problematisk å angi hvor/til hvem den enkelte i egenskap av privatperson skal henvende seg for å søke om sertifikat. Dersom forvaltningsorganet har gitt anvisning på tilfredsstillende tjenester jf. ovenfor vil det normalt opplyses der hvor og hvorledes man skal gå fram hvis man velger blant de anviste tjenestene.

- For elektronisk kommunikasjon med forvaltningen må den enkelte benytte tjenester som oppfyller de kravene som stilles.
- Dersom det benyttes kvalifiserte signaturer kan den enkelte selv velge hvilken leverandør av kvalifiserte sertifikater vedkommende vil benytte.
- Forvaltningen kan stille tilleggskrav innenfor rammen av lov om elektronisk signatur § 5.

11.2.7.2 Veiledning av bruker

Fordi bruk av elektroniske signaturer mv. er ukjent for de fleste brukere i dag er det viktig at det gis tilstrekkelig og hensiktsmessig informasjon til brukeren før teknikkene tas i bruk.

Ved anskaffelse av nøkler koder og sertifikat skal brukeren få opplysning/veiledning om:

- Ansvar og plikter i forbindelse med oppbevaring og bruk av nøkler koder og sertifikat mv.

Aktuell sertifikatpolicy og -praksis (i form av en tilpasset brukerversjon) [65]

65

Det er viktig at denne informasjonen gis i en form som brukeren kan forstå. Det kan ikke forventes at den enkelte skal kunne forholde seg direkte til den aktuelle sertifikatpolicyen og sertifiseringspraksisen. Se f.eks. *Model PKI Disclosure Statement* (PDS) i ETSI TS 101 456 *Policy Requirements for Certification Authorities Issuing Qualified Certificates* Annex B.

- Egen og andres mulighet for å sperre eller suspendere sertifikat
- Utløp av sertifikatet
- Sertifikatutsteders oppbevaring av personopplysninger oppbevaringsperioden og hvem sertifikatet kan utleveres til mv. jf. personopplysningsloven § 19
- Sertifikatutsteders ansvar og plikter
- Registreringsenhetens ansvar og plikter
- Restriksjoner på bruk av sertifikatet.

11.2.7.3 Restriksjoner på bruk av nøkler koder og sertifikat

Det er grunn til å anta at forvaltningen vil akseptere og benytte en del av de sertifikattjenestene som tilbys i markedet ellers. Disse tjenestene kan ha generell anvendelse eller være anbefalt brukt for et eller flere angitte områder av sertifikatutsteder. Det er neppe grunn til å gripe inn i dette.

Hvis det derimot skulle være aktuelt å utstede sertifikater eller andre autentiseringsdata utelukkende for bruk ved kommunikasjon med forvaltningen bør det finnes hjemmel til å pålegge brukeren å respektere dette. For å unngå tvil bør slike begrensninger framgå av sertifikatet og brukeren må gjøres særlig oppmerksom på begrensningene.

- Signaturframstillingsdata eller autentiseringsdata som er tildelt den enkelte spesielt for kommunikasjon med forvaltningen skal ikke benyttes til andre formål.
- Slike begrensninger skal framgå av sertifikatet og brukeren skal opplyses om begrensningene jf. om veiledning ovenfor.

11.2.7.4 Krav til forsvarlig bruk og oppbevaring av nøkler/nøkkelbærende medium

Uansett hvilken løsning som velges for den enkelte anvendelse må det stilles krav til den enkeltes omgang med og bruk av signaturframstillingsdata (signeringsnøkler) eller autentiseringsdata (passord/PIN-koder). Dette er en forutsetning for å kunne ha tillit til løsningen. Dette innebærer for det første å sikre at andre ikke får tilgang til koder og nøkler for det andre at koder og nøkler bare benyttes til det formålet de er utstedt for. Dette bør gjelde generelt for all bruk av sikkerhetstjenester.

For forvaltningsansatte er det i tillegg et krav at eier aldri forlater datamaskinen usikret i en slik status at andre kan fortsette en aktiv sesjon eller sende meldinger på andres vegne. Det er tvilsomt om man kan eller bør pålegge privatpersoner den siste typen restriksjoner med mindre nøkler koder eller sertifikat er utstedt særskilt for bruk mot forvaltningen. Det bør derimot gis en klar oppfordring om å følge samme regel.

Også for enkeltpersoner vil det være behov for å sikre at signaturframstillingsdata og data som skal signeres ikke «angripes» eller «misbrukes» av det informasjonssystemet de benyttes i f.eks. som følge av virus e.l. Dette stiller krav til signaturframstillingssystemet brukerens øvrige systemkonfigurasjon og det omkringliggende miljøet («brannmurer» o.l.). Privatpersoner vil normalt måtte støtte seg på sin systemleverandør når det gjelder disse forholdene. I neste omgang blir det opp til brukeren ikke å foreta handlinger som kan true sikkerheten i systemet som ukritisk nedlasting eller installering av ikke godkjent programvare. Selv om manglende oppfølging fra brukernes side kan føre med seg feil og misbruk og i neste omgang et generelt press mot tilliten til signatursystemet bør man nok være forsiktig med å legge restriksjoner på den enkeltes adgang til å anskaffe og å gjøre endringer i eget system. Derimot bør det gis anbefalinger gjerne fra sertifikatutsteder om hvorledes den enkelte bør forholde seg. For anvendelser der behovet for sikkerhet er høyt får man heller gå veien om å kreve bruk av såkalte «sikre signaturgenereringssystemer» jf. lov om elektronisk signatur kap. II eller stille andre særskilte krav til brukerens informasjonssystem.

- Eieren av signaturframstillingsdata skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre.
- Signaturframstillingsdata skal kun benyttes til de formålene de er utstedt for.

Eieren av signaturframstillingsdata bør aldri forlate arbeidsstasjon terminal eller annen enhet som benyttes for autentisering eller signaturgenerering uten å sikre at signaturframstillingsdata ikke lenger er tilgjengelige på/i enheten at den aktuelle sesjon er avsluttet eller enheten på annen måte er sikret mot misbruk[66]

- Eieren av signaturframstillingsdata skal ikke overlate disse til andre eller gi andre tilgang til dem heller ikke når andre skal handle på hans vegne. Dersom noen skal handle på vegne av en annen (etter fullmakt) skal dette skje med fullmektigens egne signaturframstillingsdata under henvisning til at meldingen er avgitt på vegne av en annen. (Den man opptrer på vegne av kan utstede rollesertifikat til sin fullmektig (når dette blir tilgjengelig).)
- Bestemmelsene om signaturframstillingsdata gjelder tilsvarende for bruk av autentiseringsdata (passord/PIN-koder).
- Eieren av signaturframstillingsdata bør kun benytte disse i informasjonssystemer som vedkommende har tillit til og følge de anbefalinger som gis av sertifikatutsteder om innretting og bruk av systemet. Man bør vise varsomhet ved endringer i systemet og man bør kontrollere materiale som skal lastes ned eller installeres i informasjonssystemet.

11.2.7.5 Varslingsplikter ved tap av nøkler mistanke om misbruk mv.

Et ledd i forsvarlig bruk av koder passord nøkler og nøkkelbærende medier er omgående varsling dersom det oppstår mistanke om at nøkler er tapt kommet på avveie eller på annen måte blir eller kan bli misbrukt. Dette gjelder uavhengig av hvem eieren er.

- Eieren av signaturframstillingsdata eller autentiseringsdata skal straks varsle sertifikatutsteder eller den som ellers er utpekt til å motta varsel dersom det oppstår mistanke om at signaturframstillingsdata eller autentiseringsdata er tapt kommet på avveie eller på annen måte blir eller kan bli misbrukt.

11.2.7.6 Krav til kontroll av sertifikater og tilbaketrekkingslister

Ved mottak av melding utstyrt med signatur må det blant annet kontrolleres om signaturen kan verifiseres om de relevante sertifikatene fortsatt er gyldige og tilfredsstillende for den aktuelle anvendelse om sertifikatet tilhører rett person mv. Hvilke kontroller som skal gjennomføres og hvilken tilleggsinformasjon

---

66

En del problemer løses dersom passord for tilgang til signeringsnøkler må oppgis hver gang signeringsnøkkelen skal benyttes slik det er foreslått i Sverige. Men med mindre signering foregår i aktive kort e.l. vil dette antakelig være avhengig av den enkeltes lokale konfigurasjon.

.

som skal innhentes vil avhenge av hvilken tjeneste som benyttes og hvor viktig den enkelte anvendelse er. Kravene kan defineres gjennom en signaturpolicy[67]

I motsetning til saksbehandler i forvaltningen som kan ha funksjonen dekket gjennom en sentralisert tjeneste må enkeltpersoner besørge nødvendig verifisering selv. Dette er oppgaver som i størst mulig grad bør løses automatisk. De vesentligste av disse funksjonene vil formodentlig være tilgjengelige og automatisert i den enkeltes lokale informasjonssystem og gjennom tjenesteleverandøren. Det kan neppe kreves at den enkelte skal kunne utføre dette manuelt. Eventuelle retningslinjer må derfor ha karakter av anbefalinger som er rettet vel så mye mot leverandører av produkter og tjenester som mot brukeren selv.

Hvis verifisering derimot ikke lykkes og dette har slik betydning at videre behandling av meldingen ikke kan skje bør brukeren på samme måte som en saksbehandler i et forvaltningsorgan initiere melding til avsender.

- Dersom melding som er utstyrt med elektronisk signatur ikke kan verifiseres i henhold til reglene som gjelder for den aktuelle meldingstypen og dette har betydning for behandling av meldingen bør det sendes melding til avsender.

11.2.7.7 Krav til/anbefaling om lokal oppbevaring av sertifikater mv.

Opplysninger som er nødvendige for å verifisere en signatur bør oppbevares sammen med meldingen eller gjennom vedlikehold av lokal historisk sertifikatdatabase og sperreliste mv. og med referanse til den enkelte melding. Slike opplysninger kan i tillegg til de relevante sertifikatene f.eks. være bekreftelse på kontroll av tilbaketrekkingsliste e.l.

I motsetning til hva som gjelder for forvaltningen vil enkeltpersoner normalt ikke ha tilgang til arkivtjeneste som kan ivareta denne funksjonen. Det er også vanskelig å se hvorledes den enkelte skal kunne klare dette på egen hånd. Det kan derfor være nødvendig å la den enkelte få basere sin langtidslagring av meldinger utvekslet med forvaltningen i forvaltningens arkiv. Dette vil i så fall ytterligere forsterke behovene for oppfyllelse av plikten til journalføring og arkivering på forvaltningens hånd. Den tiden den aktuelle transaksjonen eller informasjonsutvekslingen pågår bør den enkelte i tillegg oppbevare de nødvendige opplysningene selv. Det er også mulig at det vil vokse fram særskilte tjenester som tilbyr oppbevaring av elektronisk lagret materiale over tid.[68]

- Lagring av relevant(e) sertifikat(er) og øvrige opplysninger som er nødvendige for verifisering av signaturer som er benyttet ved kommunikasjon med forvaltningsorgan kan den enkelte overlate til forvaltningens arkiv.
- Hvorledes langtidslagring og eventuelt utlevering til enkeltpersoner skal skje følger de til enhver tid gjeldende regler for arkivet.
- Den tiden den aktuelle transaksjonen eller informasjonsutvekslingen pågår bør den enkelte i tillegg oppbevare nødvendige opplysninger selv.

67

Jf. f.eks. ETSI ES 201 733 *Electronic Signature Formats* og GlobalSign/ICRI *Signature Policies* 28 August 2000.

.

68

Se f.eks. SINTEFs forprosjekt om en «Nasjonal BitBank» i rapporten *Langtidslagring av informasjon. Underlag for etablering av en BitBank* SINTEF Rapport STF40 A99082 28. desember 1999.

11.2.8 Inngrep ved misbruk av sertifikat ved kommunikasjon med forvaltningen

Elektronisk saksbehandling må bygge på tillit til de valgte sikkerhetsløsningene. Men sikkerheten avhenger av at brukerne opptrer aktsomt og lojalt. Dersom et antall brukere misbruker en sikkerhetsløsning vil dette svekke tilliten til løsningen som helhet. Det bør derfor være mulig å sperre for brukere som misbruker løsningen. Sperring kan f.eks. skje ved at brukernavn sperres eller at sertifikater trekkes tilbake.

Dette kan være et anliggende for den enkelte sertifikatutsteder men kan også gjelde forvaltningsorganet direkte enten fordi forvaltningsorganet selv administrerer koder eller passord eller fordi forvaltningsorganet ikke lenger har grunn til å ha tillit til bruken av et bestemt sertifikat. I så fall kan sperring skje enten av sertifikatutsteder hvis den aktuelle policyen åpner for sperring etter initiativ fra utenforstående eller sertifikatutsteder selv eller i lokal sperreliste hos forvaltningsorganet hvis en slik finnes. Det bør vurderes å operere med slike «interne lister» som del av den lokale nøkkeladministrasjonen hvis borgerne står fritt til å velge sertifikattjenester fra andre enn de forvaltningen har avtale med.

Dersom borgeren benytter et sertifikat fra en frittstående sertifikatutsteder og dette sertifikatet kan benyttes også til andre formål enn kommunikasjon med forvaltningen er det ikke sikkert at et eventuelt misbruk i forbindelse med f.eks. rapportering til forvaltningen gir grunnlag for å trekke tilbake sertifikatet som sådant i og med at slik tilbaketrekking også vil sperre for andre anvendelser. Det kan likevel være grunn for forvaltningsorganet til å sperre sertifikatet for bruk mot forvaltningen. Det kan i så fall skje ved hjelp av lokale sperrelister eventuelt ved samkjøring med satsvis nedlastede sperrelister fra sertifikatutsteder. En slik løsning vil være mindre inngripende overfor sertifikateier enn sperring av sertifikatet i sertifikatutsteders sperreliste.

Samtidig må man ta høyde for at sperring av koder eller sertifikater kan ha inngripende virkning overfor den enkelte. Derfor må det etableres rutiner for kvalitetssikring av opplysninger som ligger til grunn for en slik avgjørelse adgang til overprøving håndtering av sertifikater mens klagen er under behandling og prosedyrer som sikrer at slik behandling skjer raskt.

Før sperring skjer må sertifikateier få anledning til å uttale seg. Ettersom sperring av sertifikat forutsetningsvis er en reaksjon på et grovt tillitsbrudd fra sertifikateier overfor forvaltningsorganet og fortsatt misbruk vil kunne påføre forvaltningen eller andre tap eller merarbeid bør ikke fristen være lenger enn det som er nødvendig for sertifikateier for å rette innvendinger mot sperring av sertifikatet.

Ved begrunnet mistanke om misbruk av sertifikat ved kommunikasjon med forvaltningsorgan kan forvaltningsorganet sperre brukeridentiteten eller sertifikatet for videre bruk mot organet. Det samme gjelder dersom sertifikateier misbruker tillatelse eller adgang til å kommunisere elektronisk med organet.[69]

- Før sertifikatet sperres skal forvaltningsorganet sende sertifikateier melding om at de vurderer å sperre sertifikatet og begrunnelsen for dette. Sertifikateier skal oppfordres til å uttale seg om grunnlaget for sperring. Forvaltningsorganet skal sette en frist for en slik uttalelse (som ikke skal være kortere enn (antall) dager).
- Dersom forvaltningsorganet etter å ha vurdert sertifikateiers uttalelse velger å sperre sertifikatet skal forvaltningsorganet straks sende sertifikateier melding om dette.
- Sertifikateier kan påklage vedtak om sperring.
- Klage over sperring av sertifikat skal behandles så raskt som mulig og klageorganet kan bestemme at klagen skal gis oppsettende virkning.

69

F.eks. ved systematisk feilrapportering mot et automatisert innrapporteringssystem.

- Klageorgan for sperring av sertifikat i forvaltningen utpekes av Kongen/koordinerende departement. Det kan gis særskilte regler om behandling av klage over sperring av sertifikater.
- Bestemmelsene gjelder tilsvarende for sperring av autentiseringsdata (brukernavn med tilhørende passord/PIN-kode) i informasjonssystemer tilrettelagt av forvaltningsorganet så langt de passer.

11.2.9 Kopi av signeringsnøkler

Kopiering av signeringsnøkler for privatpersoner og ansatte bør normalt ikke forekomme. Dersom en signeringsnøkkel kommer på avveie vil det være mulig for andre å opptre som eierens «elektroniske dobbeltgjenger» inntil det tilhørende sertifikatet er sperret.

Det er heller ikke noe stort behov for kopiering av signeringsnøkler. Dersom nøkkelen går tapt eller kommer på avveie kan det genereres en ny og utstedes et nytt sertifikat. For enkeltpersoner vil det neppe være noe uoverstigelig problem å være uten nøkkel og sertifikat den tiden det tar å utstede et nytt.

Data vil ikke gå tapt selv om signeringsnøkkel tapes eller et sertifikat trekkes tilbake. De problemer som er knyttet til verifisering av signaturer med tilbaketrukne sertifikater er berørt under avsnitt 11.2.4 om arkivering.

Om reserveløsninger for automatiserte systemer se punkt 11.2.5.

- Det skal ikke forekomme kopier av signeringsnøkler utstedt til enkeltpersoner.

11.3 Innholdskryptering og nøkkelhåndtering

11.3.1 Innledning

Krav til innholdskryptering[70] (sikring av konfidensialitet) utløses til dels av andre regler og bygger på andre hensyn enn krav til sikring av integritet autentisering og ikke-benekting. Det stilles også andre krav til brukere i forbindelse med innholdskryptering. Det ansees derfor hensiktsmessig å behandle disse spørsmålene separat – bl.a. for å unngå sammenblanding.

Når endelige regler skal utarbeides kan man vurdere en samordning med reglene for elektronisk kommunikasjon og signaturtjenester. En slik samordning forutsetter imidlertid at det 1) innebærer en forenkling eller annen effektivisering av regelverket og 2) ikke innebærer risiko for misforståelser. I motsatt fall vil det antakelig være mer hensiktsmessig å holde reglene atskilt i alle fall i ulike kapitler i samme forskrift/instruks. Forenklinger kan f.eks. være knyttet til felles prosedyrer for søknad og behandling av søknader om tildeling av nøkler kort koder og sertifikater. Misforståelser kan oppstå f.eks. som følge av begrepsforvirring.

Bruk av innholdskryptering stiller krav både til forvaltningens ansatte og til den enkelte som kommuniserer med forvaltningen. Dette gjelder forsvarlig omgang med nøkler valg av korrekt nøkkel for

---

70

Med innholdskryptering menes her tiltak for sikring av konfidensialitet mv. ikke kryptering av innhold i forbindelse med systemer for betal-TV rettighetsadministrasjon o.l.

kryptering (evt. av sesjonsnøkkel) prosedyrer ved mottak av kryptert materiale og sikkerhetskopiering og oppbevaring eller deponering av krypteringsnøkler. Kravet til tilgjengelighet forutsetter løsninger som sikrer at materialet ikke går tapt som følge av at nøkler mistes eller ødelegges.

De anbefalte reglene griper ikke inn i de reglene som utløser krav til bruk av innholdskryptering eller annen sikring av opplysninger men er ment som et supplement som kommer til anvendelse når kryptering eller sikringstiltak skal benyttes.

11.3.2 Samordning av krav til innholdskryptering

Krav til eller behov for innholdskryptering kan utløses fra flere hold: For det første gjennom alminnelige regler om taushetsplikt jf. forvaltningsloven § 13 flg. og tilsvarende bestemmelser i forvaltningens særlover. For det andre gjennom krav til behandling av personopplysninger jf. personopplysningsloven § 2 nr. 8 og utkast til forskrifter om sikring av personopplysninger (nå kap. 4 i utkastet til personopplysningsforskrift). For det tredje dokumenter gradert etter beskyttelsesinstruksen (eller sikkerhetsloven med forskrifter). Og avslutningsvis gjennom forvaltningens behov for å sikre opplysninger unntatt offentlighet av andre hensyn enn de som gjelder reglene ovenfor – f.eks. behandling av budsjetter e.l.

Det ville åpenbart være en fordel med størst mulig grad av samordning når det gjelder krav til innholdskryptering utløst av regler om henholdsvis taushetsplikt behandling av personopplysninger og andre forvaltningsinterne behov.

Taushetsplikt vil i mange tilfeller være knyttet til behandling av personopplysninger – og behandling av personopplysninger er formodentlig en normal del av forvaltningens kommunikasjon med borgerne i alle fall så langt det dreier seg om saksrelaterte opplysninger.

Med mindre det kan påvises særlige sikkerhetskrav på det aktuelle forvaltningsorganets område f.eks. helsevesenet trygdevesenet og sosialvesenet som kan innebære skjerpede krav bør man tilstrebe å operere med et felles sikkerhetsnivå som er tilstrekkelig i alle de tre nevnte tilfellene. Dette kan innebære en «overoppfyllelse» av kravene men vil likevel være å foretrekke fordi man regelmessig vil være underlagt krav om sikring etter mer enn ett regelverk og det vil være problematisk for den enkelte saksbehandler (eller meldingssentral) å vurdere sikkerhetsbehovet i det enkelte tilfelle.

Det er ellers nærliggende å tenke seg at vern om sensitive personopplysninger vil representere en yttergrense for hva som kreves også i forhold til alminnelig taushetsplikt.

11.3.3 Informasjon til borgerne ved formidling av personopplysninger og taushetsbelagt informasjon til forvaltningen

Forvaltningens plikt til å sikre informasjon etter reglene om taushetsplikt og behandling av personopplysninger bør om ikke annet som et utslag av veiledningsplikten utløse plikt til å informere borgerne om de risikoer som hefter ved elektronisk formidling av (person)opplysninger og til å legge til rette for at borgerne enkelt kan få tilgang til hensiktsmessige sikkerhetstjenester.

Taushetsplikten og behandlingsreglene gjelder normalt forvaltningsorganet som sådant. Den enkelte borger kan utvilsomt beslutte at vedkommende selv vil sende opplysninger ubeskyttet til forvaltningen. Men en slik beslutning bør være basert på relevant og tilstrekkelig informasjon slik at vedkommende fatter en «opplyst beslutning». Dersom forvaltningsorganet aktivt gjør tilgjengelig en kommunikasjonskanal som innebærer en risiko for brukerne vil det formodentlig føre til skjerping av veiledningsplikten slik at den enkelte bedre kan ivareta sine interesser.

Plikten må være begrenset til de tilfellene der forvaltningen faktisk har kontakt med vedkommende før opplysninger overføres f.eks. ved at vedkommende slår opp på relevant web-side laster ned et passende skjema eller på annen måte får tilgang til informasjon som opplyser om eller gir inntrykk av at opplysninger kan sendes elektronisk. Den helt egeninitierte sendingen av førstehenvendelse pr. e-post med personopplysninger eller annen informasjon som vil være taushetsbelagt på forvaltningens hånd kan man vanskelig gjøre noe med.

- Et forvaltningsorgan som legger til rette for å motta fra enkeltpersoner eller virksomheter opplysninger som på forvaltningens hånd kan være underlagt taushetsplikt eller krav til sikring etter reglene om behandling av personopplysninger skal på hensiktsmessig måte informere den enkelte om eventuelle risikoer ved elektronisk overføring av aktuelle opplysninger.
- Forvaltningsorganet skal gjøre nødvendige sikkerhetstjenester lett tilgjengelige for den enkelte eller gi opplysninger som gjør at den enkelte lett kan få tilgang til slike tjenester.
- Forvaltningsorganet skal også (på forespørsel) opplyse om hvorledes personopplysninger eller taushetsbelagt informasjon sikres under behandling i forvaltningsorganet.
- Dersom risiko for uberettiget innsyn i taushetsbelagt informasjon eller personopplysninger ikke kan forebygges på en enkel måte av den enkelte skal forvaltningsorganet ikke legge til rette for slik kommunikasjon.

11.3.4 Anskaffelse og bruk av nøkler kort koder og sertifikater mv.

Reglene for den enkeltes anskaffelse av nøkler kort koder og sertifikater bør i det vesentlige følge samme regler som for elektroniske signaturer. Det samme gjelder kravene til forsvarlig omgang med nøkler og koder samt krav til varsling ved tap eller mistanke om tap eller misbruk.

11.3.5 Kryptering av melding til forvaltningen

I de fleste tilfeller vil meldinger fra enkeltpersoner til et forvaltningsorgan angå organet som sådan og ikke bare en enkelt saksbehandler. Den enkelte vil ofte heller ikke vite hvilken saksbehandler meldingen skal rettes til. I normaltilfellene bør en melding til et forvaltningsorgan derfor benytte en felles krypteringsnøkkel for forvaltningsorganet. Den videre beskyttelsen av meldingen må ivaretas i forvaltningens system i henhold til behandlingsreglene for den aktuelle meldingen.

Det er likevel mulig at man for visse typer materiale vil ha behov for å sikre konfidensialitet helt fram til saksbehandler. Dette kan gjelde f.eks. opplysninger om forhold i barnevernet eller sosialomsorgen som kun én eller noen få saksbehandler(e) skal ha tilgang til. Det bør derfor være adgang til å gjøre unntak fra regelen om å benytte nøkkel knyttet til organet selv om en slik regel også kan nyanseres f.eks. mot avdeling e.l.

Melding adressert direkte til saksbehandler kryptert ved hjelp av saksbehandlers offentlige nøkkel forutsetter særlige rutiner internt i organet blant annet når det gjelder håndtering av nøkler i vedkommendes fravær spørsmålet om deponering av kopi av den ansattes krypteringsnøkler mv. Det må derfor være opp til det enkelte organ å legge til rette for dette jf. det som er sagt om direkte adressering og deponering under punkt 11.2.3 og 11.3.8.

- Ved kryptering av melding til forvaltningen skal det benyttes krypteringsnøkkel knyttet til forvaltningsorganet.
- Kryptering med krypteringsnøkkel knyttet til en saksbehandler kan bare benyttes dersom organet har lagt til rette for dette.

11.3.6 Restriksjoner på bruk

Det bør ikke legges restriksjoner på bruk av privatpersoners krypteringsnøkler med mindre det kan påvises særlige behov.

11.3.7 Mottak av kryptert materiale

Mottatt materiale bør dekrypteres ved mottak. Dette skal blant annet sikre at materialet faktisk er tilgjengelig for organet. Det er også vanskelig å kontrollere om en melding er fri for virus mv. så lenge den er kryptert. Meldingen bør kontrolleres før den spres videre i organisasjonens informasjonssystem. Dersom dekryptering ikke lykkes må det sendes melding til avsender om at forvaltningsorganet ikke får tilgang til meldingen og om hvilke tiltak avsender må sette i verk. Vanligvis vil det dreie seg om å sende meldingen på nytt.

Beskyttelse av data internt i etatens eget system kan skje med andre midler enn kryptering overfor omverdenen fordi det er kjente deltakere og forvaltningsorganet definerer selv «reglene» for tilgang til og bruk av systemet.

- Melding som mottas av forvaltningsorganet i kryptert form skal straks dekrypteres.
- Hvis meldingen ikke lar seg dekryptere ved mottak skal meldingen straks returneres til avsender med beskjed om at meldingen ikke lot seg dekryptere (ikke tilgjengelig for forvaltningsorganet eller annen mottaker) og at det må sendes ny melding.
- Retur av melding på slikt grunnlag skal registreres/loggføres/journalføres hos forvaltningsorganet med opplysning om hvem avsenderen var tidspunkt for mottak og retur av meldingen og angivelse av hva meldingen gjaldt hvis dette er kjent (f.eks. gjennom en eventuell åpen tittel e.l.).
- For melding som returneres fordi den ikke er tilgjengelig for forvaltningsorganet fordi det er benyttet annen krypteringsnøkkel enn angitt for organet (eller meldingens innhold av andre grunner ikke er tilgjengelig for forvaltningsorganet) gjelder forvaltningslovens regler om avvisning og oppreisning.
- Beskyttelse av data internt i etatens eget system skjer med de midler etaten eller koordinerende organ fastsetter som nødvendige og hensiktsmessige.

11.3.8 Deponering eller annen sikkerhetskopiering av krypteringsnøkler

Det er naturligvis viktig at materiale ikke blir utilgjengelig for forvaltningsorganet som følge av at krypteringsnøkler går tapt. Det kan derfor være aktuelt å stille krav om sikkerhetskopiering og/eller deponering av krypteringsnøkler.

Det finnes motforestillinger av personvernmessig art når det gjelder krav om sikkerhetskopiering og deponering av krypteringsnøkler. Men dersom det etableres krav om at man skal benytte krypteringsnøkkel knyttet til forvaltningsorganet (og ikke til saksbehandler) ved kryptering av materiale til organet og kravet til kopiering/oppbevaring eller deponering knyttes til slike nøkler burde betenkelighetene bli mindre.

Hvis man legger restriksjoner på bruk av forvaltningsansattes krypteringsnøkler til kun å gjelde kommunikasjon i forvaltningens tjeneste bør det heller ikke være store betenkeligheter knyttet til krav om sikkerhetskopiering og eventuell deponering av slike nøkler.

Det kan imidlertid tenkes tilfeller der rutiner for bruk av den forvaltningsansattes egen nøkkel er begrunnet i at organet ikke uten videre skal ha tilgang til den informasjon den enkelte saksbehandler mottar. I så fall må man vurdere strammere rutiner for deponering enn hva som ellers benyttes for organets nøkler. Det må likevel bare være i unntakstilfellene at det overhodet ikke skal være adgang til sikkerhetskopiering eller deponering av krypteringsnøkler som benyttes for materiale som gjelder forvaltningsorganets virksomhet.

Sikkerhetskopiering og/eller deponering av krypteringsnøkler forutsetter gode prosedyrer for sikring av kopiene slik at materiale ikke blir gjort tilgjengelig for uvedkommende. Tilgang til slikt materiale bør kunne gjøres tilgjengelig uten tidkrevende prosedyrer når behovet først oppstår. En begjæring fra lederen av den delen av forvaltningsorganet som det krypterte materialet sorterer under eventuelt vedkommendes overordnede bør antakelig være tilstrekkelig. Ettersom det krypterte materialet etter den avgrensningen som

er brukt her gjelder forvaltningsorganets forhold burde ytterligere begrensninger normalt ikke være nødvendig.

Hvis det skal være alminnelig adgang for den enkelte til også å benytte sin krypteringsnøkkel for private formål bør man antakelig vurdere spørsmålet om sikkerhetskopiering/deponering om igjen. Det anbefales imidlertid at man reserverer bruken av forvaltningsorganets og saksbehandlers krypteringsnøkkel for materiale som angår forvaltningsorganet.

- Krypteringsnøkler som benyttes for dekryptering av meldinger til eller internt i forvaltningsorganet kan sikkerhetskopieres og oppbevares i flere kopier for sikkerhetsformål.
- Slik sikkerhetskopiering og oppbevaring skal følge anerkjente prosedyrer for sikkerhetskopiering og oppbevaring av krypteringsnøkler.
- Det skal alltid finnes mer enn én kopi av nøkkel for dekryptering av materiale til eller i forvaltningsorganet.
- Arkivansvarlig for organet skal alltid disponere en ekstra nøkkel for dekryptering av materiale til organet.
- Arkivansvarlig kan beslutte at kopi av krypteringsnøkkel for dekryptering av materiale til forvaltningsorganet skal deponeres hos annet organ.
- Kopi av nøkkel for dekryptering skal utleveres på begjæring fra lederen av det forvaltningsorganet eller den delen av forvaltningsorganet som materialet som er kryptert med den aktuelle krypteringsnøkkelen sorterer under.
- Begjæring om utlevering fremmes skriftlig. Hvis begjæringen fremmes i elektronisk form skal den være signert med avsenders digitale signatur eller annen tilfredsstillende teknikk for autentisering av meldingens opphav.
- Det kan gjøres unntak fra reglene om sikkerhetskopiering eller deponering av krypteringsnøkler for særlige typer av materiale. Slikt unntak kan besluttes av rette myndighet eller med hjemmel i annet regelverk (f.eks. beskyttelsesinstruksen).

11.4 Fastlegging av krav og utpeking av tilfredsstillende produkter og tjenester

Det er ikke definert krav til sikkerhetsprodukter og -tjenester som forvaltningen kan ønske å bruke. Der forvaltningen går sammen om felles standarder vil det være tjenlig med et felles organ som utarbeider krav og evaluerer slike produkter og tjenester.

- Man bør utpeke et organ som utarbeider krav til sikkerhetsprodukter og -tjenester som skal benyttes i forvaltningen. (I alle fall hvis det pågående standardiseringsarbeidet knyttet til direktivet om elektroniske signaturer ikke ansees tilfredsstillende eller man ønsker å benytte alternative sikkerhetsnivåer eller -tjenester.)
- For «kvalifiserte sertifikater» må det vurderes om det skal stilles tilleggskrav. Eventuelle tilleggskrav må ligge innenfor rammen av direktiv 1999/93/EF om elektroniske signaturer artikkel 3(7) jf. forslaget til lov om elektronisk signatur § 5.
- Man bør utpeke et organ som på forvaltningens vegne vurderer om et gitt produkt/tjeneste tilfredsstiller kravene.
- Man bør utarbeide krav til dokumentasjon og eventuell sikkerhetsrevisjon av leverandører av sikkerhetstjenester til forvaltningsorganer.

- Man bør utarbeide krav til samvirke med andre leverandører av sikkerhetstjenester og -produkter til forvaltningen.
- Et forvaltningsorgan som legger til rette for elektronisk kommunikasjon skal påse at det er produkter og tjenester tilgjengelig som tilfredsstiller relevante krav.
- Forvaltningsorganet bør selv tilby eller opplyse om tilbydere av produkter og tjenester som tilfredsstiller relevante krav.
- Produkter/tjenester som tilbys via forvaltningsorganet det kommuniseres med skal i forhold til den enkelte alltid ansees å tilfredsstille relevante krav.

11.5 Rettslige virkemidler – veiledende retningslinjer avtale instruks eller lovforankrede regler?

11.5.1 Veiledende retningslinjer

Man kunne tenke seg at nødvendige retningslinjer for bruk av digitale signaturer og kryptering ved kommunikasjon med og i offentlig forvaltning ble gitt i form av en veiledning til brukerne – en slags «god skikk»-regler som kunne videreutvikles av det såkalte «markedet» gjennom bruk.

Slike «myke regler» kan nok være både hensiktsmessige og velfungerende i mange sammenhenger. Særlig kan de være hensiktsmessige på områder der bransje- eller interesseorganisasjoner er i posisjon til å nedfelle retningslinjer som det kan forventes rimelig oppslutning om eller på områder der man har tradisjon og erfaring å bygge på. Dessuten vil slike «myke regler» oftest være et tilbygg til mer generelt formulerte lovfestede rettigheter eller plikter. De vil nok sjeldnere representere de grunnleggende prinsippene på området.

De reglene som dette mandatpunktet ønsker utredet og det området de skal regulere har andre kjennetegn. For det første mangler vi tradisjon og erfaring for elektronisk kommunikasjon med forvaltningen i større skala. For det andre mangler vi praktisk erfaring med aktuelle sikkerhetstjenester blant «alminnelige brukere». Videre er ikke forvaltningen formodentlig ved et koordinerende organ uten videre noen sterk påvirkningskraft i forhold til mangfoldigheten av brukere som reglene skal rette seg mot.

Formålet med reglene er dessuten å nedfelle hovedreglene for hvorledes elektronisk kommunikasjon med forvaltningen kan og skal skje med mulighet for å tilpasse løsningene til det enkelte forvaltningsorgans behov. De konkrete løsningene f.eks. utforming og drift av sertifikattjenester tilsyns- og godkjenningsordninger mv. kan nok i større grad utvikles «i markedet». Men ettersom retningslinjene her skal utgjøre de handlingsregler som forvaltningen kan støtte seg på når virksomheten skal åpnes for elektronisk kommunikasjon kan man ikke risikere at reglene smuldrer bort som følge av svikt ved eventuelle selvreguleringsmekanismer. Det kreves mer stabilitet og forutsigbarhet i rammebetingelsene hvis de skal kunne danne basis for mer omfattende bruk av elektronisk kommunikasjon.

11.5.2 Avtaleregulering eller lovforankring

Et alternativ til rene anbefalinger og selvregulering kan være at elektronisk kommunikasjon mellom borger og forvaltning blir gjort avhengig av personlig forhåndskontakt med og registrering hos det aktuelle forvaltningsorganet. I så fall kan man tenke seg at nødvendige regler for bruk av elektronisk kommunikasjon med forvaltningen blir nedfelt i en avtale mellom forvaltningsorganet og borgerne.

Det kan være spørsmål om man har hjemmel til å la borgerne binde seg ved avtale med hensyn til hvorledes de skal kommunisere med forvaltningen. Man kan åpenbart ikke frata borgerne deres rett til å kommunisere muntlig eller på papir etter forvaltningsloven eller særlovgivningen. Men det er mulig at man avtaleveien kan legge føringer for deres opptreden når de velger å utnytte adgangen til en alternativ kommunikasjonsmåte som elektronisk kommunikasjon som forvaltningen tilbyr av eget tiltak.

En modell basert på avtaleregulering vil imidlertid lett bli uoversiktlig fordi det kan utvikle seg ulik avtalepraksis og fordi det vil være vanskelig å holde oppsyn sentralt med den praksis som følges med sikte på koordinerende tiltak. Problemet forsterkes av at det ikke bare dreier seg om sentralforvaltningen. Også den lokale statlige forvaltningen og kommunalforvaltningen bør i alle fall til en viss grad operere etter de samme reglene.

Avtaleregulering i denne sammenheng kan dessuten være problematisk fordi det forutsetter kontakt mellom forvaltningsorganet og den enkelte før sikkerhetstjenestene kan tas bruk. Det er antakelig greit når det gjelder forvaltningsansattes bruk i tjenesten eller for borgernes bruk av tjenester som det offentlige selv administrerer gjennom f.eks. tildeling av brukernavn og passord/PIN-kode for å få tilgang til en informasjonstjeneste. Her må det uansett være forhåndskontakt mellom partene. Men for borgerne vil det i mange tilfeller innebære et unødig merarbeid å måtte inngå avtale med forvaltningsorganet dersom kommunikasjonen skal baseres på bruk av f.eks. kvalifiserte sertifikater utstedt av frittstående leverandører. Publikum vil da normalt inngå avtale med sertifikatutsteder. Det ville antakelig heller ikke være noen løsning å overlate til sertifikatutstederne å ivareta det offentliges interesser i så måte. Slike sertifikattjenester vil vanligvis kunne benyttes for flere formål og det ville være uhensiktsmessig antakelig umulig å basere forvaltningens virksomhet på at sertifikatutstederne sørger for å inngå avtaler med sertifikateierne med et innhold som spesielt tilgodeser forvaltningens behov.

Et annet problem med avtaleformen som virkemiddel sett fra forvaltningens ståsted er at man ikke uten videre kan gjennomføre endringer i de avtalene som er inngått. For den enkelte er det naturligvis av betydning å ha mest mulig stabile betingelser for bruk. På den andre siden har man forvaltningens behov for enhetlige prosedyrer som kan ajourføres når utviklingen gjør det nødvendig. De reglene som har vært drøftet i avsnittene 11.2 og 11.3 om henholdsvis signering og kryptering legger føringer også for forvaltningens mulighet for å organisere sin virksomhet. Det vil ikke være holdbart om muligheten til reorganisering skal være blokkert fordi forvaltningen har inngått avtaler om en bestemt framgangsmåte for elektronisk kommunikasjon. Reglene skal være et instrument for styring i retning av effektiv elektronisk kommunikasjon ikke en tvangstrøye som hindrer en fornuftig utvikling.

Forutsatt at det etableres hensiktsmessige rutiner for varsling av brukerne når bruksbetingelsene oppdateres vil en forankring av reglene i regelverk som kan ajourføres f.eks. etter reglene om forskrifter i forvaltningsloven være et mer hensiktsmessig virkemiddel enn bruk av avtaler.

Dette utelukker naturligvis ikke bruken av avtaler som virkemiddel for å gjøre brukeren særlig oppmerksom på de reglene som gjelder og for å understreke overfor brukeren f.eks. kravene til korrekt og forsvarlig bruk av signerings- og krypteringsnøkler nøkkelbærende kort og koder. Men problemene knyttet til gjennomføring av selve avtaleinngåelsen tilsier at man bør basere seg på regler forankret i lov.

11.5.3 Bør forvaltningsinterne forhold reguleres gjennom instruks?

Utvalget antar at reglene bør finnes i en form som er mer bindende og mer forutsigbar for adressatene enn rene anbefalinger og «god skikk»-regler. Det er også lagt til grunn at avtaleregulering neppe er veien å gå men at reglene kan nedfelles i en forskrift. En slik forskrift kan være naturlig forankret i forvaltningsloven og eventuelt i lov om elektronisk signatur.

Spørsmålet er om retningslinjene berører forvaltningsinterne forhold som det kunne være mer hensiktsmessig å regulere gjennom instruks. Det kan gi mer fleksibilitet i utvikling og tilpasning av regelverket. Dessuten unngår man at forskrifter rettet mot allmennheten blir mer omfattende enn nødvendig.

På den andre siden skaper det ekstra utfordringer med hensyn til regelverksadministrasjon og -vedlikehold fordi det er en tett indre sammenheng mellom reglene som retter seg innad mot forvaltningen og reguleringen av borgernes rettigheter og plikter når det gjelder kommunikasjon med forvaltningen. Man har også det problemet at i og med at også kommunalforvaltningen skal omfattes vil instruksjonsmyndigheten for et sentralt statlig organ ikke uten videre strekke til. Og det synes unaturlig å innføre en særskilt instruksjonsmyndighet på dette området. Det virker mer ryddig å operere med forskrifter forankret i lov for de reglene som skal være felles for alle forvaltningsorganer for stat og kommune.

Det er likevel noen forhold som kan eller bør løses gjennom instruks. Dette gjelder f.eks. bestemmelsene om hvem som signerer hva hvem som er berettiget til å godkjenne utstedelse av sertifikatene til ansatte i forvaltningen mv. Borgernes rettigheter i henhold til slike sertifikater kan knyttes

til objektive kjennetegn ved de utstedte sertifikatene uten at borgerne behøver å bekymre seg om hvorvidt de bakenforliggende rutinene er fulgt jf. det som er foreslått for bruk av «segl» i punkt 11.2.5.

Tilsvarende vurderinger kan antakelig gjøres når det gjelder systemer og sikkerhetstjenester tilrettelagt eller utpekt av forvaltningen. Det bør ikke være borgernes problem om det foreligger brudd på interne instrukser så lenge systemene utad framstår som «godkjent».

Utpeking eller organisering av et organ som skal utarbeide krav til sikkerhetstjenester for forvaltningen og for evaluering eller godkjenning basert på ekstern evalueringsrapport av slike tjenester og produkter kan skje gjennom instruks. Det samme gjelder retningslinjene for det enkelte forvaltningsorgans anskaffelse av slike tjenester. Dette gjelder naturligvis innenfor rammen av reglene om offentlige anskaffelser og de hensyn som gjelder på det aktuelle forvaltningsområdet ved overgang til elektronisk kommunikasjon som hensynene bak formkrav i lovgivningen jf. f.eks. Kartleggingsprosjektets rapport [47].

Reglene bør være enhetlige. Dersom man splitter reglene og ansvaret for dem mellom forskrift og instruks og mellom ulike forvaltningsnivåer oppstår det problemer som må løses f.eks. ved gode rutiner for administrasjon og vedlikehold av regelverket som sikrer at sammenhengen mellom internt og eksternt regelverk også mellom ulike regelverksforvaltere ivaretas.

11.5.4 Oppsummering av virkemidlene

Anbefalingen er altså at man i størst mulig utstrekning nedfeller nødvendige regler i forskrift forankret i forvaltningsloven og eventuelt lov om elektronisk signatur.

Forvaltningsinterne forhold knyttet til det å utarbeide krav til godkjenne og anskaffe sikkerhetstjenester og -produkter for forvaltningen samt reglene om intern saksbehandling kan løses f.eks. gjennom instruks.

De rettslige virkningene av at man har benyttet systemer valgt eller godkjent av forvaltningen eller sertifikater tilhørende forvaltningen må framgå av forskriftene eller loven som hjemler dem.

11.6 Skisse til forskrift om elektronisk kommunikasjon med og i forvaltningen

11.6.1 Signering og autentisering

Adressat for henvendelser til forvaltningen

1. Henvendelser i elektronisk form til et forvaltningsorgan skal rettes til den adressen forvaltningsorganet har oppgitt for slike henvendelser.
2. Hvis forvaltningsorganet har tilrettelagt for henvendelse eller visse typer av henvendelser via eget nettsted/hjemmeside skal henvendelser i elektronisk form skje på den måten det er tilrettelagt for.
3. Henvendelse i elektronisk form direkte til saksbehandler av meldinger som angår forvaltningsorganet skal kun skje hvis forvaltningsorganet har lagt til rette for det og uttrykkelig tillatt slik direkte kommunikasjon generelt eller i det enkelte tilfelle.
4. Forvaltningsorganet kan avvise henvendelser som har en annen form eller er avgitt til annen adresse eller på en annen måte enn foreskrevet eller tilrettelagt for. Forvaltningsorganet skal samtidig opplyse om hva som er korrekt adresse form eller framgangsmåte. Slike opplysninger kan gis i form av henvisning til eller utsending av veiledning om forholdet.
5. Forvaltningsorganet kan bestemme at adressering direkte til saksbehandler av meldinger som angår forvaltningsorganet bare kan skje når meldingen sendes fra annet forvaltningsorgan.

Henvendelser som utløser veiledningsplikt – formfrie henvendelser

1. Henvendelser til forvaltningen som ikke er underlagt særskilte formkrav og som ikke utløser saksbehandling kan skje i elektronisk form uten bruk av sikkerhetstjenester.
2. Forvaltningsorganet kan i det enkelte tilfelle be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av henvendelsen.

Søknader og andre henvendelser som utløser saksbehandling (knyttet til en konkret sak)

1. Henvendelser som utløser saksbehandling men som ikke er underlagt særskilte formkrav kan skje uten bruk av sikkerhetstjenester.
2. Forvaltningsorganet kan i det enkelte tilfelle be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av henvendelsen. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
3. Forvaltningsorganet kan fastsette at slike krav skal gjelde generelt for nærmere angitte typer av henvendelser.
4. Forvaltningsorganet skal tilby eller gi anvisning på tjenester som gjør det mulig å oppfylle kravet til bekreftelse av identitet eller fullmakter eller de øvrige krav forvaltningsorganet har stilt.

Henvendelser som er underlagt formkrav

1. For henvendelser som er underlagt særskilte formkrav kan forvaltningsorganet gi anvisning på hvilke virkemidler som må benyttes for at henvendelse kan skje i elektronisk form herunder krav til virkemidler for sikker bekreftelse av avsenders identitet eller fullmakter. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
2. Forvaltningsorganet skal tilby eller gi anvisning på tjenester som gjør det mulig å oppfylle kravet til bekreftelse av identitet eller fullmakter eller øvrige krav forvaltningsorganet har stilt.

Henvendelser som ikke tilfredsstiller aktuelle krav

1. Et forvaltningsorgan som mottar henvendelse i elektronisk form som ikke tilfredsstiller de aktuelle kravene til slik henvendelse skal uten ugrunnet opphold gi avsender melding om dette samt gi veiledning om hvilke tiltak som må iverksettes for at henvendelsen skal kunne tas under behandling.
2. Slik veiledning kan gis ved henvisning til forvaltningsorganets offentliggjorte regler for håndtering av den aktuelle typen henvendelse.
3. Forvaltningsorganet skal registrere tidspunkt for når slik melding er sendt og til hvem.
4. Dersom feilen er av en slik art at det ikke er mulig å identifisere avsender og varsel ikke kan sendes skal det registreres opplysning om dette.
5. Forvaltningslovens alminnelige regler om avvisning og oppreisning kommer til anvendelse på de nevnte forholdene.

Underretning om vedtak

1. Underretning om enkeltvedtak kan skje i elektronisk form dersom den vedtaket gjelder/den som har krav på underretning har samtykket i dette.
2. Underretning om vedtak skal gjøres tilgjengelig fra dertil egnet informasjonssystem.

3. Den vedtaket gjelder skal få melding om at vedtak er fattet og om hvor og hvordan vedkommende kan skaffe seg kunnskap om innholdet samt en frist for når dette senest må skje.
4. Vedtakets innhold skal gjøres tilgjengelig for parten når vedkommende bekrefter sin tilknytning til saken overfor informasjonssystemet der vedtaket er lagt ut (autentisering).
5. Informasjonssystemet registrerer tidspunktet for når parten har skaffet seg tilgang til vedtaket samt data som bekrefter vedkommendes tilknytning til saken.
6. Underretning ansees å ha skjedd på det tidspunktet parten skaffet seg tilgang til vedtaket.
7. Dersom parten ikke har skaffet seg tilgang til vedtaket innen 7 dager fra det tidspunkt det ble sendt melding om vedtaket eller vedtaket ble gjort tilgjengelig skal underretning skje i henhold til de reglene som gjelder for underretning om enkeltvedtak på det aktuelle området når det ikke er gitt samtykke til elektronisk kommunikasjon.

Klage

1. Klage over enkeltvedtak kan sendes i elektronisk form dersom forvaltningsorganet har tilrettelagt for det eller underretning om vedtaket er skjedd i elektronisk form.
2. Forvaltningsorganet kan be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er nødvendig for håndtering av klagen. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
3. Forvaltningsorganet skal tilby eller gi anvisning på tjenester som gjør det mulig å oppfylle kravet til bekreftelse av identitet eller fullmakter eller de øvrige kravene forvaltningsorganet har stilt.
4. Hvis det skal framsettes klage i elektronisk form og forvaltningsorganet har lagt til rette for klage ved bruk av sitt informasjonssystem skal denne framgangsmåten benyttes.
5. Et forvaltningsorgan som mottar klage i elektronisk form skal straks sende kvittering til avsender for mottatt klage.
6. Klager har plikt til å kontrollere at han mottar kvittering for innsendt klage. Dersom slik kvittering ikke er mottatt innen 24 timer skal klager sende klagen på nytt med angivelse av når den ble sendt første gang.

Innsyn i opplysninger og dokumenter i elektronisk form

1. Begjæring om innsyn i dokumenter eller opplysninger i en sak kan sendes forvaltningsorganet i elektronisk form.
2. Forvaltningsorganet kan i det enkelte tilfelle be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av henvendelsen. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
3. Dersom forvaltningsorganet fører elektronisk arkiv kan innsyn gis i elektronisk form.
4. Med mindre innsyn kan kreves etter offentlighetsloven gis innsyn i elektronisk form bare under forutsetning av at det kan gjennomføres tilfredsstillende bekreftelse av vedkommendes tilknytning til saken og sikkerhet for at dokumentene kun gjøres tilgjengelige for denne.

Høring og kommentar til høring av forskrifter og liknende

1. Høringsbrev til adressater med eget/sentralt e-postmottak kan sendes i elektronisk form. I stedet for fullstendig høringsbrev kan det sendes melding om hvor høringsbrevet er gjort tilgjengelig med oppfordring om å skaffe seg tilgang innen et nærmere angitt tidspunkt. Dersom vedkommende ikke har skaffet seg tilgang til høringsbrevet innen angitt frist bør høringsbrevet sendes i papirbasert form med mindre forvaltningsorganet har bestemt noe annet for den aktuelle høringen.
2. Uttalelser til høringen kan avgis i elektronisk form. Slik uttalelse avgis til den e-postadressen forvaltningsorganet har angitt for den aktuelle høringen eller på annen måte som forvaltningsorganet har gitt anvisning på.
3. Forvaltningsorganet kan be om opplysninger som bekrefter avsenders identitet eller fullmakter dersom dette er av betydning for håndtering av uttalelsen. Forvaltningsorganet kan også stille krav om at særlige sikkerhetstjenester skal tas i bruk.
4. Forvaltningsorganet skal tilby eller gi anvisning på tjenester som gjør det mulig å oppfylle kravet til bekreftelse av identitet eller fullmakter eller øvrige krav forvaltningsorganet har stilt.

Arkiv og langtidslagring

1. Melding som er signert med en digital signatur og som blir arkivert skal arkiveres sammen med sertifikat som bekrefter signaturen og øvrige opplysninger som er nødvendige for å verifisere signaturen herunder bekreftelse på at sertifikatet ikke var trukket tilbake på det tidspunkt verifisering fant sted.
2. For meldinger der sertifikatets gyldighetsperiode er kortere enn tiden det kan ta å bekrefte meldingens innhold og for meldinger som ved arkivering eller i løpet av oppbevaringstiden skal konverteres til annet format skal arkivet ved mottak verifisere signaturen og deretter på hensiktsmessig måte bekrefte knyttingen mellom meldingen meldingens signatur og aktuelt sertifikat sammen med opplysning om tidspunktet for bekreftelsen. Arkivet skal sikre integriteten til meldingene og bekreftelsen av de nevnte forholdene i oppbevaringsperioden. Arkivet kan beslutte at denne framgangsmåten skal benyttes også for andre meldinger (enn de som er nevnt i første setning).
3. Dersom arkivet ikke lykkes i å verifisere signaturen skal det lagres opplysning om det om mulig sammen med opplysning om årsaken til at verifisering ikke lyktes.
4. Melding eller resultatet av en automatisert databehandling (f.eks. fra automatisert tjeneste med web-grensesnitt) som er bekreftet med annen autentiseringsteknikk enn digital signatur skal lagres sammen med opplysninger om at korrekt autentisering har funnet sted og om mulig hvilken teknikk som er blitt benyttet.

11.6.2 Innholdskryptering og nøkkelhåndtering

Utstedelse og bruk av sertifikater for informasjonssystemer

1. Informasjonssystemer som benyttes i forbindelse med helt eller delvis automatiserte behandlinger og som i sitt resultat er eller framstår som avgjørelser i forvaltningslovens forstand skal utstyres med sertifikat som identifiserer den etaten som informasjonssystemet behandler meldinger for.
2. Sertifikatet skal inneholde opplysninger som overfor mottaker av sertifikatet bekrefter knyttingen mellom en behandling utført av informasjonssystemet og den aktuelle etat.

3. Mottaker av meldinger knyttet til slike sertifikater kan forholde seg til meldingen som om den var signert av en person i forvaltningen med fullmakt til å avgi eller signere nevnte melding eller avgjørelse med mindre vedkommende visste eller måtte vite at meldingen eller avgjørelsen var blitt til ved en feil.
4. Søknad om utstedelse av sertifikat som knytter signaturverifiseringsdata (offentlig nøkkel) til et informasjonssystem og en offentlig etat og som skal brukes ved behandlinger som kan resultere i avgjørelser etter forvaltningsloven skal godkjennes av den som er bemyndiget til å tildele fullmakter på etatens vegne.

Sårbarhetsbetraktninger – sikring av nøkler for informasjonssystemer

1. For et informasjonssystem som er utstyrt med sertifikat for forvaltningsorganet skal det være lagt opp rutiner som sikrer at systemet raskt kan settes i drift med nye signaturgenereringsdata og nytt sertifikat dersom det sertifikatet som er i bruk blir trukket tilbake eller signaturgenereringsdata går tapt.
2. Det bør vurderes om informasjonssystemet skal være utstyrt med signaturgenereringsdata og sertifikat fra mer enn én sertifikatutsteder.
3. Signaturgenereringsdata skal være sikret mot misbruk etter anerkjente prinsipper for informasjonssystemers sikkerhet.

Anskaffelse av nøkler koder og sertifikat

1. Et forvaltningsorgan kan gi sine ansatte anvisning om hvilke sikkerhetstjenester de skal benytte under tjeneste for organet og hvor de skal henvende seg eller gå fram for å anskaffe nødvendige nøkler koder sertifikater mv.
2. Forvaltningsansatte skal under tjeneste for arbeidsgiver kun benytte sertifikater utstedt av sertifikatutsteder som er godkjent av arbeidsgiver eller av et forvaltningsorgan som har koordineringsansvar for forvaltningens virksomhet.
3. Koordinerende forvaltningsorganer kan bestemme at det under tjeneste for forvaltningsorganer kun skal benyttes sertifikater fra sertifikatutsteder som har inngått rammeavtale om levering av slike tjenester til forvaltningen.
4. Dersom rammeavtalen løper ut og ikke blir fornyet i løpet av sertifikatets gyldighetsperiode skal sertifikatet likevel kunne benyttes i resten av gyldighetsperioden med mindre sertifikatutsteders sertifikat blir trukket tilbake eller nødvendige katalogtjenester mv. ikke lenger er tilgjengelige.
5. Koordinerende forvaltningsorganer kan bestemme at slikt sertifikat likevel ikke skal benyttes etter at rammeavtalen er løpt ut.

Innsamling av opplysninger og samtykke til utlevering av sertifikat mv.

1. Innsamling av opplysninger som skal benyttes i sertifikat skal skje direkte fra den opplysningen gjelder eller med dennes uttrykkelige samtykke jf. lov om elektronisk signatur § 7 [52].
2. I forbindelse med søknad fra forvaltningsansatt om sertifikat til bruk i tjenesten skal sertifikatutsteder be om den ansattes samtykke til utlevering av sertifikatet til andre jf. (forutsetningsvis) lov om elektronisk signatur § 14 annet ledd bokstav b).
3. Man bør søke samtykke til utlevering av opplysninger om den ansattes arbeidsområde eller fullmakter i tjenesten når disse opplysningene er lagret i tilknyttet katalog og ikke direkte i det aktuelle sertifikatet forutsatt at opplysningene kan forventes å ha betydning for anvendelsen av sertifikatet. Slike opplysninger skal kun utleveres i forbindelse med verifisering av det aktuelle sertifikatet.

Veiledning av den ansatte

Ved anskaffelse av nøkler koder og sertifikat skal den ansatte få opplysning/veiledning om:

1. Ansvar og plikter i forbindelse med oppbevaring og bruk av nøkler koder og sertifikat mv.
2. Aktuell sertifikatpolicy og -praksis (i form av en tilpasset brukerversjon)
3. Egen og andres mulighet for å sperre eller suspendere sertifikatet
4. Utløp av sertifikatet
5. Sertifikatutsteders oppbevaring av personopplysninger oppbevaringsperioden og hvem sertifikatet kan utleveres til mv. jf. personopplysningsloven § 19
6. Sertifikatutsteders ansvar og plikter
7. Registreringsenhetens ansvar og plikter
8. Restriksjoner på bruk av sertifikatet.

Restriksjoner på bruk av nøkler koder og sertifikat

1. Autentiseringsdata eller sertifikat (f.eks. ansattsertifikat) som inneholder peker til et forvaltningsorgan som arbeidsgiver skal kun benyttes i tjeneste for arbeidsgiver.
2. Personlige (private) sertifikater skal ikke benyttes i tjeneste for arbeidsgiver.

Krav til forsvarlig bruk og oppbevaring av den ansattes nøkler/nøkkelbærende medium

1. Eieren av signaturframstillingsdata skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre.
2. Signaturframstillingsdata skal kun benyttes til de formålene de er utstedt for.
3. Eieren skal aldri forlate arbeidsstasjon terminal eller annen enhet som benyttes for autentisering eller signaturgenerering uten å sikre at signaturframstillingsdata ikke lenger er tilgjengelig på/i enheten at den aktuelle sesjonen er avsluttet eller enheten på annen måte er sikret mot misbruk.
4. Eieren av signaturframstillingsdata skal ikke overlate disse til andre eller gi andre tilgang til dem heller ikke når andre skal handle på hans vegne. Dersom noen skal handle på vegne av en annen (etter fullmakt) skal dette skje med fullmektigens egne signaturframstillingsdata under henvisning til at meldingen er avgitt på vegne av en annen. (Den man opptrer på vegne av kan utstede rollesertifikat til sin fullmektig (når dette blir tilgjengelig).)
5. Bestemmelsene om signaturframstillingsdata gjelder tilsvarende for bruk av autentiseringsdata (passord/PIN-koder).
6. Den ansatte skal ellers følge instruksene arbeidsgiver har fastsatt om bruk og sikring av virksomhetens informasjonssystem herunder om kontroll med materiale som skal lastes ned eller installeres i informasjonssystemet.

Varslingsplikter ved tap av nøkler mistanke om misbruk mv.

1. Eieren av signaturframstillingsdata eller autentiseringsdata skal straks varsle sertifikatutsteder eller den som ellers er utpekt til å motta varsel dersom det oppstår mistanke om at signaturframstillingsdata eller autentiseringsdata er tapt kommet på avveie eller på annen måte blir eller kan bli misbrukt.

Krav til kontroll av sertifikater og tilbaketrekkingslister

1. Dersom melding som er utstyrt med elektronisk signatur ikke kan verifiseres i henhold til reglene som gjelder for den aktuelle meldingstypen og dette har betydning for

behandling av meldingen i forvaltningsorganet skal det sendes melding til avsender i henhold til reglene under punkt 11.2.3.

Krav til/anbefaling om lokal oppbevaring av sertifikater mv.

1. Kopi av relevant(e) sertifikat(er) og øvrige opplysninger som er nødvendige for verifisering av signaturer over tid bør oppbevares i arkivet.
2. Dersom meldingen i en periode lagres lokalt hos brukeren uten å være oversendt arkivet bør opplysningene lagres lokalt sammen med meldingen.

Valg av sikkerhetstjeneste

1. For elektronisk kommunikasjon med forvaltningen må den enkelte benytte tjenester som oppfyller kravene som stilles for den aktuelle anvendelse.
2. Dersom det benyttes kvalifiserte signaturer kan den enkelte selv velge hvilken leverandør av kvalifiserte sertifikater vedkommende vil benytte.
3. Forvaltningen kan stille tilleggskrav innenfor rammen av lov om elektronisk signatur § 5.

Veiledning av bruker

Ved anskaffelse av nøkler koder og sertifikat skal brukeren få opplysning/veiledning om:

1. Ansvar og plikter i forbindelse med oppbevaring og bruk av nøkler koder og sertifikat mv.
2. Aktuell sertifikatpolicy og -praksis (i form av en tilpasset brukerversjon)
3. Egen og andres mulighet for å sperre eller suspendere sertifikatet
4. Utløp av sertifikatet
5. Sertifikatutsteders oppbevaring av personopplysninger oppbevaringsperioden og hvem sertifikatet kan utleveres til mv. jf. personopplysningsloven § 19
6. Sertifikatutsteders ansvar og plikter
7. Registreringsenhetens ansvar og plikter
8. Restriksjoner på bruk av sertifikatet.

Restriksjoner på bruk av nøkler koder og sertifikat

1. Signaturframstillingsdata eller autentiseringsdata som er tildelt den enkelte spesielt for kommunikasjon med forvaltningen skal ikke benyttes for andre formål.
2. Slike begrensninger skal framgå av sertifikatetet og brukeren skal opplyses om begrensningene jf. om veiledning ovenfor.

Krav til forsvarlig bruk og oppbevaring av nøkler/nøkkelbærende medium

1. Eieren av signaturframstillingsdata skal oppbevare og benytte disse på en slik måte at de ikke gjøres tilgjengelige for andre.
2. Signaturframstillingsdata skal kun benyttes til de formålene de er utstedt for.
3. Eieren av signaturframstillingsdata bør aldri forlate arbeidsstasjon terminal eller annen enhet som benyttes for autentisering eller signaturgenerering uten å sikre at signaturframstillingsdata ikke lenger er tilgjengelig på/i enheten at den aktuelle sesjonen er avsluttet eller enheten på annen måte er sikret mot misbruk.
4. Eieren av signaturframstillingsdata skal ikke overlate disse til andre eller gi andre tilgang til dem heller ikke når andre skal handle på hans vegne. Dersom noen skal handle på vegne av en annen (etter fullmakt) skal dette skje med fullmektigens egne signaturframstillingsdata under henvisning til at meldingen er avgitt på vegne av en

annen. (Den man opptrer på vegne av kan utstede rollesertifikat til sin fullmektig (når dette blir tilgjengelig).)
5. Bestemmelsene om signaturframstillingsdata gjelder tilsvarende for bruk av autentiseringsdata (passord/PIN-koder).
6. Eieren av signaturframstillingsdata bør kun benytte disse i informasjonssystemer som vedkommende har tillit til og følge de anbefalinger som gis av sertifikatutsteder om innretting og bruk av systemet. Man bør vise varsomhet ved endringer i systemet og man bør kontrollere materiale som skal lastes ned eller installeres i informasjonssystemet.

Varslingsplikter ved tap av nøkler mistanke om misbruk mv.

1. Eieren av signaturframstillingsdata eller autentiseringsdata skal straks varsle sertifikatutsteder eller den som ellers er utpekt til å motta varsel dersom det oppstår mistanke om at signaturframstillingsdata eller autentiseringsdata er tapt kommet på avveie eller på annen måte blir eller kan bli misbrukt.

Krav til kontroll av sertifikater og tilbaketrekkingslister

1. Dersom melding som er utstyrt med elektronisk signatur ikke kan verifiseres i henhold til reglene som gjelder for den aktuelle meldingstypen og dette har betydning for behandling av meldingen bør det sendes melding til avsender.

Krav til/anbefaling om lokal oppbevaring av sertifikater mv.

1. Lagring av relevant(e) sertifikat(er) og øvrige opplysninger som er nødvendige for verifisering av signaturer som er benyttet ved kommunikasjon med et forvaltningsorgan kan den enkelte overlate til forvaltningens arkiv.
2. Hvorledes langtidslagring og eventuelt utlevering til enkeltpersoner skal skje følger de til enhver tid gjeldende regler for arkivet.
3. Den tiden den aktuelle transaksjonen eller informasjonsutvekslingen pågår bør den enkelte i tillegg oppbevare nødvendige opplysninger selv.

Inngrep ved misbruk av sertifikat ved kommunikasjon med forvaltningen

1. Ved begrunnet mistanke om misbruk av sertifikat ved kommunikasjon med forvaltningsorgan kan forvaltningsorganet sperre brukeridentiteten eller sertifikatet for videre bruk mot organet. Det samme gjelder dersom sertifikateier misbruker tillatelse eller adgang til å kommunisere elektronisk med organet.
2. Før sertifikatet sperres skal forvaltningsorganet sende sertifikateier melding om at de vurderer å sperre sertifikatet og begrunnelsen for dette. Sertifikateier skal oppfordres til å uttale seg om grunnlaget for sperringen. Forvaltningsorganet skal sette en frist for slik uttalelse (som ikke skal være kortere enn (antall) dager).
3. Dersom forvaltningsorganet etter å ha vurdert sertifikateiers uttalelse velger å sperre sertifikatet skal forvaltningsorganet straks sende sertifikateier melding om dette.
4. Sertifikateier kan påklage vedtak om sperring.
5. Klage over sperring av sertifikat skal behandles så raskt som mulig og klageorganet kan bestemme at klagen skal gis oppsettende virkning.
6. Klageorgan for sperring av sertifikat i forvaltningen utpekes av Kongen/koordinerende departement. Det kan gis særskilte regler om behandling av klage over sperring av sertifikater.

7. Bestemmelsene gjelder tilsvarende for sperring av autentiseringsdata (brukernavn med tilhørende passord/PIN-kode) i informasjonssystemer tilrettelagt av forvaltningsorganet så langt de passer.

Kopi av signeringsnøkler

1. Det skal ikke forekomme kopier av signeringsnøkler utstedt til enkeltpersoner.

Informasjon til borgerne ved formidling av personopplysninger og taushetsbelagt informasjon til forvaltningen

1. Et forvaltningsorgan som legger til rette for å motta fra enkeltpersoner eller virksomheter opplysninger som på forvaltningens hånd kan være underlagt taushetsplikt eller krav til sikring etter reglene om behandling av personopplysninger skal på hensiktsmessig måte informere den enkelte om eventuelle risikoer ved elektronisk overføring av aktuelle opplysninger.
2. Forvaltningsorganet skal gjøre nødvendige sikkerhetstjenester lett tilgjengelige for den enkelte eller gi opplysninger som gjør at den enkelte lett kan få tilgang til slike tjenester.
3. Forvaltningsorganet skal også (på forespørsel) opplyse om hvorledes personopplysninger eller taushetsbelagt informasjon sikres under behandling i forvaltningsorganet.
4. Dersom risiko for uberettiget innsyn i taushetsbelagt informasjon eller personopplysninger ikke kan forebygges på en enkel måte av den enkelte skal forvaltningsorganet ikke legge til rette for slik kommunikasjon.

Kryptering av melding til forvaltningen

1. Ved kryptering av melding til forvaltningen skal det benyttes krypteringsnøkkel knyttet til forvaltningsorganet.
2. Kryptering med krypteringsnøkkel knyttet til en saksbehandler kan bare benyttes dersom organet har lagt til rette for dette.

Mottak av kryptert materiale

1. Melding som mottas av forvaltningsorganet i kryptert form skal straks dekrypteres.
2. Hvis meldingen ikke lar seg dekryptere ved mottak skal meldingen straks returneres til avsender med beskjed om at meldingen ikke lot seg dekryptere (ikke tilgjengelig for forvaltningsorganet eller annen mottaker) og at det må sendes ny melding.
3. Retur av melding på slikt grunnlag skal registreres/loggføres/journalføres hos forvaltningsorganet med opplysninger om hvem avsenderen var tidspunkt for mottak og retur av meldingen og angivelse av hva meldingen gjaldt hvis dette er kjent (f.eks. gjennom en eventuell åpen tittel e.l.).
4. For melding som returneres fordi den ikke er tilgjengelig for forvaltningsorganet fordi det er benyttet annen krypteringsnøkkel enn angitt for organet (eller meldingens innhold av andre grunner ikke er tilgjengelig for forvaltningsorganet) gjelder forvaltningslovens regler om avvisning og oppreisning.
5. Beskyttelse av data internt i etatens eget system skjer med de midlene etaten eller det koordinerende organet fastsetter som nødvendige og hensiktsmessige.

Deponering eller annen sikkerhetskopiering av krypteringsnøkler

1. Krypteringsnøkler som benyttes for dekryptering av meldinger til eller internt i forvaltningsorganet kan sikkerhetskopieres og oppbevares i flere kopier for sikkerhetsformål.
2. Slik sikkerhetskopiering og oppbevaring skal følge anerkjente prosedyrer for sikkerhetskopiering og oppbevaring av krypteringsnøkler.
3. Det skal alltid finnes mer enn én kopi av nøkkel for dekryptering av materiale til eller i forvaltningsorganet.
4. Arkivansvarlig for organet skal alltid disponere en ekstra nøkkel for dekryptering av materiale til organet.
5. Arkivansvarlig kan beslutte at kopi av krypteringsnøkkel for dekryptering av materiale til forvaltningsorganet skal deponeres hos annet organ.
6. Kopi av nøkkel for dekryptering skal utleveres på begjæring fra lederen av det forvaltningsorganet eller den delen av forvaltningsorganet som materialet som er kryptert med den aktuelle krypteringsnøkkelen sorterer under.
7. Begjæring om utlevering fremmes skriftlig. Hvis begjæringen fremmes i elektronisk form skal den være signert med avsenders digitale signatur eller annen tilfredsstillende teknikk for autentisering av meldingens opphav.
8. Det kan gjøres unntak fra reglene om sikkerhetskopiering eller deponering av krypteringsnøkler for særlige typer av materiale. Slikt unntak kan besluttes av rette myndighet eller med hjemmel i annet regelverk (f.eks. beskyttelsesinstruksen).

11.6.3 Fastlegging av krav og utpeking av tilfredsstillende løsninger

Fastlegging av krav og utpeking av tilfredsstillende produkter og tjenester

1. Man bør utpeke et organ som utarbeider krav til sikkerhetsprodukter og -tjenester som skal benyttes i forvaltningen. (I alle fall hvis det pågående standardiseringsarbeidet knyttet til direktivet om elektroniske signaturer ikke ansees tilfredsstillende eller man ønsker å benytte alternative sikkerhetsnivåer eller -tjenester.)
2. For «kvalifiserte sertifikater» må det vurderes om det skal stilles tilleggskrav. Eventuelle tilleggskrav må ligge innenfor rammen av direktiv 1999/93/EF om elektroniske signaturer artikkel 3(7) jf. forslaget til lov om elektronisk signatur § 5.
3. Man bør utpeke et organ som på forvaltningens vegne vurderer om et gitt produkt/tjeneste tilfredsstiller kravene.
4. Man bør utarbeide krav til dokumentasjon og eventuell sikkerhetsrevisjon av leverandører av sikkerhetstjenester til forvaltningsorganer.
5. Man bør utarbeide krav til samvirke med andre leverandører av sikkerhetstjenester og -produkter til forvaltningen.
6. Et forvaltningsorgan som legger til rette for elektronisk kommunikasjon skal påse at det er produkter og tjenester tilgjengelig som tilfredsstiller relevante krav.
7. Forvaltningsorganet bør selv tilby eller opplyse om tilbydere av produkter og tjenester som tilfredsstiller relevante krav.
8. Produkter/tjenester som tilbys via forvaltningsorganet det kommuniseres med skal i forhold til den enkelte alltid ansees å tilfredsstille relevante krav.

11.7 Forslag til videre tiltak

Utvalget anbefaler at man utreder hvilke interne rutiner og programmer for kopling mot postmottak og arkiv som må være på plass før man starter med digitale signaturer og innholdskryptering.

- Man bør utrede om forvaltningsloven bør åpne for helt automatiserte beslutningsprosesser og hvilke typer sårbarhet det åpner for.
- Utvalget anbefaler at man vurderer andre måter å regulere kravene i beskyttelsesinstruksen på enn slik dagens instruks legger opp til. En løsning kan være å vurdere om disse reglene helt eller delvis kan inngå i en eventuell ny forskrift under forvaltningsloven bl.a. som utfyllende regler i forhold til lovens pålegg om å behandle taushetsbelagte opplysninger på en betryggende måte. Det bør bl.a. vurderes om det er mulig å samordne kravene for graden «Fortrolig» i beskyttelsesinstruksen med krav som følger f.eks. av taushetsplikt og sikring av sensitive personopplysninger. Utvalget mener derfor at beskyttelsesinstruksen bør oppheves forutsatt at man finner hensiktsmessige alternativer som forvaltningen er bedre tjent med.
- Dersom beskyttelsesinstruksen beholdes i sin nåværende form mener utvalget det er viktig å ta opp til ny vurdering hvilke regler som skal gjelde for opplysninger gradert etter beskyttelsesinstruksen ved elektronisk kommunikasjon. Utvalget mener at elektronisk behandling av opplysninger gradert «Fortrolig» bør kunne behandles etter reglene foreslått i denne utredningen med nødvendig presisering av standarder og anbefalte sikkerhetsnivåer. Utvalget mener følgelig at regler for elektronisk behandling av opplysninger gradert «Fortrolig» kan bygge på eller samordnes med utvalgets skisse til regelverk.
- Man bør vurdere om det skal utvikles spesialregler for fristavbrudd ved elektronisk formidling av klage f.eks. når klage leveres over dedikert informasjonstjeneste tilrettelagt av forvaltningsorganet.
- Man bør vurdere løsning basert på at forvaltningsorganet alltid skal kvittere for mottatt klage.
- Man bør også vurdere om meldinger som *verken* er saksdokument (kan evt. knyttes til om det skal journalføres og/eller arkiveres etter arkivloven) *eller* relevant som dokumentasjon etter økonomireglementet skal være helt unntatt fra reglene om bruk av autentiseringstjenester eller signeringsteknologi.
- Man bør utrede behov for og eventuelt krav til bruk av tidsstempling og lagring av informasjon hos en tiltrodd tredjepart om forvaltningen og befolkningen har slike behov.
- Man bør vurdere om det bør stilles overordnede funksjonelle krav til lagring som vil oppfylles av blant annet standarder som Noark-4 [57] (godkjent standard for elektronisk arkivsystem etter arkivloven og forskriftene) europeisk standard for (utvidede) signaturformater (ETSI ES 201 733).

Del V
Elektroniske ID-kort

12 Behovet for elektroniske ID-kort

12.1 Beskrivelse av problemstillingen

I forbindelse med utviklingen av elektroniske tjenester fra forvaltningen basert på Internett kan det være av interesse å vurdere en alternativ modell for spredning av offentlige personsertifikater. I denne modellen sørger det offentlige for et tilbud om å utstyre enkeltpersoner med et smartkort med sertifikater og private nøkler. Disse kortene kalles elektroniske identitetskort (EID-kort). Slike kort vil kunne brukes til å legitimere brukerne overfor elektroniske tjenester og for å sende signerte søknader henvendelser etc. elektronisk til forvaltningen. Den offentlig utstedte elektroniske legitimasjonen vil i så fall også kunne brukes som en generell elektronisk identitet overfor andre elektroniske tjenester enn de som tilhører forvaltningen. Men utvalget har ikke som mandat å utrede generelle identitetskort for befolkningen.

Sertifikatene i elektroniske identitetskort skal være offentlige personsertifikater i samsvar med det høyeste av nivåene som er skissert i kapittel 8.

Det er en forutsetning for diskusjonen i dette kapitlet at det skal være valgfritt for hver enkelt person om man vil anskaffe seg et slikt kort med offentlige personsertifikater. Det skal ikke gjøres obligatorisk for den enkelte å ha et slikt kort eller å bruke det. Det understrekes også at det heller ikke vil være tale om å gi dette offentlig utstedte kortet monopol på deler av sertifikatmarkedet men at et slikt offentlig elektronisk identitetskort vil konkurrere med andre utstedere av sertifikater.

Problemstillingen handler om elektroniske identitetskort for enkeltpersoner der brukeren anvender en privat nøkkel til å identifisere seg overfor et system. Et elektronisk ID-kort kan om ønskelig plasseres på samme fysiske enhet som andre fysiske og visuelle ID-kort og distribueres sammen med disse. Det kan også være mulig å kombinere identitetskortet med attributt- eller rolleinformasjon som sier noe om hvem innehaveren er i en viss sammenheng eller spesifiserer enkelte rettigheter som innehaveren har. Et ID-kort har ofte navn adresse fødselsdato gyldighetsområde (f.eks. at det er et førerkort for motorsykkel) og stempel eller annen informasjon som tilkjennegir utstederen. Vi er vant med at legitimasjon sjekkes manuelt og visuelt.

12.1.1 Hva et EID-kort kan inneholde

eRegel-prosjektet [47] nevner som en mulighet at objektive fakta om en person f.eks. navn alder adresse stilling kan lagres i et personsertifikat. Et sertifikat som skal brukes som elektronisk ID-kort må ha et innhold som med stor sannsynlighet er stabilt i gyldighetsperioden eller den tiden legitimitetsforholdet består. Dette kalles tidsinvariant informasjon. Sertifikater må byttes/fornyes når innholdet ikke lenger er korrekt når sertifikatet går ut eller når en nøkkel på andre måter ikke lenger er gyldig.

Adresse er et eksempel på tidsvariant informasjon (informasjon som ofte endres) som neppe bør være i et sertifikat. Det kan medføre at en stor del av befolkningens sertifikater må endres unødig ofte. Adresseinformasjon kan i stedet lett slås opp i en passende katalog.

En elektronisk ID vil være et sertifikat (eller en samling av sertifikater) signert av en sertifikatutsteder. En EID kan/bør ha nøkler for autentisering og signering sertifikater for disse og nøkkel for dekryptering.

Sertifikatet bør inneholde:

- Navn som er sjekket iht. folkeregisteret
- En identifikator som er unik innen utstederens domene og som kan koples mot fødselsnummer ved tjenstlig behov ev. fødselsnummer direkte
- Gyldighetsperiode
- Sertifikatutstederinformasjon.

12.1.2 Generelt om standarder for elektroniske identitetskort

Det finnes etablerte internasjonale standarder for visuelt ID-kort. (ISO Standard 7501-3 Machine Readable Travel Documents – Identity Cards).

Standard innhold i et EID-kort

Elektroniske identifikasjonskort (EID) er i ferd med å bli standardisert. Imidlertid går utviklingen fort på teknologisiden og standardiseringsprosessen kan bli hengende etter. Sverige er i en ledende posisjon. De har allerede vedtatt viktige deler av systembeskrivelsen som svensk standard (SS 61 43 30 61 43 31 og 61 43 32) og mer er under arbeid. Svenskene arbeider hardt for å få dette vedtatt som internasjonal standard og mye tyder på at de vil lykkes. Finland har adoptert det vesentligste av svenskenes beskrivelser for det finske EID-kortet. Finnene har også tatt ledelsen i et arbeid med elektroniske ID-kort under eEurope-paraplyen.

De standarder og spesifikasjoner som er gjeldende for EID-kort stiller meget strenge krav til rutinene for bestilling av kort utstedelse av kortet via flere delprosesser og til selve kortet og chipen.

Bruk av EID-kort

Et EID-kort kan inneholde flere nøkkelsertifikater. Et EID-kort med personsertifikater gir grunnlag for tilgang til for eksempel:

- Enkelte datasystemer i forvaltningen
- Annen informasjon via navnet eller fødselsnummeret. Det kan være fra kataloger som inneholder mer om ansettelsesforhold eller sier om eieren er gammel nok til å kjøpe øl
- Andre nøkkelsertifikater for digital signering og kryptering f.eks. rollesertifikater
- Nøkkelsertifikater med navn man er kjent ved i andre sammenhenger tilknyttet et ansettelsesforhold med ulike e-postadresser osv.

Et generelt identitetssertifikat som inneholder få eller ingen tidsvariante elementer der lagringsmåten for sertifikatet er god og der utleveringsmåten inngir tillit kan forenkle registreringen ved utstedelse av andre sertifikater.

Bruk av EID-kort forutsetter:

- Smartkort
- Smartkortleser i tilknytning til en PC
- Programvare på PC for behandling av informasjonen i kortet inkludert tilgang til sertifikatutsteders tilbaketrekkingslister og programvare hos de forvaltningsenhetene som skal behandle informasjonen.

12.1.3 Forvaltningens behov for ID-kort

Ønsket om enklest mulig tilgang til tjenester for sertifikateiere og myndighetenes krav om bruk av identifikasjon kan stå i konflikt med personverninteresser. Store deler av forvaltningen har tjenstlig behov for tilgang til korrekt navn og fødselsnummer i henhold til folkeregisteret. Det har imidlertid kommet motforestillinger fra flere hold mot å ha fødselsnummer direkte i sertifikatene. Det synes derfor å være naturlig å kreve at elektronisk ID skal inneholde korrekt navn og en unik identifikator som utsteder vil kunne kople med fødselsnummer. Utsteder eller en tjenesteoperatør for utsteder må kunne framskaffe fødselsnummer til etater og brukere i forvaltningen som har et legitimt tjenestemessig behov for dette. Alternativt kan fødselsnummer brukes der dette er påkrevet.

Av praktiske grunner er det også ønskelig at flere forvaltningssektorer aksepterer det samme identitetssertifikatet slik at ett logisk ID-kort vil gi tilgang til mange offentlige tjenester for enkeltpersoner.

Kortet og nøklene i det vil kunne anvendes til f.eks. elektronisk post fremme av klager tjenesteyting mot gebyrer (f.eks. attester fra Løsøreregisteret) og til dokumentinnsyn.

Forvaltningen kan i enkelte sammenhenger trenge å vite om en person har organisatorisk tilknytning til en etat eller en tjeneste. Tilknytningen vil man i mange situasjoner måtte avgjøre manuelt fordi den er beskrevet i attributter (felt i sertifikatet) som ikke alltid lar seg behandle maskinelt.

Forvaltningens behov for digitale signaturer sertifikater og elektroniske identiteter er diskutert i kapitlene 7 8 og 9.

Utvalget anbefaler at et eventuelt EID-kort må følge de anbefalingene som er gitt i disse kapitlene.

Forvaltningens viktigste behov er at de offentlige personsertifikatene gir et troverdig grunnlag for elektronisk identifisering av personen. Det er derfor nødvendig at sertifikatene i et EID-kort er tidsinvariante (stabile over tid). Det vil gi grunnlag for oppslag om annen mer foranderlig personinformasjon og forenkle utstedelse av andre sertifikater som for eksempel er knyttet til ansettelsesforhold. Samtidig får bare institusjoner som har tjenstlig grunn for det tilgang til fødselsnummeret.

Forvaltningen har en opplagt interesse av at enkeltpersoner har sertifikater og private nøkler som tilfredsstiller forvaltningens krav til elektronisk kommunikasjon. I denne utredningens kapittel 9 er det satt opp noen modeller for hvordan ansvaret for utstedelse av sertifikater kan plasseres.

I en av disse modellene beskrives etablering av en sentral offentlig tjeneste som utsteder offentlige personsertifikater til enkeltpersoner. Før man oppretter en slik ordning bør flere spørsmål avklares. Blant annet må man vurdere hvilke konsekvenser det kan få for det norske sertifikatmarkedet dersom en slik tjeneste blir en stor aktør i markedet. Videre bør man konkretisere med tanke på spørsmål om mulighet for kryptering av fødselsnummer annen unik identitet hva kortet kan inneholde hva det kan brukes til behovet for smartkort vs. mykt sertifikat for elektronisk ID og kvalifiserte sertifikater. Det må også understrekes at et slikt offentlig elektronisk identitetskort som brukes av svært mange privatpersoner vil gjøre risikoen større for at det legges igjen elektroniske spor og at disse kan følges.

12.1.4 Anvendelsesområder og motivasjon

Publikum må motiveres til både å anskaffe seg og å bruke sine elektroniske ID-er. Det må regnes som sannsynlig at motivasjonen for å anskaffe et sertifikat øker med antall mulige anvendelsesområder. Det kan følgelig være ønskelig at enkeltpersoner kan bruke samme sertifikater og nøkkelpar mot forvaltningen som mot andre tjenester. Derfor bør det vurderes om offentlig sektor heller bør oppfordre andre sertifikatutstedere i markedet til å utstede sertifikater som oppfyller forvaltningens krav til elektronisk ID.

Erfaringene fra Finland underbygger dette. Det finske elektroniske ID-kortet har nå eksistert i et års tid men det har vært vanskelig å finne gode elektroniske tjenester som motiverer enkeltpersoner til å ta i bruk et slikt kort. Mangelen på praktisk nyttige elektroniske tjenester har ført til at det i løpet av det første bruksåret bare er utstedt ca. 6–7000 elektroniske ID-er. Dersom det skal skapes interesse for å ta i bruk et slikt kort ser det derfor ut til at det må etableres tjenester som baseres på en felles autentiseringsløsning og som kan få enkeltpersoner til å se verdien og nytten i dette kombinerte elektroniske og fysiske identifikasjonsdokumentet. I Finland har man inngått samarbeidsavtale med en stor bank om bruk av offentlig utstedte sertifikater.

Elektronisk pass er en type elektronisk identifikasjonsdokument som det har vært stilt store forventninger til. Det fysiske passet er for tiden det eneste offisielle reisedokumentet for norske borgere som skal passere grensen til andre land. Et elektronisk pass vil i praksis kunne bli sammenkoplet med et fysisk identifikasjonsdokument. Arbeidet med å standardisere og ta i bruk dette har imidlertid hatt begrenset framdrift og status beskrives for øyeblikket som «flytende». Det kan derfor virke som om den mest fornuftige holdningen for norske myndigheter er å vente og se. Imidlertid må det ifølge Justisdepartementet antas at det også i Norge etter hvert vil bli spørsmål om tilsvarende «enkle» reisedokumenter på noe sikt blant annet som en mulig forpliktelse i forbindelse med Schengen-samarbeidet. Et gjennombrudd innenfor bruken av elektroniske pass kan endre mye av diskusjonen som er ført i dette kapitlet.

12.1.5 Priser administrasjon organisering

Hvis forvaltningen skal opprette en sentral institusjon for tildeling av EID-kort bør forvaltningen se nærmere på behovet og eventuelt utrede kravene i større detalj. Smartkort med sertifikater kan ha kortere levetid enn f.eks. pass og bør derfor prises lavere.

Et offentlig identitetskort bør ikke være gratis for innehaverne. Det finnes flere modeller for prising der henholdsvis utstedelse av sertifikat periodiske avgifter for å eie sertifikater og bruken av dem er prisbelagt. I tillegg vil sertifikateierne kunne få utgifter til programvare og utrustning (f.eks. kortleser) som må installeres hos dem slik at de kan nyttiggjøre seg sertifikatene. Også sertifikatbrukere må muligens betale for å gjøre oppslag i kataloger eller for å få verifisert et mottatt sertifikat.

Administrasjon og organisering bør plasseres i et sentralt offentlig organ og må tillegges en velfungerende enhet. Denne enheten bør stå i nær forbindelse med folkeregisteret. Det må videre utredes om deler av utstedelse registrering av brukere distribusjon og verifisering av elektronisk identitet med fordel kan plasseres hos underleverandører. Alle disse sidene ved sertifikatutstedelse vil kreve store oppstartkostnader og løpende driftskostnader. Det vil blant annet ligge store startkostnader i å etablere et sikkert produksjonsmiljø for sertifikater og kort og i å få på plass en logistikk for kort og data som kan ha tilstrekkelig tillit. Det vil også være kostbart å bygge opp det nødvendige apparatet for å motta meldinger om tilbaketrekking av sertifikater og iverksette slike. Programvare både for sertifikatutstedelsen så vel som i identitetskortene vil bli en betydelig utgift som vil kreve oppdateringer og tilpasninger.

Et viktig poeng når det gjelder publikums modenhet for å ta i bruk elektroniske ID-kort er utbredelsen av utstyret for kortlesing. Kortlesere kan kjøpes som tilleggsutstyr til en rimelig pris men finnes ennå i liten grad tilgjengelig som en standardisert del av PC-en. Håndtering av kortlesere krever fremdeles en del kompetanse kompetanse som det er rimelig å anta at ikke finnes i alminnelige husholdninger. Norsk Tippings testing av elektroniske tippekort våren 2001 vil være den første prøvesteinen når det gjelder publikums modenhet for denne typen tekniske løsninger.

Utstedere som konkurrerer på markedet arbeider nå med å etablere et produksjonsmiljø for sertifikater. Forvaltningen kan i denne sammenhengen sies å ha muligheten til både å stimulere markedet og til å konkurrere med det. Forvaltningen har ved tidligere anledninger ikke uttrykt noe ønske om å konkurrere med private sertifikatutstedere. En nærliggende løsning blir dermed at norske offentlige myndigheter spiller en sentral rolle ved å stille krav til utstederne i markedet og kjøpe sertifikater av dem som oppfyller forvaltningens krav.

12.2 Anbefaling

På grunnlag av vurderinger framlagt i dette kapitlet vil utvalget ikke anbefale at forvaltningen går i gang med etablering av en offentlig ordning for utstedelse av elektroniske ID-kort nå.

Det ansees foreløpig som tilstrekkelig at enkeltpersoner skaffer seg sertifikater fra utstedere i markedet. Offentlig sektor må motivere sertifikatutstederne til å produsere sertifikater som blir ansett som gode nok og som kan aksepteres av forvaltningen. Alle kvalifiserte sertifikater som er på de to høyeste nivåene etter punkt 8.2.5 og som oppfyller forvaltningens krav til innhold bør kunne aksepteres for kommunikasjon mot forvaltningen. Dette kan gjøres gjennom å inngå samarbeidsavtaler med relevante aktører i markedet jf. punkt 9.3.

Det kan heller ikke utelukkes at enkelte andre sertifikater som ikke er evaluert i henhold til disse nivåene i mange sammenhenger kan være akseptable for forvaltningen.

Forvaltningen bør oppmuntre sertifikatutstederne til å produsere sertifikater som dekker forvaltningens behov. Bl.a. bør forvaltningen løpende vurdere om den kan ta i bruk elektroniske ID-kort som kommersielle aktører tilbyr og på denne måten bidra til rammebetingelser som legger til rette for et velfungerende marked for bruk av elektronisk identitet.

Utvalget mener at man bør høste erfaringer både fra markedet og fra andre offentlige utstedere av slike EID-kort før en eventuell videre utredning av saken gjennomføres.

De teknologiske forholdene rundt elektroniske pass er ikke ferdig tilrettelagt og er foreløpig ikke noen motivasjon for å starte utstedelse av offentlig elektronisk ID.

Del VI
Konsekvenser av utvalgets anbefalinger

13 Kvalitative administrative og økonomiske konsekvenser

13.1 Utgangspunkter

For å nå de politiske målene om fornyelse av offentlig sektor bl.a. ved å innføre døgnåpen forvaltning mener utvalget at løsninger som sørger for sikker effektiv og pålitelig infrastruktur for elektronisk informasjonsutveksling er viktige virkemidler. Utvalget foreslår derfor enkelte sentrale fellestiltak. I tillegg foreslår utvalget en rekke tiltak på frivillig basis som den enkelte virksomhet i utgangspunktet må dekke selv.

De sentrale tiltakene utvalget anbefaler er i hovedtrekk følgende:

- Etablering av det som kalles en samordningsfunksjon som består av et nytt fast samordningsutvalg for forvaltningens felles behov ledet av Arbeids- og administrasjonsdepartementet eller Nærings- og handelsdepartementet med et sekretariat
- Etablering av et Forum for digitale signaturer for forvaltning næringsliv og leverandører
- Etablering av en ny rammeavtale for forvaltningen
- Etablering av avtaler med aktører i markedet om utstedelse av sertifikater til enkeltpersoner
- Bruk av stimuleringsmidler for å fremme bruken av digitale signaturer i elektronisk samhandling med og i offentlig forvaltning.

Utvalgets forslag er først og fremst utformet for å bidra til at hele området for sikker elektronisk forvaltning og kommunikasjon kan hjelpes fram uavhengig av tid og geografi. Dette vil gi bedre og mer effektiv tilgang til sikre elektroniske tjenester fra det offentlige for både enkeltpersoner og næringsliv og bety en effektivisering for det offentlige selv. Det er viktig at flest mulig skal få del i denne utviklingen slik at løsningene ikke blir nyttige bare for de mest ressurssterke. Gjennomføring av disse tiltakene vil medføre noen initielle kostnader og driftskostnader for forvaltningen som utvalget mener det er nødvendig og naturlig at man tar på vegne av fellesskapet.

Utvalget mener det er avgjørende at man fra sentralt statlig hold dekker kostnader som er nødvendige for å etablere *viktige fellesløsninger* men at den enkelte virksomhet for øvrig dekker kostnadene ved bruk av digitale signaturer og kryptering over egne budsjetter innenfor de tidsrammer som Regjeringen har satt for å nå målene om døgnåpen og elektronisk forvaltning innen år 2003.

Utvalgets forslag vil bidra til *kvalitativ nytte* for enkeltvirksomheter forvaltningen enkeltpersoner og næringsliv (se punkt 13.2). Utvalget legger til grunn at noen tjenester neppe kan tilbys elektronisk uten bruk av digitale signaturer eventuelt at tjenestene tilbys med dårligere sikkerhet/kvalitet. *Administrative* konsekvenser av innstillingene i utredningen er knyttet til nye eller endrede funksjoner og ansvarsområder både i de enkelte forvaltningsorganer og samordnet for hele eller deler av forvaltningen (se punkt 13.3). *Økonomiske* konsekvenser er et langt mer sammensatt bilde. Utvalget har ikke hatt mulighet for å gå ned i detaljene. For en del områder kan man bare hinte om retning for utvikling mens man i andre tilfeller kan kvantifisere økonomiske aspekter (se punkt 13.4).

13.2 Kvalitative betraktninger

13.2.1 Kost-/nyttevurderinger for bruk av PKI-teknologi

Nytteeffektene ved elektronisk saksbehandling og elektroniske tjenester er knyttet både til innsparinger for forvaltningen selv og for kommunikasjonspartnere og til bedre kvalitet på offentlige tjenester. Kvalitetsforbedringer er først og fremst knyttet til raskere saksbehandling og bedre tilgjengelighet uavhengig av sted og åpningstid. I mange tilfeller vil imidlertid elektroniske tjenester også innebære mindre risiko for feil f.eks. i datagrunnlaget for en saksavgjørelse.

Det er viktig å være klar over at digitale signaturer og PKI kun har verdi i den grad teknologien anvendes til konkrete formål. Digitale signaturer er heller ikke bare et sikkerhetstiltak men en teknologi som muliggjør nye elektroniske tjenester. Diskusjonene i punktene 13.4.2 og 13.4.4 gir en begrunnelse for dette synspunktet.

Elektroniske tjenestetilbud og elektronisk saksbehandling i offentlig sektor vil stille forskjellige krav avhengig av hva slags tjenester og saksbehandling det er snakk om. Et sentralt spørsmål som må vurderes i det enkelte konkrete tilfellet er behovet for digitale signaturer og meldingskryptering for elektroniske dokumenter.

Der det ikke er behov for signaturer kan det likevel være ønskelig å benytte PKI for å gi en sikker identifikasjon og autentisering av brukerne f.eks. ved bruk av en offentlig elektronisk tjeneste. Teknologien vil i tilfelle også beskytte kommunikasjonen mot innsyn og uautoriserte endringer gjennom kryptering.

Ett eksempel på kvalitetsforbedring knyttet til bruk av PKI er Skattedirektoratets tjeneste for forhåndsutfylt selvangivelse. Her har man til nå benyttet en PIN-kodebasert autentisering og ut fra sikkerhetsnivået i dette kan man tilby et visst utvalg av informasjon og operasjoner. Neste trinn operativt i pilotversjon våren 2001 er autentisering basert på PKI men ikke digitale signaturer. Dette gir økt sikkerhet og mulighet for mer personaliserte tjenester og økt utvalg av funksjoner og informasjon. Neste versjon vil også ta i bruk digitale signaturer og da vil man kunne tilby en fullstendig elektronisk selvangivelsestjeneste.

Innføring av elektroniske tjenester må gjøres etter kost-/nyttevurderinger og risikovurderinger der kostnadene og nytten av PKI-bruk ofte vil stå helt sentralt. Denne teknologien oppfattes i dag som kompleks og det betyr også at kostnadene kan være høye. Men som nevnt over kan nytteverdien i noen tilfeller være slik at tjenester ikke kan tilbys elektronisk uten bruk av denne teknologien f.eks. der det er krav om signaturer. Da må man se på gevinsten av at tjenestene kan tilbys elektronisk.

Det er også klart at dersom infrastruktur og brukere er på plass vil nye tjenester kunne basere seg på dette ut fra helt andre kost-/nyttevurderinger enn den situasjonen man vil ha initielt for de første eksemplene på tjenester som baserer seg på digitale signaturer.

Man bør vurdere:

- Økte kostnader mot andre muligheter som kan gi større nytte f.eks. tilgangen til alternative metoder og kostnader knyttet til disse.
- Økte kostnader ved at man må opprettholde to parallelle systemer ett papirbasert og ett elektronisk. Dette innbefatter å opprettholde kompetansen rundt manuelle rutiner som man kanskje ikke trenger i forbindelse med et elektronisk system.
- Om elektroniske transaksjoner kan påføre motparten utgifter. Høye kostnader kan innskrenke antall mulige brukere noe som i sin tur begrenser nytten ved elektronisk kommunikasjon.
- Utviklings- og vedlikeholdskostnadene ved elektronisk kommunikasjon.
- Om det er mulig å endre de underliggende rutinene rundt manuell saksbehandling slik at de kan automatiseres.

- Om hvordan teoretiske effektiviseringsgevinster ved overgangen til sikre elektroniske tjenester kan realiseres i praksis.
- Krav om signatur i forhold til gjeldende rett.
- Sedvane og innarbeidet praksis innenfor den aktuelle sektoren.

13.2.2 Risikoanalyse som element i en kost-/nyttevurdering

I en kost-/nyttevurdering er det sentralt å vurdere den risikoen for skade eller tap som kan oppstå ved bruk eller ikke-bruk av PKI.

Risikovurderinger må foretas der informasjonen regnes som sensitiv i en eller annen forstand for enkeltpersoner/bedrifter for saksbehandling og vedtak eller for virksomheten som sådan. Vurderingen skal identifisere teknikker og styringsmekanismer som best minimerer risikoer gir akseptable kostnader og maksimerer nytten for de involverte parter. Mye kan kvantifiseres men noen faktorer kan bare gis kvalitative estimater. Det kan f.eks. være vanskelig å bestemme verdien av preventive tiltak mot bedrageri.

Ved risikovurdering ser man på:

- Sannsynligheten for at skade/tap kan opptre
- Kostnadene ved potensiell skade
- Kostnadene ved å ta i bruk forebyggende sikringstiltak tiltak for å reparere eventuelle skader og kostnader ved ikke å gjøre noe.

De alternativene som etablerer et akseptabelt risikonivå bør uttrykkes som netto nytte for både forvaltningen og enkeltpersoner/bedrift. Hvis nytten er negativ kan forvaltningen bestemme at det foreløpig ikke er naturlig å ta i bruk elektronisk samhandling på det aktuelle området.

På den annen side er det ikke slik at enhver nyttevurdering avgjøres av en risikovurdering. Et tiltak kan godt ha negativ (eller positiv) nytte selv om risikoen er lik null. Netto nytte avgjøres av hvorvidt kostnadene er større eller mindre enn beregnet nytte.

En risikoanalyse vil alltid måtte koples med vurderinger i henhold til gjeldende lover og regelverk (f.eks. personvernhensyn) slik at sikkerhetsnivået er høyt nok til å tilfredsstille pålagte krav.

13.3 Administrative konsekvenser

13.3.1 Felles administrative konsekvenser

Etablerte ordninger

Noen felles administrative funksjoner er allerede på plass:

- Post- og teletilsynet er gjennom den nye loven og forskriften om elektroniske signaturer tillagt tilsyn med utstedere av kvalifiserte signaturer [52].
- Norsk Akkreditering har fått i oppdrag av Nærings- og handelsdepartementet å etablere en norsk ordning for akkreditering og sertifisering av informasjonssikkerhet i organisasjoner (jf. St.prp. nr. 1 (1989–99) Nærings- og handelsdepartementet). Sertifiseringsordningen og standarden BS 7799 er nærmere beskrevet av Norsk Akkreditering. Se på nettet: http://www.justervesenet.no/na/default.htm. Velg «informasjonssikkerhet». Ordningen kan delvis bidra til et grunnlag for tillit til den generelle informasjonssikkerheten hos f.eks. sertifikatutstedere men ikke for sikkerhet konkret knyttet til digitale signaturer mv.

- Forsvarets overkommando/Sikkerhetsstaben (FO/S) er gjennom vedtak i Stortinget etter forslag fra regjeringen (St.prp. nr. 1 (1989–99) Nærings- og handelsdepartementet) tillagt myndighet for sikkerhetsmessig sertifisering/godkjenning av IT-sikkerhet i produkter og systemer. Ordningen er rettet mot sivil sektor og basert på frivillighet. Det er ikke avklart om FO/S vil få noen oppgaver knyttet til godkjenning av sikre signaturframstillingssystemer.
- Norsk Teknologisenter har ansvaret for etablering av norske standarder innen de aktuelle områdene. Det arbeides for tiden (januar 2001) med oversettelse til norsk av en ny internasjonal standard (IS 17799) for informasjonssikkerhet i organisasjoner basert på den nevnte britiske standarden BS 7799 del I.
- Innkjøpsordning for sertifikater programvare for digitale signaturer og meldingskryptering smartkort og smartkortlesere er etablert i regi av Forvaltningsnettsamarbeidet – alle forvaltningsvirksomheter kan handle via disse rammeavtalene.

Foreslåtte ordninger

Denne utredningen konkluderer med at det er behov for å plassere ansvaret for koordinering av forvaltningens arbeid innen området digitale signaturer og PKI på ett sted. Utvalget foreslår etablering av en *samordningsfunksjon* i form av et permanent samordningsutvalg med et sekretariat jf. punkt 9.6. Dette er en ny rolle innen forvaltningen. Plasseringen av sekretariatet må avklares.

Samordningsfunksjonen vil ha overordnet ansvar for kvalitetskrav og sikkerhetskrav for løsninger internt i forvaltningen og på grenseflaten mellom forvaltningen og privat sektor (både virksomheter og privatpersoner). Den vil ha ansvaret for forvaltningens felles spesifikasjoner i samarbeid med de ansvarlige for anskaffelser og rammeavtaler som f.eks. Forvaltningsnettsamarbeidet og med tilsyns- og standardiseringsorganer.

Denne utredningen konkluderer også med at det bør være aktuelt å opprette et felles *Forum for digitale signaturer* for forvaltningen næringslivet og leverandører av sertifikattjenester. Samtrafikkspørsmål vil være spesielt viktige for et slikt forum.

Felles prosjekter anvendelser tjenester m.m.

I tillegg til prosjekter innen enkelte forvaltningsorganer er det flere eksempler på samarbeidsprosjekter som involverer flere forvaltningsvirksomheter bl.a. helsesektoren (f.eks. i regi av Rikstrygdeverket) felles innrapporteringsprosjekter (Skattedirektoratet Statistisk sentralbyrå og Brønnøysundregistrene) og andre. Det bør oppmuntres til flere slike samarbeidsprosjekter.

Det er identifisert et potensial for samarbeid om felles tjenester. Innen digitale signaturer og PKI gjelder dette særlig samtrafikktjenester for verifisering av sertifikater. Arbeid med samtrafikktjenester anbefales av denne utredningen mens det ikke anbefales å starte initiativer for sertifikatkataloger nå.

Statens forvaltningstjeneste/Statskjøp arbeider med etablering av en elektronisk markedsplass for forvaltningen. Det er et klart behov for digitale signaturer i en slik sammenheng og det er viktig at et koordinerende organ samarbeider med dette og liknende prosjekter f.eks. i sammenheng med Nærings- og handelsdepartementets satsning innen elektronisk handel.

Kompetanseoppbygging

IT-infrastrukturer kan være store og komplekse. For å forstå dem er det nyttig å se helheten og forstå sammenhengen mellom dem [31]. Den viktigste kompetansen er antakelig ikke knyttet til teknologien alene men til sammenhengene mellom teknologi og institusjonelle og sosiale strukturer i samfunnet. PKI er et del-område som både er komplekst og nytt. Store forandringer skjer raskt. I tillegg til at den foreslåtte samordningsfunksjonen skal ha en rolle og må ha gode kunnskaper om området er det slik at effektiv utnyttelse av PKI krever kompetanse i de enkelte forvaltningsorganene. Etablering av kurstilbud og andre kompetansebyggende tiltak vil være av stor betydning på PKI-området. Det vil være naturlig at bl.a.

Statskonsult som statens sentrale organ for kompetanseutvikling og opplæring engasjerer seg i dette og bygger opp tilbud i takt med de videre behovene på området.

En rekke forvaltningsorganer har meget god kompetanse. Utfordringene ligger også i å få disse miljøene til å samarbeide i størst mulig grad både med tanke på konkrete oppgaver og for kompetanseoppbygging og -utveksling. Den foreslåtte samordningsfunksjonen kan få et særlig ansvar for å holde oversikt over relevante kompetansemiljøer og -personer og for å stimulere til faglig kontakt.

Felles administrative konsekvenser vil også være knyttet til kontakt med samarbeidspartnere innen forskning og utvikling og kontakt med leverandører av produkter og tjenester. I tillegg kommer standardiseringsarbeid internasjonalt som må følges opp inkludert kontakter som må knyttes og vedlikeholdes mot relevante internasjonale samarbeidspartnere. Dette er en oppgave som må ivaretas av relevante standardiseringsorganisasjoner som Norsk teknologisenter og sekretariatet for IT-standardisering i forvaltningen hos Statskonsult og som kan kreve økte ressurser.

13.3.2 Administrative konsekvenser for forvaltningsorganer

Etablering av digitale signaturer og sertifikater

Dersom forvaltningsorganet selv og/eller grupper av ansatte skal ta i bruk digitale signaturer må forvaltningsorganet inngå avtale om kjøp og vedlikehold av nødvendig programvare og utstyr og avtale med en sertifikatutsteder. Det anbefales å basere dette på Forvaltningsnettsamarbeidets rammeavtaler.

For å få utstedt sertifikater må forvaltningsorganet ha oppnevnt en eller flere registreringsenheter/-steder. Dette vil vanligvis bli ivaretatt av personer internt i organisasjonen men det kan også være en fellesfunksjon for flere forvaltningsorganer. Men registreringsenheten må være lokal slik at personer som skal ha sertifikat kan få det ved et personlig frammøte med legitimering hos registreringsenheten. Personene som skal ha rollen som registreringsenhet må få utstyr og opplæring og må være godkjent av sertifikatutstederen. Dersom dette er eget personale vil det vanligvis være enten teknisk driftspersonale eller ansatte i personalavdelingen. Det er naturlig at funksjonen med registrering knyttes til personalavdelingen. Ansatte der må få opplæring særlig i den tekniske og sikkerhetsmessige delen av driften av en slik funksjon.

Bruk av digitale signaturer og meldingskryptering må reflekteres i virksomhetens sikkerhetspolicy. Det er naturlig med en gjennomgang av sikkerhetspolicyen ved innføring av denne teknologien. Dette bør spesielt innebære en gjennomgang av sikkerheten for de personene og tjenestene som skal bruke eller verifisere digitale signaturer. Merk at anbefalinger og regelverk fra bl.a. FO/S og Datatilsynet tilsier at hver virksomhet som bruker kryptografiske metoder skal utpeke en kryptoansvarlig med spesielt ansvar for dette området.

Bruk av digitale signaturer og sertifikater

Bruken av digitale signaturer og sertifikater isolert sett kan gjøres ganske enkel. Utfordringen er å få bruken inn i den rette sammenhengen ved elektronisk saksbehandling og kommunikasjon. Dette vil kreve god dokumentasjon av nye tilpassede rutiner fulgt av en endringsprosess for å ta disse rutinene i bruk. Det er sjelden formålstjenlig å overføre papirbaserte rutiner direkte til elektronisk samhandling.

Innføring av nye rutiner kan medføre nye roller og funksjoner og dette kan innebære til dels store administrative konsekvenser avhengig av i hvor stor grad eksisterende rutiner må endres. Eksempler er spesielt knyttet til drift og administrasjon av tjenester som elektronisk postmottak og elektronisk arkiv.

Utvikling av nye elektroniske tjenester eller tilpasning av eksisterende tjenester til bruk av digitale signaturer vil kunne medføre endrede driftsrutiner.

Kompetanseoppbygging

Innen de enkelte forvaltningsorganene er det flere typer ansatte som trenger spesiell kompetanseoppbygging. Dette gjelder selvfølgelig brukerne som må vite hvordan de skal bruke f.eks. smartkort og programvare og hvilke rutiner som gjelder for elektronisk saksbehandling og kommunikasjon. Endrede rutiner vil kunne medføre et betydelig behov for opplæring. Dette vil være en nødvendig konsekvens ved overgang til elektronisk kommunikasjon.

Det anbefales at det blir utarbeidet et kursopplegg basert på de kursene som allerede tilbys innen området. Merk at sertifikatutstedere og programvareleverandører som har rammeavtale under Forvaltningsnettsamarbeidet er forpliktet til å tilby kurs for brukere til sine kunder.

Rollen som registreringsenhet er viktig og den krever spesiell opplæring. Både utstyr og opplæring for personer som skal fylle rollen som registreringsenhet/sted skal være en del av avtaler om kjøp av sertifikattjenester under Forvaltningsnettsamarbeidets rammeavtaler.

Driftspersonale i forvaltningsorganet vil trenge opplæring relatert til installasjon drift og vedlikehold av programvare og utstyr (som smartkortlesere). Driftspersonale må også vite hvilke spesielle sikkerhetskrav som eventuelt gjelder knyttet til bruk av digitale signaturer og meldingskryptering. Leverandører innen Forvaltningsnettsamarbeidet er forpliktet til å gi slik opplæring til sine kunder men det anbefales at Statskonsult eller andre også utarbeider driftskurs.

13.4 Økonomiske konsekvenser

Grovt sett er elementene i en økonomisk analyse disse:

- Utgifter knyttet til innføring av en felles PKI
- Utgifter knyttet til integrering av digitale signaturer m.m. i eksisterende og nye systemer
- Økonomiske besparelser knyttet til en slik innføring.

Dette kan til en viss grad settes opp mot:

- Kostnader ved eventuelle alternative metoder for å oppnå de samme målene.

13.4.1 Kostnader for administrative tiltak

Fellesadministrative tiltak

Følgende administrative kostnadselementer kan forutsees. Det gjøres ikke noe forsøk her på å kvantifisere disse punktene:

- Kostnader knyttet til den foreslåtte samordningsfunksjonen og til forvaltningens andel av andre koordineringstiltak som felles erfaringsforum for forvaltningsorganer næringsliv og leverandører
- Kostnader knyttet til spesifikasjonsarbeid avtaleverk administrasjon m.m. av felles innkjøpsordninger (Forvaltningsnettsamarbeidet)
- Kostnader knyttet til internasjonal koordinering
- Kostnader knyttet til utvikling og gjennomføring av kompetansehevende tiltak – disse kostnadene kan til en viss grad skyves over på de enkelte forvaltningsorganer gjennom deltakeravgifter o.l.
- Kostnader i form av særskilte midler satt av til stimuleringstiltak som det kan tildeles penger fra for å stimulere utviklingen på viktige områder for fellesskapet.

Det er stipulert at samordningsfunksjonen bør kunne tilføres 1–2 årsverk til sekretariatet med et driftsbudsjett på totalt kr 6 5 mill. i det første driftsåret (2001). Det stipuleres at hver av samordningsutvalgets medlemmer vil trenge å nedlegge 2 månedsverk årlig til arbeidet. Mer ressurser vil kreves av den som skal lede utvalget. Videre foreslår utvalget at stimuleringsmidlene som tildeles blir på kr 9 mill. og at de administreres av samordningsfunksjonen/-utvalget. Til sammen utgjør dette altså et forslag om å bevilge kr 15 5 mill. over statsbudsjettet for å fremme det utvalget anser som nødvendige løsninger

for å få til elektronisk døgnåpen forvaltning på en forsvarlig måte i løpet av 2003 som er den tidsfristen som er satt av regjeringen.

Administrative tiltak i de enkelte forvaltningsorganer

Gjennomgang og endring av rutiner for saksbehandling og kommunikasjon kan være et meget komplisert og kostnadskrevende arbeid men er nødvendig for å kunne ta ut gevinstene som følger av bruk av elektronisk kommunikasjon og digitale signaturer. Kompleksiteten i dette vil variere sterkt fra forvaltningsorgan til forvaltningsorgan.

Det skal normalt ikke kreves mye ekstra ressurser i en driftsfase i forhold til i en situasjon uten bruk av digitale signaturer. Noe ekstra ansvar vil falle på driftspersonale spesielt knyttet til planarbeid og tiltak i organisasjonen herunder ansvaret for informasjonssikkerhet sikkerhetsfunksjoner og PKI. En rolle som registreringsenhet vil normalt ikke medføre mye ekstra arbeid men dette avhenger selvfølgelig av virksomhetens størrelse antallet personer som skal ha sertifikater og hvor hyppig det skal skje.

Opplæring av brukere og kompetanseoppbygging generelt kan medføre en god del kostnader.

13.4.2 Kostnader ved tilrettelegging av PKI for forvaltningen

Følgende kostnadselementer kan identifiseres for forvaltningen utover de mer administrative kostnadene som er nevnt over:

- Innkjøp vedlikehold og bruk av sertifikater programvare og utstyr (smartkort og kortlesere m.m.) for forvaltningen selv
- Eventuell støtte til etablering av felles tjenester f.eks. samtrafikktjeneste og kataloger
- Eventuell støtte til sertifikatutstedere for å få etablert tjenester som er i henhold til forvaltningens behov – se nedenfor.
- Kostnader for den enkelte virksomhet i forbindelse med bruk av sertifikater utstedt av markedsaktører.

Det siste elementet vil utgjøre en utgift knyttet til felles funksjoner og kan vurderes i tilknytning til administrative kostnader som diskutert over.

Det finnes et visst grunnlagsmateriale for kalkulasjon av kostnader knyttet til kjøp og drift av teknologien. Dette kan baseres på cirkapriser oppgitt av leverandører fra maksimumspriser gitt i rammeavtalene i Forvaltningsnettsamarbeidet og på beregninger gjort av svenske myndigheter [32]. En generell betraktning er at to elementer er av meget stor betydning for prisene:

- Antall sertifikater som blir utstedt og antall programvarelisenser smartkort etc.
- Antall tjenester som sertifikater kan brukes mot og volum for trafikken mot disse tjenestene.

En sertifikattjeneste på kommersielt grunnlag er meget kostbar å etablere og relativt kostbar i drift. Dersom tjenesten bare skal utstede et fåtall sertifikater blir kostnadene per sertifikat store. Samtidig er markedet neppe villig til å betale en høy pris for sertifikater smartkort m.m.

Potensial for økonomisk gevinst for tjenesteleverandørene ligger derfor ikke i selve PKI-tjenesten men i inntekter fra nye tjenester som blir muliggjort (ev. kvalitetsmessig forbedret) ved bruk av PKI og digitale signaturer. Kostnader ved sertifikatutstedelse må i stor grad kompenseres ved inntjening gjennom tjenestetilbud og dette forutsetter at sertifikatutstederen selv driver disse tjenestene eller har avtaler med tjenestetilbydere som sikrer en viss økonomisk kompensasjon. Sertifikatutstedere kan også ha betalingsmodeller som er delvis basert på avgift for bruk av nøkler og sertifikater og da blir volumet av bruken viktig.

Det er faktisk grunnlag for å påstå at sertifikatutstedere i Norge må kalkulere med å tape penger på sertifikattjenesten isolert sett gitt de prisene som man kan forvente at markedet vil akseptere for sertifikater

og det volumet man kan forvente i Norge. Inntektene kommer fra andre tjenester. Et eksempel på dette er bankene der BankID kan være et virkemiddel for å få på plass inntektsbringende elektroniske banktjenester.

For forvaltningen er dette enda et argument for å basere seg på tjenester kjøpt fra aktører i markedet. Forvaltningens egne elektroniske tjenester kan være en selvstendig grunn til å skaffe seg sertifikater m.m. Men muligheten for tilgang til slike tjenester kan være et meget godt tilleggsargument overfor brukere som kanskje primært skaffer seg sertifikater for å få adgang til f.eks. banktjenester. Dette vil kunne føre til bedre økonomiske betingelser for forvaltningen enn man vil oppnå ved å etablere en egen sertifikattjeneste.

Med en løsning der sertifikater m.m. kjøpes i markedet av alle aktører er forvaltningens kostnader i utgangspunktet knyttet til eget innkjøp av sertifikater programvare smartkort og kortlesere.

Prisene vil være sterkt avhengig av volum men en pris på ca. 1000 kr per installasjon virker sannsynlig (kortleser kort og sertifikat). Sertifikater vil normalt bli byttet annethvert år mens smartkort kan ha en levetid på to sertifikatperioder altså fire år. Iberegnet en årlig avgift for sertifikater og vedlikeholdskostnader for programvare kan man regne en pris på ca. 2000 kr over en fireårsperiode. Ved store volumer må man som i andre sammenhenger kunne regne med rabatter fra leverandørene med fallende priser jo større volumer som kjøpes. Flere leverandører har slike volumprisingsskjemaer.

Etter denne perioden vil brukerne trenge nye smartkort og man kan påregne oppgradering av programvare m.m. Man kan da regne med en ny fireårssyklus antakelig med lavere kostnader under forutsetning av at PKI-teknologi har blitt massemarkedprodukter på dette tidspunktet.

Trykking/preging av kort som fysiske identitetsbevis multifunksjonelle kort (flere applikasjoner enn elektronisk ID i samme kort) og brukerstøtte m.m. er ikke med i denne beregningen.

Gitt et visst volum for forvaltningens innkjøp er det lite trolig at prisene vil bli særlig høyere enn antydet og med et gjennomslag for PKI-teknologi i markedet kan prisene godt bli lavere.

Alternative teknologier til smartkort som kan tenkes benyttet på egnede områder i forvaltningen har prisantydninger som går ut på at dersom en elektronisk ID legges integrert med programvaren for nettlesere vil prisen bli ca. 40 % lavere. Elektronisk ID i mobiltelefon (dvs. bruk av SIM-kortet for lagring av nøkler) kan komme som produkt allerede i løpet av 2001 og man antar at prisen vil være ca. 20 % lavere enn for smartkort. Men slike ID vil ha begrenset funksjonalitet i forhold til signering av dokumenter.

Pris per transaksjon ved bruk av digitale signaturer er vanskelig å estimere. Noen leverandører antyder at de vil forsøke en prismodell der det avregnes for bruk av sertifikater og nøkler. Prising for dette er ikke klar. Prosessering av transaksjoner *med* digitale signaturer er mer komplisert og kostnadskrevende enn uten bl.a. kreves sjekk for tilbaketrekking. Svenske estimater sier 5 kr per transaksjon men dette virker høyt. Kr 2 50 virker som et mer reelt estimat.

Når det gjelder sertifikater programvare og smartkort for aktører i privat sektor (næringsliv og privatpersoner) vil dette i utgangspunktet måtte kjøpes av disse aktørene i markedet. Man skal imidlertid være oppmerksom på at forvaltningen vil være avhengig av at de tilgjengelige tjenestene holder et visst nivå. Det vil også påløpe kostnader for systemintegrasjon for bruk av digitale signaturer.

Integrasjon av programvare for digitale signaturer er en potensielt komplisert oppgave. Det må derfor være et mål for forvaltningen å utarbeide felles spesifikasjoner som gjør at graden av «skreddersøm» for hver enkelt tjeneste og programvareintegrasjon blir minst mulig.

Mye av problematikken her er knyttet til samtrafikk og håndtering av sertifikater fra forskjellige utstedere. Standarder for sertifikatformater og løsninger som gjør at man slipper å gjøre individuelle tilpasninger i hver enkelt tjeneste for å kunne akseptere sertifikater fra forskjellige utstedere er viktig. Samtrafikktjenester kan være et viktig virkemiddel.

Leverandørene til Forvaltningsnettsamarbeidets rammeavtaler kan allerede i dag levere integrasjon av digitale signaturer med et godt utvalg av brukerprogramvare. Framtidige spesifikasjoner må fokusere på hva behovene er for forvaltningens brukere og sørge for at de nødvendige integrasjonene er tilgjengelige i markedet. Man bør være oppmerksom på at det er ganske stor sannsynlighet for at man vil være nødt til å kjøpe programvaren for digital signatur og kryptering fra samme leverandør som man har valgt som sertifikatutsteder men det finnes også eksempler på generell programvare som kan håndtere forskjellige typer sertifikater og smartkort.

Kostnader knyttet til systemintegrasjon kvantifiseres ikke her. Dette er utviklingskostnader som sannsynligvis vil bli relativt høye dersom slik integrasjon skal gjennomføres for hver enkelt offentlige virksomhet.

13.4.3 Kostnader ved alternative metoder

Det finnes i dag ikke alternative standardiserte teknologier som dekker funksjonaliteten knyttet til digitale signaturer og PKI [66]. Mulige alternativer er avgrensede spesialtilpassede løsninger. For de første tjenestene/anvendelsene for digitale signaturer og PKI som blir introdusert vil nok kostnadene isolert sett øke ved at man samtidig arbeider i retning av en generell infrastruktur istedenfor å finne en løsning for en enkelttjeneste. Med det omfanget bruken av digitale signaturer antas å få i løpet av noen ganske få år skulle det likevel være rimelig klart at isolerte løsninger er lite formålstjenlige. Det vil innebære at brukerne må skaffe seg en elektronisk ID for hver tjeneste som skal benyttes.

For autentisering – der det ikke er eksplisitt behov for signaturer – kan man basere seg på passord fra statiske passord/PIN-koder til forskjellige former for engangspassord lik det som brukes i dagens nettbanker. De beste systemene for engangspassord gir nok en like sikker autentisering som PKI-baserte metoder og de understøtter mobilitet. Erfaringer viser at slike løsninger er relativt kostbare. Dessuten er problemet at brukerne blir nødt til å skaffe seg et slikt system for hver tjeneste eventuelt huske et passord for hver tjeneste. Dette blir fort uhåndterlig særlig når man ser på totalbildet for offentlige og private tjenester.

En ser at kostnadene ved administrasjon av slike løsninger fort kan bli meget høye i tillegg til at kompleksiteten gir økt mulighet for feil. Passordbaserte løsninger skalerer rett og slett ikke til en kombinasjon av mange tjenester og mange brukere. På samme måte skalerer heller ikke løsninger som baserer seg på PKI dersom PKI innføres uten samordning.

13.4.4 Potensial for reduserte kostnader

Gevinstpotensialet for elektroniske tjenester og elektronisk saksbehandling er åpenbart og argumentene skal ikke gjengis her. Spørsmålet som knytter seg til bruk av digitale signaturer og sertifikater er da hvilket gevinstpotensial dette gir for elektroniske tjenester som ikke vil kunne tas ut uten anvendelse av PKI.

Denne utredningen peker på at det finnes tjenester som ikke bør tilbys elektronisk uten digitale signaturer og i andre tilfeller er det snakk om vesentlige kvalitetsmessige forbedringer for tjenester knyttet til bruk av digitale signaturer. Utredningen grunngir at disse argumentene er vesentlige nok til at de rettferdiggjør de kostnadene som er beskrevet i de foregående avsnittene.

Et viktig problem i forhold til bruk av PKI er den langsomme takten for å ta i bruk PKI. Utbredelsen av konkrete løsninger har foreløpig gått langsomt. Elektroniske offentlige tjenester er avhengig av et visst volum når det gjelder bruk for å være kostnadseffektive. Innsparingene gjennom mer effektiv (elektronisk) behandling og mindre volum på manuelle rutiner rundt papirhåndtering må overstige kostnadene ved å tilby tjenesten elektronisk. Antallet sertifikateiere både internt i offentlig forvaltning i næringslivet og blant privatpersoner er i dag lite. Men nå er det stort fokus på PKI og digitale signaturer både i Norge og internasjonalt. Det forventes en stor økning i antallet brukere etter hvert som teknologien gir tilgang til stadig flere og mer avanserte elektroniske tjenester. Ett eksempel er bankenes satsning basert på endringene i finansavtaleloven som nå muliggjør elektronisk avtaleinngåelse og langt mer avanserte elektroniske banktjenester enn vi har sett til nå. Elektroniske tjenester tilbudt fra det offentlige kan gi større etterspørsel etter sertifikattjenester. En del offentlige institusjoner er langt framme f.eks. skatteetaten og Rikstrygdeverket. For offentlige tjenester blir dette også et spørsmål om å gripe anledningen i forhold til antallet brukere som kan oppnås på kort sikt.

Utvalget gjør ikke noe forsøk på å kvantifisere potensialet for reduserte kostnader knyttet til tilgjengeliggjøring av nye elektroniske tjenester og kvalitetsforbedringer av andre tjenester som krever digitale signaturer. Dette hører med til gevinster knyttet til innføring av døgnåpen forvaltning. Det legges til grunn at det finnes et slikt potensial av et ikke ubetydelig omfang. Det legges også til grunn at i henhold til politiske målsettinger skal forvaltningen fornyes og effektiviseres innen rimelig kort tid (jf. Fornyelsesprogrammet eNorge-planen døgnåpen forvaltning mv.) og at det må gjøres på en forsvarlig og kostnadseffektiv måte. Det er i denne sammenhengen utvalgets forslag fremmes.

13.5 Forslag som ikke koster noe?

En variant av temaet i forrige punkt er å se på muligheten for å fremme forslag om tiltak som ikke koster noe i kroner og øre (i hvert fall ikke i første omgang). En rekke av utvalgets forslag knytter det seg ikke direkte kostnader til. De er anbefalinger som den enkelte virksomhet person eller bedrift kan velge å følge eller ikke. Konsekvenser av slike anbefalinger er vanskelige å tallfeste. Men det er lett å tenke seg at de representerer en type tilrettelegging som vil fungere kostnadsbesparende fordi den enkelte virksomhet kan benytte seg av løsninger som er gjennomtenkt på kompetent sentralt hold framfor å måtte «finne opp hjulet» hver for seg.

En annen mulighet er å tenke seg innføring og bruk av PKI-løsninger med og i forvaltningen som foregår uten å koordinere eller tilrettelegge i det hele tatt. Dette vil sannsynligvis føre til innføring og bruk ut fra den enkelte virksomhets egen tenkning og tilrettelegging. De største etatene har nok ressurser til å gjøre dette men de mellomstore og små vil neppe være i stand til det. Etter en stund vil det vokse fram PKI-områder for enkeltvirksomheter kanskje for hele sektorer sannsynligvis med større ulikhet i valg av løsninger mindre i stand til samhandling. De kan tenkes å fungere tilfredsstillende en stund men det er grunn til å tro at nytteeffekten blir mindre over tid ettersom hindringene for samhandling blir mer synlige og problematiske. Det vil sannsynligvis være mer kostnads- og ressurskrevende for den enkelte virksomhet å stå for alt som skal til for å få digitale signaturer (eller alternative løsninger) og kryptering til å fungere uten de fellestiltakene og den tilretteleggingen utvalget foreslår. Den samlede utgiften ved innføring av sikker elektronisk døgnåpen forvaltning vil sannsynligvis bli betydelig høyere for hele forvaltningen.

Vedlegg 1

Aktuelle prosjekter tilknyttet forvaltningen

For å kunne foreslå hvordan ansvar for utstedelse og administrasjon av forvaltningens sertifikater bør organiseres er det ønskelig med en kartlegging av forvaltningens behov.

Følgende spørsmål bør belyses for systemer/applikasjoner som trenger sikkerhet for å gi enkeltpersoner tilgang over Internett:

- Risiko- og kost-/nytteanalyse for å gjøre applikasjonen tilgjengelig via Internett
- Applikasjonens krav til sikkerhet (f.eks. lovpålegg om underskrift identifisering av bruker konfidensialitet) og nivå for sikkerheten (myke eller harde sertifikater krav til identifisering)
- Brukerkategorier f.eks. tilgang for hele befolkningen grupper av enkeltpersoner bedrifter eller bare for ansatte
- Hvilke risikoer utsettes brukerne for
- Transaksjonsvolumer transaksjonstyper (enkelttransaksjoner eller hele filer) og fordeling over året
- Finansiering av applikasjonen
- Den nåværende sikkerhetsløsningen
- Tidsplan for igangsetting av den elektroniske applikasjonen
- Forvaltningsenhetens behov for tilgang til informasjon fra andre deler av forvaltningen
- Enhetens behov for tjenester/service fra en sertifikatutsteder hva enheten ønsker å utføre selv.

Nedenfor følger informasjon om prosjekter i tilknytning til offentlig forvaltning som på ulike måter har behov for sikker elektronisk kommunikasjon. De fleste trenger digitale signaturer men ikke alle. I tillegg trenger de fleste andre typer sikkerhetstjenester. Til sammen sier det noe om hva slags sikkerhetsnivåer og sertifikattyper det er behov for.

1.1 Offentlig innkjøp

Når det offentlige står for innkjøp av varer og tjenester er det i motsetning til i næringslivet en del overordnede prinsipper som må ivaretas:

- Åpenhet – kunngjøring og elektronisk informasjon må være tilgjengelig for hele verden
- Lik adgang – alle må i prinsippet kunne inngi tilbud uavhengig av sitt teknologiske nivå
- Likebehandling av tilbyderne – elektroniske systemer må være tilstrekkelig generelle og utbredte slik at alle leverandører lett kan knytte seg til
- Ikke-diskriminerende – elektroniske dokumenter og standarder må være kjent for alle.

Elektronisk handel skal generelt redusere transaksjonskostnadene i innkjøpsprosessen. Det offentlige har en forholdsvis høy transaksjonskostnad i forhold til næringslivet på bakgrunn av ovennevnte krav. Imidlertid bidrar systemer for elektronisk handel til rimeligere datafangst og bedre datagrunnlag for å

oppnå kostnads- og konkurransefordeler. Elektronisk handel er i det offentliges øyne ikke ett system eller én fastlagt serie med aktiviteter. Det er dels alternative virkemidler for å håndtere store volumer basert på EDI/EDIFACT dels komplekse anskaffelser med kravspesifikasjoner publisert på web.

For dem som leverer inn tilbud er konfidensialitet viktig og de må også være trygge på at bare de tilbudene som var levert på rett måte er med i konkurransen. Dette må det være mulig å kontrollere (i dag er det gjerne offentlig anbudsåpning av papirkonvoluttene).

Behov: Konfidensialitet (fram til åpning også for mottaker) integritet levering til rett tid sikring mot lesing før et bestemt tidspunkt ikke-benekting av sending og mottak bekreftelse på mottak tidsstempling ved sending.

Arbeids- og administrasjonsdepartementet (AAD) planlegger et eget program for elektronisk handel ved offentlige innkjøp som vil forfølge slike sentrale problemstillinger. Se http://ehandel.dep.no/. Her ligger det mye nyttig informasjon om offentlig innkjøp og programmets strategiske satsning. Når det gjelder etablering av en markedsplass heter det her bl.a.:

Hovedhensikten med å etablere en markedsplass er fra Programmets side å gi virksomheter i det offentlige tilgang til et hjelpemiddel for å implementere egen forsyningsstrategi og å etablere et redskap for å kunne realisere direkte og indirekte besparelser muliggjort ved elektronisk handel. Direkte besparelser kan eksempelvis oppnås gjennom høyere omsetningsvolumer på inngåtte rammeavtaler ved at informasjon om avtalene og mulighet til å bestille fra disse spres til relevante brukere mens indirekte besparelser eksempelvis kan oppnås gjennom forbedringer av innkjøpsrutiner elektronisk behandling av informasjon gjennom hele handelsprosessen og enklere tilgang til informasjon om leverandører og deres produkter ved kvalifisering.

Norsk Hydro Norske Skog Orkla Statoil og det offentlige har sammen med andre virksomheter et sammenfallende behov for tilgang til en velfungerende transaksjonsplattform for å kunne drive elektronisk handel på en effektiv måte. Det er vesentlig at en slik transaksjonsplattform er åpen for alle aktører – både kjøpere og selgere – som ønsker å benytte den og at kostnadene og den teknologiske terskelen for tilknytning og bruk ikke er for høye.

Ved å inngå et samarbeid om etablering av en regional horisontal markedsplass gis både det offentlige og næringslivet tilgang til en enhetlig løsning for å drive elektronisk handel. På denne måten reduseres kjøpernes og leverandørenes kostnader ved å ta i bruk elektronisk handel betydelig. Samtidig vil en slik løsning kunne gi store nok volumer til at en slik markedsplass sikres en kostnadseffektiv og lønnsom drift.

Det vil være opp til den enkelte samarbeidspartner å avgjøre hvilke sluttbrukerapplikasjoner de vil benytte mot markedsplassen. Programmet vil på vegne av det offentlige inngå rammeavtale med én eller flere aktører om tilgang til sluttbrukerapplikasjoner.

Norsk Hydro Norske Skog Orkla Statoil og Programmet vil gjennom en felles prosjektgruppe se nærmere på om det er grunnlag for en felles etablering av en regional horisontal markedsplass i løpet av januar 2001. Herunder skal videre framdrift planlegges. Målet er en rask etablering av markedsplassen og for det offentlige tas det sikte på at markedsplassen og relevante sluttbrukerapplikasjoner skal være tilgjengelige for allmenn bruk innen utgangen av 2001.

På dette tidspunktet er det ikke avklart i hvilken grad dette fellesprosjektet også tar sikte på å levere sikre betalingsløsninger osv.

1.2 Handel

Når det gjelder de overordnede målsettinger og prioriteringer for e-handel vises det til St.meld. nr. 41 1998–99 *Om elektronisk handel og forretningsdrift* [58]. I kapittel 5 beskrives og forklares betydningen av elektroniske signaturer. Arbeidet med elektroniske signaturer er også forankret i regjeringens handlingsplan *eNorge 2.0* (kap. 3 e-handel og kommunikasjon) [21] hvor det heter at sikkerhet og tillit i kommunikasjonsnettene er viktig og ett av tiltakene er at det skal «gjennomføres en informasjonskampanje om e-signaturer …» jf. punkt 1.3.15.

Statssekretærutvalget for IT satte problemstillingen på dagsordenen høsten 1998. «Fellesforum for elektronisk handel» er etablert av Nærings- og handelsdepartementet og består av interesseorganisasjoner offentlige etater og enkeltbedrifter. Fellesforumets nettsted http://www.handel.no ble «åpnet» av

statsminister Stoltenberg 11. des. 2000. Fellesforumet skal med sitt nettsted virke som en møteplass for myndigheter næringslivsaktører interesseorganisasjoner og virkemiddelapparatet. Nettstedet handel.no skal være en informasjons- og kunnskapskanal med målsetting om å fremme elektronisk handel og elektronisk forretningsdrift. Næringslivet inviteres til å bidra med artikler osv.

Elektronisk handel er gitt stor oppmerksomhet i flere internasjonale fora bl.a. OECD EU/EØS WTO og FN. Med unntak av noen sentrale arbeider i regi av FN deltar Norge aktivt i det internasjonale arbeidet som tar sikte på å få til gode rammebetingelser et klart regelverk og en hensiktsmessig regulering av handelen over nettet.

I tillegg fokuseres det på elektronisk handel i bransjer nasjoner regioner og standardiseringsorganisasjoner. Blant nasjonene finner vi USA Canada Japan Singapore Malaysia og Australia. En sentral region for forvaltningen er Europa med EU. En viktig kommunikasjon i denne sammenhengen datert 16.4.1997 fra Kommisjonen til Rådet og Parlamentet er *A European Initiative in Electronic Commerce* COM(97)157. Dette er den første policyuttalelsen fra Kommisjonen der bruken av kryptering og digitale signaturer i forbindelse med elektronisk handel er et sentralt tema. Se til orientering web-siden til EU med oversikt over område 47. Dette er en innfallsport til en nærmest overveldende mengde informasjon som fortløpende ajourføres om ulike initiativer både i EU og i resten av verden.

Elektroniske signaturer og autentisering er og vil i tiden framover være viktig på e-handelområdet. Det vises i den forbindelse til det store antallet i befolkningen som nå tar i bruk nettbanker. Med innføring av e-giro forventes det at omfanget vil øke ytterligere.

1.3 Kommunal- og regionaldepartementet – pilotprosjektet EDNA

Kommunal- og regionaldepartementet og Husbanken gjennomførte pilotprosjektet EDNA – Elektronisk Dokumentutveksling i Norsk Administrasjon.

Pilotprosjektet ble igangsatt i 1995/96 med utgangspunkt i eksisterende edb-systemer og med krav om å overholde gjeldende rammer og regler for saksbehandlingen i forvaltningen. Det var praktisk bruk av digitale signaturer kryptering og TTP-tjeneste som var de sentrale målene. Disse sikkerhetstiltakene ble ansett som nødvendige å prøve ut for på sikt å kunne gå over fra papirbasert til elektronisk basert kommunikasjon og saksbehandling på generell basis.

EDNA var et pionerprosjekt på forvaltningsområdet ikke bare i nasjonal men også i internasjonal sammenheng. Det ble etablert helt konkrete operative løsninger for å ivareta krav til signatur konfidensialitet og arkivering ut fra de formulerte forvaltnings- og sikkerhetsbehovene samt krav til leverandøruavhengighet. Løsningene og erfaringene fra dette prosjektet har klar eksempel- og overføringsverdi for offentlig sektor. Dette var løsninger for å ivareta sentrale sikkerhetsfunksjoner ikke et elektronisk saksbehandlingssystem som sådant. I et framtidig elektronisk saksbehandlingssystem må slike sikkerhetsfunksjoner som ble utprøvd i praktisk bruk være integrert.

Behov: Meldingsintegritet autentisering av opphav konfidensialitet.

1.4 Innrapportering til kommune og stat – KOSTRA

Rutinene for informasjonsutveksling mellom kommunene/fylkeskommunene og staten skal effektiviseres gjennom elektronisk rapportering. KOSTRA-prosjektet (KOmmuneSTatRApportering) skal sikre en struktur og et innhold i kommunenes og fylkeskommunenes rapportering av regnskaps- og tjenesteproduksjonsdata som gir relevant styringsinformasjon og muligheter til sammenlikninger mellom kommuner og fylkeskommuner.

Det stilles krav om kryptering av individbasert informasjon innenfor rapportering av data fra helse- og sosialsektoren. Det er så langt ikke stilt krav til integritets- eller autentiseringsmekanismer for rapporteringen. Dette er krav som muligens vil kunne bli stilt dersom rapporteringsomfanget øker eller deler av det som rapporteres skal rapporteres til flere enn Statistisk sentralbyrå (SSB) som er eneste mottaker av rapporterte data pr. i dag. Prosjektet som ledes av Kommunal- og regionaldepartementet (KRD) er ferdig ved rapporteringen for året 2001 dvs. i februar 2002. Da går det over i vanlig driftsfase.

Behov: Konfidensialitet.

1.5 Skattedirektoratet og elektroniske signaturer

Skattedirektoratet har i flere år arbeidet med å etablere forskjellige løsninger for elektronisk innrapportering og elektronisk samhandling med skatteyterne.

De har løsninger for selvangivelsen (PSA) merverdiavgiftsoppgaven (MVA 3) skattekort og næringsoppgaver til SLN hvor ulike sikkerhetsløsninger benyttes. Funksjonaliteten i løsningene begrenses av hvilke sikkerhetsløsninger som er tilgjengelige i markedet.

Skattedirektoratet har i en EDI-løsning allerede tatt i bruk PKI med bruk av smartkort med to nøkkelpar. Dette har vist seg umodent og tungt å installere men må være målsettingen for arbeidet som gjøres i årene som kommer.

Bortsett fra EDI-løsningen hvor det benyttes digitale signaturer har Skattedirektoratet fokusert mest på krypterings- og autentiseringsutfordringene. For at de skal kunne tilby fullverdige løsninger hvor «alt» kan vises og gjøres på Internett må både kryptering autentisering og signering være mulig. Sporbarhet og ikke-benekting er to andre viktige elementer i våre løsninger. Dette stiller ikke bare krav til PKI-løsningen men også til logging i f.eks. en juridisk logg.

Skattedirektoratet ser det som en klar fordel at man i en nasjonal infrastruktur for nøkkelhåndtering har så få aktører at det er overkommelig for applikasjonsleverandørene å tilpasse seg alle løsningene som er godkjent i det norske markedet.

De ser det å ta i bruk PKI-løsninger med sertifikater lagret i arbeidsstasjon eller server som et skritt i riktig retning og som en mulighet til å lære befolkningen hva dette er. Så kan smartkort-løsningene følge etter og gi ytterligere sikkerhet og dermed mulighet for ytterligere funksjonalitet i løsningene når disse er modne. Det bør helst ikke ta for lang tid for da vil direktoratets systemer måtte stoppe opp i sin utvikling for å vente på sikkerhetsløsningene.

1.6 Innrapportering til og i det offentlige mv.

Statskonsult har i sin rapport *Elektronisk datautveksling og innrapportering* 1998:15 gitt en generell oversikt over området og innføring i problemstillingene.

Skattedirektoratets seneste anbudsinnbydelse ELEKTRA har til hensikt å styrke skatteetatens service overfor næringslivet. Det pågår flere større utviklingsprosjekter for overlevering av oppgaver som hver for seg vil gi positive nytteeffekter:

- System for likning av næringsdrivende (SLN)
- Nytt forvaltningssystem for merverdiavgiften (MVA3)
- Forhåndsutfylt selvangivelse (PSA)
- Grunnlagsdata oppgaver fra tredjemann (GRLD)

Krav til autentisering må ivaretas der det ikke brukes digitale signaturer. Dessuten må kravet til full sporbarhet/ikke-benekting møtes. Krav til konfidensialitet må også møtes for graderte opplysninger. En formidlingssentral vil være ansvarlig for nøkkeladministrasjon for de som benytter digitale signaturer og krever at den tilpasses en nasjonal infrastruktur når denne er på plass. Skattedirektoratet ønsker ett sikkerhetssystem for alle prosjekter med innrapportering og ber en formidlingssentral om støtte. Når både signering og kryptering utføres er det den signerte meldingen som krypteres. Når samme part både signerer melding og mottar kryptert melding skal det benyttes forskjellige nøkkelpar for de to funksjonene.

Når andre algoritmer benyttes velges nøkkellengder som gir tilsvarende grad av sikkerhet. Det stilles også krav til bruk av kryptografiske løsninger.

Behov: Autentisering og meldingsintegritet sporbarhet og ikke-benekting tidsstempling logging og konfidensialitet.

1.7 Brønnøysundregistrene

Når det gjelder innrapportering til Brønnøysundregistrene gjelder det offentlig tilgjengelig informasjon (regnskap) som ikke er konfidensiell. Her er det derimot krav om signatur og ofte flere enn en signatur.

1.7.1 Nettbasert Registrering

Prosjektet skal utvikles av NRD (Norway Registers Development AS) og BR (Brønnøysundregistrene) med støtte fra SND (Statens nærings- og distriktsutviklingsfond). Utviklingen skal starte i første kvartal 2001 og avsluttes i august 2001.

Utviklingsprosjektet skal realisere en nettbasert registreringsapplikasjon som skal være tilgjengelig fra en web-browser der man kan registrere endre og slette data i Enhetsregisteret og Foretaksregisteret. Systemet skal bygges opp slik at det i ettertid er mulig å benytte moduler fra systemet i andre eksterne saksbehandlersystemer og «blankettutfyllingssystemer». Meldingsflyten skal realiseres så generelt at meldinger skal kunne sendes til andre interne og eksterne «registersystemer».

Informasjonen som sendes skal pakkes i XML-format.

Realiseringen skal gjennomføres slik at systemet er forberedt for digitale signaturer men digitale signaturer skal ikke implementeres i dette utviklingsprosjektet.

1.7.2 ELMER

ELMER (enklere og mer effektiv rapportering) er et pilotprosjekt i regi av Nærings- og handelsdepartementet Handels- og Servicenæringens Hovedorganisasjon og Næringslivets Hovedorganisasjon. Prosjektet er startet og skal etter planen avsluttes 30.4.2001. Deltakere i prosjektet er ressurspersoner fra SSB Brønnøysundregistrene og ELMER.

Prosjektet skal levere følgende:

- Et eksempel på og utprøving av en innrapporteringsoppgave utført via en elektronisk dialog (intelligent skjema)
- Et eksempel på og utprøving av en innrapporteringsoppgave utført via automatisk datafangst i bedriftens systemer og maskinell oversendelse
- Eksempler på XML Schema-definisjoner for oppgavene som det testes med
- En sluttrapport for piloten med erfaringsbeskrivelse og anbefaling om videre arbeid.

For første strekpunkt skal følgende gjøres:

1. Utvikle XML Schema-spesifikasjon for samordnet registermelding
2. Spesifisere logikken i dialogen
3. Lage design for dialogen
4. Programmere logikken.

Dette har klare relasjoner til prosjektet Nettbasert Registrering ved BR.

For andre strekpunkt skal følgende gjøres:

1. Utvikle XML Schema-spesifikasjon for detaljomsetningsstatistikken
2. Spesifisere overføringsmetode for oversendelse av data
3. Installere og tilpasse produkt(er) for automatisk datafangst i bedriften(e)
4. Teste reelle overføringer og sammenlikne resultater med «gammel» metode.

Dette har klare relasjoner til IDUN-prosjektet i Statistisk sentralbyrå.

ELMER skal ikke se på problematikk vedrørende digitale signaturer men på muligheten for å benytte Oppgaveregisteret som en datadefinisjonsdatabase ved generering/validering av elektroniske meldinger.

1.7.3 Regnskapsdatabaseprosjektet (RdB)

RdB-prosjektet har til oppgave å utvikle en elektronisk regnskapsdatabase. For at BR skal kunne legge inn data i regnskapsdatabasen skal det også etableres et mottak for elektroniske årsregnskap samt løsning for årsregnskap som kommer inn på papir.

Løsningen for den elektroniske overleveringen fra de næringsdrivende/selskapene til Regnskapsdatabasen blir samordnet med løsningen for innrapportering til Skattedirektoratet v/SLN-prosjektet. I dette samarbeidsprosjektet deltar både Skattedirektoratet Statistisk sentralbyrå og Brønnøysundregistrene.

Overleveringsløsningen som utvikles i regi av SLN-prosjektet har fått utviklet en avgiverløsning som har vært testet i 2 piloter og nå skal over i pilot 3. Denne løsningen utvikles av Telenor Bedrift og tar for seg følgende:

- Digital signatur ved hjelp av smartkort kortleser og TTP (tiltrodd tredjepart ErgoGroup). Dette er testet ut i de 2 første pilotene men vil være valgfritt i pilot 3.
- Kryptering ved hjelp av offentlig og privat nøkkelpar som er utstedt av TTP-en.
- Overføring av årsregnskap ved hjelp av EDIFACT og meldingstype INFENT. Dette overføres ved hjelp av mail til FMS (formidlingssentral for Brønnøysundregistrene ErgoGroup)
- Inhouse-formatet mellom FMS og Brønnøysundregistrene overføres på fil. Dette skjer ved hjelp av fast linje.
- Alle poster/elementer som blir overført er kodet i Oppgaveregisteret ved Brønnøysundregistrene

I tillegg legges det opp til en alternativ innrapporteringskanal via Internett. Det er mulig at en slik løsning vil erstatte EDIFACT med XML.

For årsregnskap som kommer inn på papir vil BR fortsatt skanne og OCR-lese disse. Årsregnskapene blir lagret som image og vil være grunnlaget for manuell registrering i ettertid. Man vil imidlertid kun registrere resultatregnskapet og balanse for selskapet og konsernet. Resten av den tekstlige informasjonen som noter styrets beretning revisjonsberetningen og kontantstrømoppstilling vil ikke bli registrert. Denne informasjonen vil være tilgjengelig til det elektroniske regnskapet som image.

For å registrere disse regnskapene manuelt hadde de en anbudsrunde som gikk ut i desember (åpning av anbudspapirer 2. januar 2001) hvor det skal velges en leverandør som skal ta seg av mesteparten av registreringen. Regnskapsregisteret forbeholder seg retten til å ta på seg en viss del av dette arbeidet for å bygge opp intern kompetanse.

Behov: Autentisering.

1.8 Finansdepartementet

Finansdepartementet har etablert en mottakstjeneste for lokale regnskapssystemer som rapporterer til det sentrale statsregnskapet. Her stilles det krav til dataintegritet og kontroller som sikrer konsistens i data fra regnskapsførerne. Videre stilles det krav til autentisering tilgjengelighet og lagring av data (i 10 år).

1.9 Datatilsynet

Datatilsynet vil iht. til ny lov om personopplysninger bli mottakere av et antall meldinger. Nåværende konsesjonsordning foreslås delvis erstattet av en meldingsordning. Dette kan innebære behov for visse sikkerhetsfunksjoner avhengig av type opplysninger som meldingen forutsettes å inneholde.

1.10 Riksarkivet

Riksarkivet har utarbeidet ny arkivstandard NOARK-4 [57] der det stilles krav til bekreftelse på avsenders autentisitet og opprettholdelse av dokumenters integritet ved forsendelse og arkivering. Det stilles krav om opplegg for å utnytte og administrere digitale signaturer ved sending/mottak av eksterne dokumenter samt ved arkivering.

1.11 Vegdirektoratet – Virtuell trafikkstasjon

Vegdirektoratet arbeider med planer om å tilby døgnåpne elektroniske tjenester til sine brukere i bilbransjen og på sikt også til vanlige enkeltpersoner. «Virtuell trafikkstasjon» er det konseptet planene baserer seg på. Vegdirektoratet har satt seg som mål å drive effektivt og samtidig gi brukerne lett tilgjengelige selvbetjente tjenester som til dels kan erstatte behovet for oppmøte på trafikkstasjoner (biltilsyn). Flere trafikkstasjoner skal etter hvert nedlegges og de fleste oppgavene som disse utfører overføres til elektroniske tjenester. Oppgaver som krever personlig frammøte – som førerprøver – planlegges lagt til kjøreskoler eller andre typer skoler. Selve «bilskranken» på trafikkkontorene vil kunne overføres til offentlige servicekontorer eller til bilforhandlere.

Vegdirektoratet har som mål å spare inn 200 årsverk på slike oppgaver i 2002.

De første elektroniske tjenestene som skal bli tilgjengelige fra en virtuell trafikkstasjon er bestilling av timer til bilkontroller førerprøver mv. Dette er en tjeneste der det ikke sees behov for autentisering fordi risikoen for skade vurderes som liten.

Videre skal det tilbys elektronisk søknad om førerkort. Heller ikke her ser man behov for sterk autentisering over nett. Søkeren vil kun bli bedt om å oppgi sitt fødselsnummer som autentisering. Dette begrunnes med det faktum at personen uansett må møte opp fysisk for å bli fotografert og hente førerkortet som skal signeres fysisk ved avhenting.

Vegdirektoratet legger opp til at brukere av slike elektroniske tjenester skal kunne få tilbakemeldinger via e-post.

I januar 2002 planlegger Vegdirektoratet å ha tilgjengelig tjenesten for registrering av bil og utstedelse av vognkort. Tjenesten vil i første omgang bli tilgjengelig for bilimportørene og bilforhandlerne. Den vil kreve digitale signaturer. Det er representanter for bilfirmaer med sertifikat som angir virksomhetens organisasjonsnummer som skal signere elektroniske skjemaer for bilregistrering. Vegdirektoratet ønsker selv å ha et register med oversikt over alle sertifikater (personer som har sertifikater) som blir utstedt for dette formålet. Det planlegges også å kople denne tjenesten sammen med en tjeneste for tegning av ansvarsforsikring.

På lengre sikt skal bilregistreringstjenesten bli tilgjengelig for vanlige enkeltpersoner som vil kunne foreta elektronisk bilregistrering og ev. skifte av forsikringsselskap hjemmefra.

Andre elektroniske tjenester som planlegges omfatter dispensasjonssøknader fra eiere av tunge transportkjøretøyer og innrapportering til det såkalte COC-registeret når det gjelder samsvar av kjøretøyer (for å motvirke tyveri o.l.).

Vegdirektoratet gjennomfører også et internt prosjekt under navnet EBASUS. Prosjektet omhandler elektronisk fakturahåndtering og -betaling. Prosjektet har som mål å effektivisere prosesser knyttet til behandling av inngående fakturaer og interne utbetalinger som reiseregninger variable arbeidstillegg overtidsutbetalinger m.m. Prosjektet forutsetter at det skal opprettes sentrale fakturamottak der fakturaer vil bli skannet eller sendt direkte via elektronisk kommunikasjon (e-post arbeidsflytløsninger) til de personer som skal attestere og anvise. Autentisering av utstedere av interne fakturaer kan skje ved hjelp av PKI men også andre autentiseringsløsninger. Anvisning skal skje ved bruk av digitale signaturer. Det skal settes i gang utvikling av en pilotløsning for hele Østfold fylke i 2001. Finansdepartementet deltar i styringsgruppen for prosjektet og har gitt signaler om at nødvendige dispensasjoner fra økonomireglementet i staten vil bli gitt. Det forutsettes at ca. 80 personer vil få sertifikater for signering i pilotprosjektet. Vegdirektoratet satser her på å anvende standardløsninger for digitale signaturer som er tilgjengelige i markedet.

1.12 Patentstyret

Patentstyret er en offentlig etat som forvalter lov om patenter lov om varemerker og mønsterloven. I tillegg har Patentstyret også omfattende rådgivende tjenester kurs med mer.

Patentstyret startet høsten 1997 SANT-programmet *Saksbehandling ved Anvendelse av Ny Teknologi*.SANT innebærer at etaten legger om til full elektronisk saksbehandling innen første halvår 2002. Det franske Group Decan har blitt tildelt kontrakten for levering av SANT-systemet.

Et av målene for SANT-programmet er at kundene skal kunne utveksle dokumenter og kommunisere med Patentstyret elektronisk. Patentstyret vil også gjøre sine store databaser tilgjengelige for kunder og offentligheten via Internett på en sikker måte.

Patentstyrets ledelse besluttet den 23.2.2000 å gå til innkjøp av et støttesystem som kan oppfylle disse målene. Prosjektet har fått navnet TAKISAI. Formålet er å etablere en løsning hvor:

- Patentsøknader mønstersøknader og varemerkesøknader innleveres elektronisk
- All korrespondanse (brevveksling) i ovenstående utveksles elektronisk via Internett
- Søkere rettighetsinnehavere og parter i IP-saker via Internett kan få informasjon om sine saker direkte i Patentstyrets databaser
- Man sørger for sensitive avanserte søkemuligheter via Internett
- Man sørger for automatisk overvåkning av rettigheter og ny informasjon i databasene via Internett
- Sikkerhetsløsning.

Patentstyret har de aller strengeste krav til sikkerhet. Kundene søker om beskyttelse av industrielle rettigheter og det er viktig at utenforstående ikke gis tilgang til informasjon hvor ikke dette spesifikt skal gjøres etter bestemmelser i lov.

Prosjektet har inngått et samarbeid med ErgoGroup og baserer seg på bruk av smartkort og digitale signaturer.

Patentstyret vil opprette anslagsvis 20–30 forskjellige elektroniske skjemaer som kundene skal benytte. Kundene kan fritt benytte og hente disse fra Patentstyrets hjemmeside. Kunden fyller ut skjemaet og sender dette til Patentstyret. Alle skjemaer er beskyttet mot endringer. Kundene må benytte seg av systemet dersom de ønsker å kommunisere elektronisk med Patentstyret. Det eneste alternativet er vanlig papir.

TTP-leverandøren vil sannsynligvis få ansvaret for alt mottak og all forsendelse av korrespondanse på Patentstyrets vegne. Her vil filene bli gjenkjent og eventuelt konvertert til et filformat spesifisert fra Patentstyret.

Tabell V1.1 Patentstyret – noen tall (anslag)

Nye patentsøknader pr. år	7 000
Nye varemerkesøknader	16 000
Mønstersøknader	1 000
Antall formelle korrespondanser pr. år	120–150 000

All korrespondanse i forbindelse med en søknad er juridiske verdipapirer. Derfor er en SSL-løsning ikke god nok.

Det skal lages en database som har både en åpen og en lukket del. I den åpne delen skal søkere få tilgang til sin sak ved å autentisere seg via et smartkort. Andre får tilgang til at det er sendt søknad innen et bestemt område. Avanserte søk skal være mulig men Patentstyret ønsker at det skal kunne belastes brukeren via smartkortet.

Den lukkede delen er et internt hjelpemiddel med konfidensielle opplysninger om søknadene. Den vil bli brukt av ca. 200 ansatte.

Det er ikke vesentlig hvem som søker. I papirsystemet blir ikke navnet bak signaturen sjekket. Patentstyret tar stilling til innholdet i søknaden og gjør vedtak. Men Patentstyret trenger å vite at den korresponderer med den som søkte. Søknader vil i stor grad bli sendt inn via patentkontorer som har en sekretærfunksjon og vil representere mange søkere. Det vil antakelig bli ca. 200 eksterne brukere.

Patentstyret har ennå ikke bestemt hvilken unik identifikator de skal bruke i sertifikatene men de trenger tilgang til fødselsnummer. I utgangspunktet vil de ta imot alle sertifikater også fra utlandet. Men det kan bli vanskelig å verifisere dem og finne ut om de er gyldige. Patentstyret kan ønske seg en kryssertifisering innen patentverdenen.

Patentstyret har ikke fastsatt pris på nødvendige anskaffelser for aktuelle brukere.

1.13 Helsesektoren

I helsesektoren formidles store mengder informasjon innen administrativ saksbehandling og pasientbehandlingen. Årlig foretas ca. 15–18 millioner konsultasjoner i primærhelsetjenesten 3 3 mill. polikliniske konsultasjoner og 850 000 opphold i somatiske sykehus. Hver konsultasjon er opphav til registrering lagring behandling og formidling av informasjon i betydelig grad og det anslås utveksling av ca. 60 mill. meldinger i helsesektoren årlig.

All informasjon knyttet til den enkelte pasientbehandling er i hovedsak sensitiv informasjon og det stilles krav til sikkerhet at informasjonen er korrekt og i samsvar med behandlingen og at kun personer med rett til innsyn får det.

Pasientjournalen er det viktigste dokumentet i pasientbehandlingen. Her pålegges helsepersonell å dokumentere sin virksomhet dvs. å føre systematiske nedtegnelser om pasientens tilstand utførte behandlinger røntgenundersøkelser prøvesvar osv. Pasientjournalen anvendes i pasientbehandlingen som kommunikasjon mellom helsepersonell for internkontroll og kvalitetssikring som grunnlag for ulike meldinger som skal gis etter lovgivning og som dokumentasjon i forbindelse med erstatningssaker klagesaker og identifikasjon i forbindelse med ulykker etc.

Overføring av sensitiv pasientinformasjon formidles daglig og er i tillegg til journalkopier resepter henvisninger epikriser prøvesvar utdrag av pasientopplysninger fra journaler m.m. Informasjonen formidles mellom helsepersonell apotek laboratorium røntgeninstitutter Rikstrygdeverket og forvaltningen (i klagesaker for tilsynsformål). I tillegg overføres sensitiv pasientinformasjon til lokale helseregistre (institusjonsregistre) og til sentrale større registre. Som ved annen dokumentforsendelse er det behov for identifisering av avsender og beskyttelse mot ikke-autorisert innsyn.

Mye av informasjonsoverføringen i helsevesenet skjer i dag mellom kjente parter i et avtaleforhold. Men med fritt sykehusvalg og økt konkurranse og arbeidsdeling mellom ulike tjenesteytere vil det i stadig økende grad være behov for sikker identifisering av avsender verifisering av helsepersonells rolle profesjon eller autorisasjon/lisens ved elektronisk informasjonsoverføring.

1.1.2001 trådte ny lov om helsepersonell i kraft. Regler for journalføring er hjemlet i denne. Forskrift til loven likestiller elektronisk og papirbasert pasientjournal. Pasientjournalen er det grunnleggende «saksbehandlingssystemet» i helsevesenet. Der skal all helsehjelp og relevant informasjon om pasienten nedtegnes. Helsepersonellets dokumentasjonsplikt og ansvar for journalnedtegnelser er knyttet til den helsehjelpen som ytes. Nedtegninger i pasientjournalen skal signeres men det stilles ikke spesielle krav til hvordan dette skal ivaretas.

Det foreligger forslag til ny lov om helseregistre hvor det legges opp til at departementet kan gi bestemmelse om form og frist for innsamling av helseopplysninger til sentrale helseregistre herunder pålegg om sikkerhet bruk av standarder kode og klassifikasjonssystemer m.m.

Behov

Autentisitet: bekrefte identiteten til avsenderen av en melding eller et dokument eventuelt bekrefte identiteten til en bruker ved tilgang til et system/en tjeneste

- Ikke-benekting: få sikkerhet for at avsenderen av dokumentet/meldingen vedstår seg dets/dets innhold
- Integritet: sikre at innholdet ikke endres (eller at eventuelle endringer av dokumentet etter signering kan oppdages) ved overføring av journalinformasjon henvisninger epikriser/behandlingssammendrag meldinger og legeregninger til Rikstrygdeverket elektroniske resepter m.m.)
- Konfidensialitet: all overføring av sensitiv personinformasjon pasientinformasjon mellom ulike virksomheter må krypteres (også innenfor regionale helsenett)
- Autentisere mottaker dvs. være sikker på at dokumentet/meldingen sendes til riktig person/institusjon.

I en del tilfeller er det nødvendig med en kvittering fra mottaker på at et dokument er mottatt og lest.

1.13.1 Helsevesenets behov for sertifikater

Helsepersonell er personlig ansvarlige for den helsetjenesten de yter. Ansvaret er nedfelt i lov om helsepersonell som trådte i kraft 1.1.2001. Helsehjelp er her definert som enhver handling som har forebyggende diagnostisk behandlende helsebevarende eller rehabiliterende mål og som utføres av helsepersonell.

Helsepersonell kan jobbe flere steder ha flere arbeidsgivere og ivareta mange ulike roller f.eks.:

- En lege kan ha privat praksis jobbe deltid som offentlig ansatt lege (kommunelege og/eller tilsynslege i sykehjem/institusjon) ha vakter på kommunal eller interkommunal legevakt og jobbe deltid på sykehus.
- En fysioterapeut kan ha privat praksis og være tilknyttet et sykehjem (helseinstitusjon).

Autorisasjonen som lege sykepleier e.l. endres ikke når en skifter mellom slike roller. Det faktiske ansvarsområdet/myndighetsområdet kan likevel endres vesentlig når en bytter rolle. Dette innebærer at den totale autorisasjonen endres når en bytter rolle. Det vil imidlertid være vanskelig å ivareta (dvs. holde ved like) alle rollene i et ansattsertifikat e.l. Det vil være enklere å sjekke autorisasjonen mot en katalogtjeneste.

Helsepersonell trenger et personlig sertifikat med identifikasjon som kan benyttes i ulike roller i ulike organisatoriske sammenhenger og som er stabilt over tid. All dokumentasjon av handlingen må kunne spores tilbake til den som har gitt helsehjelpen eller som er faglig ansvarlig.

Utstedelse og vedlikehold av profesjons- eller rollesertifikater vil kreve mer administrasjon og stiller større krav til forvaltning og tilbakekallingsrutiner enn rene personsertifikater. En person kan f.eks. miste en forskrivningsrett men vil likevel kunne praktisere som helsepersonell. Rollesertifikater vil måtte endres ved oppgradering av autorisasjoner etter tilleggsutdanning spesialistgodkjenning m.m. Kontroll av helsepersonells profesjon og autorisasjon/lisens kan ivaretas gjennom en katalogtjeneste eller oppslag i Helsepersonellregisteret. Det vil gjøre sertifikatutstedelsen og -forvaltningen enklere enn utstedelse av profesjons- eller rollesertifikater basert på autorisasjoner.

Ansattsertifikat eller virksomhetssertifikat vil ikke dekke alle grupper av helsepersonell i privat praksis. Hvorvidt det er ønskelig med et ansattsertifikat internt i en virksomhet for aksess til systemer o.l. er noe den enkelte virksomhet bør kunne vurdere. Det ansees som lite aktuelt å styre aksess til systemer i helsevesenet gjennom generelle rollesertifikater eller ansattsertifikater for helsepersonell – som en felles ordning for sektoren. Autorisasjon av brukere til systemer kan enklere ivaretas gjennom ulike katalogtjenester. Et sertifikat som entydig identifiserer brukeren vil da være tilstrekkelig.

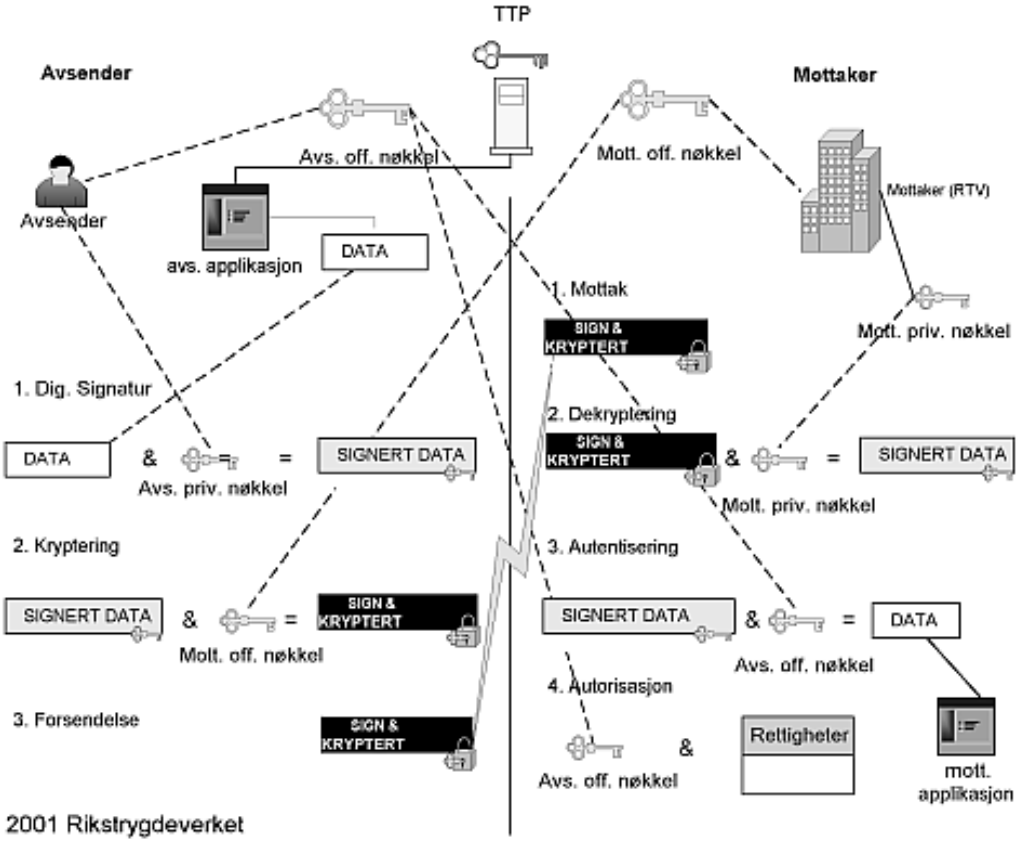
Konklusjon: Helsevesenets behov for sertifikater til bruk i samhandling mellom helsepersonell vil kunne dekkes gjennom rene personsertifikater evt. profesjonssertifikater som entydig identifiserer helsepersonell og som knytter personen til nøkler for signering.

1.13.2 Helsevesenets kommunikasjon med brukerne

Publikum vil etter hvert forvente at man skal kunne kommunisere elektronisk med sin lege for å stille spørsmål bestille time fornye resepter e.l. Sikkerhetskravene for å løse dette må ivaretas gjennom helsenettarbeidet. En elektronisk identifikasjon hvor borgerne/pasientene får sine personlige nøkler for sikker kommunikasjon med det offentlige kan i framtiden tenkes brukt for å identifisere pasienten i elektronisk kommunikasjon med helse- og trygdevesenet og for å dokumentere/bekrefte pasientens samtykke til overføring/utlevering av informasjon til andre. Identifikasjonen kan også tenkes brukt for å gi pasienten tilgang til egen helseinformasjon.

1.14 Rikstrygdeverket

RTV har benyttet PKI-løsninger ved beregning av økonomiske oppgjør med legene (LRK – LegeRegningsKontroll) siden 1996 og med oppgjør fra sykehusenes poliklinikker (POLK – Poliklinisk Kontroll) siden 1998. Dette er oppgjør basert på digitale signaturer både smartkort- og softwarebaserte løsninger kryptering og TTP-tjenester. Figur 1.1 illustrerer PKI-modellen som benyttes i RTV.



Figur V1.1 PKI-modell for Rikstrygdeverket

SESAM (Sikker Elektronisk Samhandling i Helsevesenet) har besluttet å evaluere POLK-løsningen som et eksempel på storskalabruk av digitale signaturer for sikker elektronisk meldingsutveksling. Dette er et av tre områder som dekkes av SESAM-prosjektet som skal være en utprøvingsarena for bruk av digitale signaturer og PKI i stor skala.

De andre prosjektområdene i SESAM er:

- Sikker e-post
- Sikker web-løsning.

KITH (Kompetansesenteret for IT i helsesektoren) har avgitt sin rapport angående POLK og følgende avsnitt angående PKI er sitert nedenfor. (Hele rapporten er offentlig tilgjengelig som KITH Rapport 21/00 ISBN 82-7846-101-5.)

Sitater fra POLK-rapporten:

POLK benytter seg av en PKI-basert løsning for kryptering og signering av meldingene som utveksles. Løsningen som er valgt er beskrevet i dokumentet «Sikkerhet i EDIFACT-meldingen – MEDRUC Poliklinikk oppgjørskrav fra sykehus» en implementering av EDIFACT-meldingene som med ett unntak er i overensstemmelse med KITH-rapport 9/95 «Håndbok for sikkerhet i EDIFACT-baserte meldinger – MEDRPT/MEDPRE/LEGOPP».

Kryptering og signeringsfunksjonaliteten er tett knyttet opp til EDIFACT-formatet. For digital signatur benyttes signaturforsterket MEDRUC-melding og for krypteringsformål pakkes MEDRUC-meldingen inn i en kryptert CIPHER-melding.

I første fase av prosjektet har RTV selv operert som TTP og utstedt sine egne sertifikater men løsningen har mulighet for å håndtere flere TTP-er etter hvert som disse blir tilgjengelige i markedet. For øyeblikket leverer ErgoGroup sertifikater til sykehusene som benytter POLK.

RTV's egne sertifikater var av typen X.509 v.2 sertifikatene fra ErgoGroup er X.509 v.3. Algoritmene som benyttes (disse opplysningene er utledet fra «Sikkerhet i EDIFACT-meldingen MEDRUC Poliklinikk oppgjørskrav fra sykehus») er:

- For generering av hash for meldingen: MD5
- For signering: RSA med nøkkellengde på 512 bits
- For kryptering: Meldingen komprimeres med GZIP og krypteres med DES. DES-nøkkelen krypteres med RTV's offentlige RSA-nøkkel.

For sertifikater av versjon 2 utføres det ikke kontroll av revokeringslister men eventuelle revokerte sertifikater fjernes fra RTV's katalogstruktur slik at meldinger signert med den private nøkkelen knyttet til et ikke godkjent sertifikat ikke vil godtas.

For sertifikater av versjon 3 kan revokeringslister kontrolleres online vha. LDAP-tilgjengelig katalog.

Vedlegg 2

Sertifikatprofiler for norsk forvaltning

2.1 Innledning

Dette notatet er laget av PKI Consulting Services for Arbeids- og administrasjonsdepartementet. Formålet med notatet er å utarbeide et forslag til sertifikatprofiler med begrunnelser for en del av valgene.

Utredningen her gjelder bare sluttbrukersertifikater ikke CA-sertifikater.

Sertifikatene skal bygge på X.509 v3 og profilen RFC 2459. RFC 2459 er den allment brukte standard for sertifikatprofilering. Sertifikatbruk i norsk offentlig sektor bør være i samsvar med denne. RFC 2459 er imidlertid svært bred og krever ytterligere nivåer av profilering for praktisk bruk.

I diskusjonen her er det tatt utgangspunkt i den stabile RFC 2459 fra 1999.

Kvalifiserte sertifikater (Qualified Certificates = QC) er en profil basert på RFC 2459. Det finnes en Internet Draft-spesifikasjon for QC som er skrevet med intensjon om å støtte kravene til kvalifiserte sertifikater og avanserte elektroniske signaturer som framkommer i EU-direktivet. I tillegg har det europeiske initiativet for standardisering rundt elektroniske signaturer (EESSI) gjort en del presiseringer og tilføyelser til denne. Likevel er det fortsatt behov for å gjøre flere profileringer og valg for faktisk bruk. Det er forsøkt å ta hensyn til krav og anbefalinger for kvalifiserte sertifikater i spesifikasjonene her.

I Internet Draft for Qualified Certificates er det gjort følgende tilleggsvalg og definisjoner:

- Definisjoner av navn og identitetsinformasjon for å identifisere subjekt (sertifikatinnehaver) på en mest mulig uniform måte.
- Definisjon av identitetsinformasjon for CA.
- Ytterligere definisjon av hvordan «keyUsage»-utvidelsen skal brukes.
- Struktur for lagring av biometrisk informasjon.
- Definisjon av lagring og representasjon av predefinerte erklæringer om sertifikatets bruk som kvalifisert sertifikat («qcStatements»-utvidelsen):
- Erklæring om at sertifikatet er utstedt som kvalifisert sertifikat (enten ved å referere til en policy som klart indikerer at den er for slike eller gjennom en eksplisitt erklæring)
- Erklæring om begrensning i verdi for de transaksjoner som sertifikatet kan brukes til (gjennom en erklæring og angivelse av et beløp)
- Erklæring om hvor lenge registreringsinformasjon om innehaver vil bli arkivert.

qcStatements er en privat utvidelse («extension») som stammer fra det kvalifiserte sertifikatet og benyttes for å understreke overfor brukeren at det her handler om et kvalifisert sertifikat. Et standardforslag til tekst for en egenerklæring om at man har med et kvalifisert sertifikat å gjøre finnes i ETSI's draft standard for «Qualified Certificate Profile». Det er ennå usikkert i hvilken grad dette kommer til å bli presentert for brukeren gjennom standard programvare. Man har foreløpig for liten erfaring med utvidelser for kvalifiserte sertifikater til å kunne gjøre seg opp noen mening om hvordan disse brukes av andre sertifikatutstedere.

Alle referanser forutsetter at navn på utsteder og innehaver skal kodes som sekvenser av navneattributter. Når sekvensen av attributter utgjør et unikt navn er dette et DN (Distinguished Name). Alle navn må være unike innenfor en kontekst gitt av sertifikatutsteder og bruksområde.

Navn på utstedere og sertifikatinnehavere bør skrives i et alfabet som minimum inneholder norske tegn fortrinnsvis som en UTF8-string fordi RFC 2459 setter dette som et krav til alle sertifikater som utstedes etter 31.12.2003.

Det er også et poeng at informasjonen som står i commonName og organizationName-attributtene er umiddelbart gjenkjennbar for brukerne fordi denne informasjonen kan vises fram av de fleste klientprogrammer. Det er høyst variabelt i hvilken grad f.eks. e-postklienter er i stand til å vise annen sertifikatinformasjon.

Attributtet «SerialNumber» står ikke listet opp eksplisitt blant attributtene som foreslås brukt i navnene på utstedere og sertifikatinnehavere i RFC 2459. Imidlertid er «SerialNumber» tatt med i anbefalingen av profil for kvalifiserte sertifikater og i den nye draft-profilen som IETF nå har utarbeidet og som på sikt skal erstatte RFC 2459. Det anbefales derfor å benytte «SerialNumber» i stedet for alternativet «dnQualifier» til å lagre unik identifikasjon. Merk også at «SerialNumber» tillater bruk av andre tegn enn tall slik at sekvenser med bruk av bokstaver bindestreker eller blanke som skilletegn er fullt ut akseptable.

Ikke alle nettlesere presenterer feltet CertificatePolicies for brukeren. Det bør derfor vurderes om man gjør som svenskene og legger et lesbart navn for policyen til bakerst i *commonName* i issuer-feltet.

Det er gjort forsøk på å begrense mengden informasjon som skal inn i sertifikatene bl.a. med tanke på at plassen i smartkort vil være begrenset.

Det er ikke tatt stilling til valg av nøkkellengder eller til hvordan data om sertifikatinnehaver initielt blir identifisert og registrert. Sertifikatene er også forsøkt beskrevet uavhengig av valg av lagringsmedium for nøklene.

Det er ikke tatt stilling til hvilke data om sertifikatinnehavere som skal lagres i kataloger. Katalogene kan bestå både av offentlig lesbar informasjon og av informasjon som det ikke gis leseaksess til ved alle katalogoppslag.

Det er satt opp forslag til følgende fire typer av sertifikater:

- Ansattsertifikat
- Virksomhetssertifikat
- Offentlig personsertifikat
- Profesjonssertifikat.

Rene autorisasjonssertifikater og rollesertifikater (attributtsertifikater) beskrives ikke i dette notatet.

Det anbefales *ikke* å gjøre som danskene foreslår å innføre en ny privat utvidelse i sertifikatene som eksplisitt sier om det er et personsertifikat ansattsertifikat virksomhetssertifikat eller profesjonssertifikat. Dette betyr at det må være mulig algoritmisk (i programvare) å finne ut hva slags sertifikat en står overfor. (En øvelse for å verifisere dette er gjort for FSP-1-sertifikattyper tidligere.) I praksis kan dette gjennomføres ved f.eks. å ha de obligatoriske elementene i subject-navnet i forskjellige forhåndsbestemte rekkefølger.

I tabellene benyttes følgende forkortelser i kolonnen «Forekomst»:

M	Obligatorisk felt (Mandatory)
R	Bør inngå i profilen (Recommended)
---	Brukes ikke i aktuell profil
O	Valgfritt ikke obligatorisk felt (uten ytterligere føringer på forekomst (Optional))

I tabellene benyttes følgende forkortelser i kolonnen «Må sjekkes»:

Ja	Feltet må sjekkes av sertifikatbruker. Dersom sertifikatbruker ikke er i stand til å kontrollere feltet når sertifikatet prosesseres skal sertifikatet forkastes. (Critical)

Nei Sertifikatbruker kan selv bestemme om feltet skal sjekkes. Det er ikke avgjørende at sertifikatbruker er i stand til å sjekke feltet. (Non-critical)

2.2 Ansattsertifikat

Ansattsertifikatet skal baseres på RFC 2459 og spesifikasjonene for kvalifiserte sertifikater. I tillegg har Forvaltningsnettsamarbeidet spesifisert krav til og innhold i ansattsertifikater gjennom FSP-1 sertifikatpolicy.

Ansattsertifikatet er et personlig sertifikat for ansatte i en bedrift eller en etat. Ansattsertifikatet er et identitetssertifikat. Det er spesifisert uavhengig av valgt lagringsmedium for nøkler.

Ansattsertifikat inneholder ikke personens fødselsnummer eller annen informasjon som gjør vedkommende unikt definert på nasjonal basis. Hovedkravet her er i stedet at personen skal være entydig identifiserbar innenfor den virksomheten hvor vedkommende er ansatt.

Det foreslås at Elektronisk Ansatt-ID kan bestå av tre sertifikater:

- Sertifikat for ikke-benekting (elektronisk signatur) med *non-repudiation*-biten satt i keyUsage-feltet
- Sertifikat for autentisering med *authentication-biten* satt i keyUsage-feltet
- Kryptering og transport av sesjonsnøkler med bitene *keyEncipherment* og/eller *dataEncipherment*satt i keyUsage-feltet.

Anvendelse av tre sertifikater kan være vanskelig for enkelte typer programvare spesielt på klientsiden men også på sertifikatutstedersiden.

Det er med rette stilt spørsmål ved innehavers bruk av ansattsertifikatet i privat sammenheng. Det antas at ansattsertifikatet og de tilhørende nøklene er så nøye knyttet til ansettelsesforholdet at de ikke bør benyttes til rent privat bruk. Dette gjelder alle typer nøkler men særlig for krypteringsnøkler og kryptering/dekryptering som privatperson.

Det er ikke obligatorisk å oppgi i sertifikatet hvilken underenhet (organizationUnit) en ansatt tilhører. Dermed reduseres risikoen for at sertifikatet vil måtte utstedes på nytt ved endringer i organisasjonsstrukturen.

Det foreslåtte ansattsertifikatet skiller seg fra forslaget i FSP-1 ved at den ansattes fullstendige navn slik dette er registrert i folkeregisteret er fjernet fra subjectAltName. Det bør ikke være nødvendig å ha med mellomnavn som aldri brukes etc. i et ansattsertifikat.

Et annet avvik fra FSP-1 er at attributtet SerialNumber brukes i subject til å angi intern informasjon som skal sørge for unik identifikasjon av sertifikatinnehaver. Dette nummeret bør holdes unikt og konstant i den forstand at det knyttes til en og bare en ansatt det kan følge den ansatte gjennom forskjellige roller og stillinger og det vil ikke bli brukt om igjen hvis den ansatte forlater virksomheten.

Tabell V2.1 Forslag til grunnleggende sertifikatfelter fra X.509 for ansattsertifikat

Feltnavn	Forekomst	;Kommentar
version	M	=2 (for X.509 v.3)
serialNumber	M	RFC 2459 stiller svært få krav unntatt at serienummeret må være numerisk og entydig. Den enkelte utsteder er ansvarlig for at serienumrene sikres entydighet
signature	M	En av disse to signatur-algoritmene skal benyttes: – md5WithRSAEncryption – sha-1WithRSAEncryption

Feltnavn	Forekomst	;Kommentar
issuer	M	Følgende attributter skal benyttes: – ;*countryName* (Landkode =NO) – ;*organizationName* (Registrert navn (fra Brønnøysundreg.) for ;utstedende organization myndighet etc.) – ;*serialNumber* (Organisasjonsnummer for utsteder (fra Brønnøy ;sundreg.)) – *commonName* (Navn som utstederen er kjent under) *countryName organizationName og serialNumber* skal til sammen være tilstrekkelig for å gi en unik identitet som ifølge kravene i *Qualified Certificate-profilen* skal være en *unmistakable identity* hvilket innebærer at identiteten skal være opplagt forståelig for avhengige parter. *commonName* skal inneholde et alminnelig navn som utstederen er kjent under f.eks. Kbank.
validity	M	Gyldighetsperiode Fra – til i samsvar med RFC 2459
subject	M	Det grunnleggende kravet er unik identifikasjon av den enkelte ansatte innenfor organisasjonen. Følgende attributter *skal* benyttes: – ;*countryName* (Landkode =NO) – ;*organizationName* (Organisasjonsnummer (fra Brønnøysund ;registrene) og alminnelig brukt navn for organisasjonen hvor serti ;fikatinnehaver er ansatt) – ;*commonName* (Navn som alminnelig benyttes på personen) NB: Av praktiske årsaker plasseres både organisasjonsnummeret og navnet som virksomheten vil være kjent under i ett og samme attributt. – For å skille mellom flere ansatte med samme navn kan man benytte: – *serialNumber* (Organisasjonsintern unik identifikator av den ansatte kan f.eks. være ansattnummer eller tre-bokstavers initialer) Kombinasjonen av disse attributtene skal entydig definere personen som er sertifikatinnehaver. subject kan i tillegg inneholde andre attributter men disse skal ikke være nødvendige for å identifisere personen. Attributtet *organizationUnitName* kan brukes til å angi avdeling eller organisasjonsenhet. *common name* skal inneholde et navn som personen vil bli identifisert med. Det skal være mulig å «undertrykke» uønskede mellomnavn etc.
subjectPublicKeyInfo	M	– ;I sertifikater for autentisering eller ikke-benekting skal dette være ;rsaEncryption – ;I sertifikat for kryptering skal dette være rsaEncryption eller Diffie-HellmanKeyExchange
issuerUniqueIdentifier	---	Brukes ikke
subjectUniqueIdentifier	---	Brukes ikke

Tabell V2.2 Standard utvidelser for ansattsertifikat

Feltnavn	Må sjekkes	Forekomst	Kommentar
authorityKeyIdentifier	Nei	M	Gir mulighet til å identifisere den offentlige nøkkel som hører sammen med den private CA-nøkkel som er brukt til å signere sertifikatet.
subjectKeyIdentifier	Nei	M	Gir mulighet til å identifisere den offentlige nøkkel

Feltnavn	Må sjekkes	Forekomst	Kommentar
			som er i sertifikatet.
keyUsage	Ja	M	Information om «keyUsage» skal finnes. Om *nonRepudiation* er valgt tillates ingen annen «Usage».
privateKeyUsagePeriod		---	Brukes ikke
certificatePolicies	Nei	M	OID til den policy sertifikatet er utstedt under.
policyMappings		---	Brukes ikke
subjectAltName	Nei	R	Det anbefales å legge inn sertifikatinnehavers e-postadresse (i organisasjonen). E-postadresser skal kodes som IA5-strenger.
issuerAltName		---	Brukes ikke
subjectDirectoryAttributes		---	Brukes ikke
basicConstraints		---	Brukes ikke i sluttbrukersertifikatene
nameConstraints		---	Brukes ikke
policyConstraints		---	Brukes ikke
cRLDistributionPoints	Nei	M	
extKeyUsage		---	Brukes ikke

Tabell V2.3 Private utvidelser for ansattsertifikat

Feltnavn	Må sjekkes	Forekomst	Kommentar
AuthorityInfoAccessSyntax	Nei	O	
biometricInfo	Nei	O	
qcStatements	Nei	O	Anbefales å legge inn OID til «egenerklæring» for utstedere av kvalifiserte sertifikater
cardNumber	Nei	O	

2.3 Virksomhetssertifikat

Virksomhetssertifikatet skal baseres på RFC 2459.

Virksomhetsssertifikatet skal sikre kommunikasjon til og fra virksomheter og organisasjonsenheter.

Virksomhetssertifikatet er spesifisert uavhengig av valgt lagringsmedium for nøkler.

Det er ikke knyttet noe personinformasjon eller personidentifikasjon til virksomhetssertifikatet. Det er således ingen personvernhensyn som må avklares.

Eksempler på bruk av virksomhetssertifikat er at en bedrift eller institusjon mottar kryptert e-post eller at det foretas en toveis autentisering mellom en klient og virksomheten f.eks. mellom en skatteyter og skatteetaten. Det kan også tenkes situasjoner der en ansatt i en virksomhet vil signere meldinger med en nøkkel som tilhører virksomheten. I slike tilfeller vil knytting mellom den ansatte som har signert og meldingen eller dokumentet være at vedkommendes navn framgår av det signerte innholdet.

Elektronisk virksomhets-ID kan bestå av opptil tre sertifikater.

- Sertifikat for ikke-benekting (elektronisk signatur) med *non-repudiation*-biten satt i keyUsage-feltet
- Sertifikat for autentisering med *authentication*-biten satt i keyUsage-feltet
- Kryptering og transport av sesjonsnøkler med bitene *keyEncipherment* og/eller *dataEncipherment*satt i keyUsage-feltet.

Ettersom kvalifiserte sertifikater pr. definisjon utstedes til individer er det ikke meningsfylt å snakke om kvalifiserte virksomhetssertifikater. For helhetens skyld er imidlertid de private utvidelsene fra spesifikasjonen for kvalifiserte sertifikater tatt med også i denne tabellen.

Det foreslåtte virksomhetssertifikatet skiller seg fra forslaget i FSP-1 ved at man i subject benytter serialNumber i stedet for dnQualifier til å angi virksomhetens organisasjonsnummer. I forhold til FSP-1 foreslås det også å flytte virksomhetens fullstendige navn fra subjectAltName til organizationName-attributtet i subject og at navn i daglig bruk flyttes fra organizationName til commonName (internt i subject).

Tabell V2.4 Forslag til grunnleggende sertifikatfelter fra X.509 for virksomhetssertifikat:

Feltnavn	Forekomst	;Kommentar
version	M	=2 (for X.509 v.3)
serialNumber	M	RFC 2459 stiller svært få krav unntatt at serienummeret må være numerisk og entydig. Den enkelte utsteder er ansvarlig for at serienumrene sikres entydighet
signature	M	En av disse to signatur-algoritmene skal benyttes: – ;md5WithRSAEncryption – ;sha-1WithRSAEncryption
issuer	M	Følgende attributter skal benyttes: – ;*countryName* (Landkode =NO) – ;*organizationName* (Registrert navn (fra Brønnøysundreg.) for ;utstedende organisasjon myndighet etc.) – ;*serialNumber* (Organisasjonsnummer fra Brønnøysundregistrene) – ;*commonName* (Navn som utstederen er kjent under) *countryName organizationName* og *serialNumber* skal til sammen være tilstrekkelig for å gi en unik identitet som i følge kravene i *Qualified Certificate*-profilen skal være en *unmistakable identity* hvilket innebærer at identiteten skal være opplagt for avhengige parter. *commonName* skal inneholde et alminnelig navn som utstederen er kjent under f.eks. Kbank.

Feltnavn	Forekomst	;Kommentar
validity	M	Gyldighetsperiode Fra – til i samsvar med RFC 2459
subject	M	Følgende attributter skal benyttes: – ;*countryName* (Landkode f.eks. NO) – ;*serialNumber* (Organisasjonsnummer (fra Brønnøysundregist ;rene)) – ;*organizationName* (Offisielt registrert navn (fra Brønnøysund ;reg.) på virksomheten f.eks. Christiania Bank & Kreditkasse) De tre attributtene over skal entydig definere virksomheten Dersom virksomheten har fått utstedt sertifikater for flere underenheter/avdelinger skal – ;*organizationUnitName* benyttes til å skille mellom disse. I tillegg anbefales det for bedrifter der «organizationName» ikke benyttes i daglig tale å benytte: – ;*commonName* (Navnet virksomheten som innehar sertifikatet er ;kjent under f.eks. Kbank)
subjectPublicKeyInfo	M	– ;I sertifikat for autentisering eller ikke-benekting skal dette være ;rsaEncryption – ;I sertifikat for kryptering skal dette være rsaEncryption eller ;Diffie-HellmanKeyExchange
issuerUniqueIdentifier	---	Brukes ikke
subjectUniqueIdentifier	---	Brukes ikke

Tabell V2.5 Standard utvidelser for virksomhetssertifikater

Feltnavn	Må sjekkes	Forekomst	Kommentar
authorityKeyIdentifier	Nei	M	Gir mulighet til å identifisere den offentlige nøkkel som hører sammen med den private CA-nøkkel som er brukt til å signere sertifikatet.
subjectKeyIdentifier	Nei	M	Gir mulighet til å identifisere den offentlige nøkkel som er i sertifikatet.
keyUsage	Ja	M	Informasjon om «keyUsage» skal finnes. Om *nonRepudiation* er valgt tillates ingen annen «Usage».
privateKeyUsagePeriod		---	Brukes ikke
certificatePolicies	Nei	M	
policyMappings		---	Brukes ikke
subjectAltName	Nei	R	Anbefales å inneholde «firmapostadresse» for sertifisert virksomhet. E-postadresser skal kodes som IA5-strenger. Kan også – i stedet eller i tillegg – inneholde sertifisert virksomhets web-adresse (Uniform Resource Locator)
issuerAltName		---	Brukes ikke

Feltnavn	Må sjekkes	Forekomst	Kommentar
subjectDirectoryAttributes		---	Brukes ikke
basicConstraints		---	Brukes ikke i annet enn CA-sertifikater
nameConstraints		---	Brukes ikke
policyConstraints		---	Brukes ikke
cRLDistributionPoints	Nei	M	
extKeyUsage		---	Brukes ikke

Tabell V2.6 Private utvidelser for virksomhetssertifikater

Feltnavn	Må sjekkes	Forekomst	Kommentar
AuthorityInfoAccessSyntax	Nei	O	
biometricInfo	Nei	---	
qcStatements	Nei	---	
cardNumber	Nei	O	

2.4 Offentlig personsertifikat

Offentlige personsertifikater skal baseres på RFC 2459 og spesifikasjonene for kvalifiserte sertifikater. Det er et personlig identitetssertifikat.

Et offentlig personsertifikat er et sertifikat for privatpersoner til bruk blant annet mot forvaltningen. Med privatpersoner menes alle individer som enten er norske statsborgere eller bosatt i Norge og følgelig kan ha behov for å kommunisere med norske myndigheter.

Spesifikasjonen av offentlige personsertifikater er gjort uavhengig av valgt lagringsmedium for nøkler.

Forvaltningen vil kreve at man via sertifikatet skal kunne få tilgang til innehaverens fødselsnummer fordi forvaltningen har behov for en på nasjonalt nivå unik identifikator av sertifikatinnehaver. I praksis vil dette bety at man via sertifikatet skal kunne få tilgang til innehaverens fødselsnummer. Den enkleste måten å løse dette på vil være å ha fødselsnummeret i sertifikatene. Ettersom sertifikatinnholdet må regnes som offentlig lesbar informasjon foreslås det i stedet å bruke en numerisk eller alfanumerisk identifikator som sikrer unikhet i «subject»-attributtet i sertifikatet og at sertifikatutsteder blir pålagt å ha en kopling mellom denne unike verdien og fødselsnummeret. Denne unike subjekt-identifikatoren skal plasseres i attributtet

serialNumber. En sertifikatinnehaver skal få tildelt et slikt entydig nummer hos hver enkelt sertifikatutsteder. Hvis en og samme sertifikatinnehaver har fått utstedt flere sertifikater hos en utsteder skal den unike identifikatoren ha samme verdi for alle disse sertifikatene. Identifikatoren bør også beholdes uendret hvis personen f.eks. skifter navn. Identifikatorverdien skal ikke brukes om igjen hvis sertifikatinnehaver dør eller flytter ut av Norge.

Bruk av pseudonymer anbefales ikke. Hvis pseudonym skal brukes kan det legges til som et ekstra attributt i subject-feltet. Unik subjekt-identifikator og vanlig brukt navn skal uansett finnes i sertifikatet.

Elektronisk ID for privatpersoner vil bestå av tre sertifikater. (Her avviker det fra det svenske forslaget til «Medborgarcertifikat» men er på linje med norsk arbeid i blant annet Forvaltningsnett og BankID.):

- Sertifikat for ikke-benekting (elektronisk signatur) med*non-repudiation* biten satt i keyUsage-feltet
- Sertifikat for autentisering med *authentication* biten satt i keyUsage-feltet
- Kryptering og transport av sesjonsnøkler med bitene *keyEncipherment* og/eller *dataEncipherment*satt i keyUsage-feltet.

Anvendelse av tre sertifikater kan være vanskelig for enkelte typer programvare spesielt på klientsiden men også på utstedersiden.

Tabell V2.7 Forslag til grunnleggende sertifikatfelter fra X.509 for offentlig personsertifikat:

Feltnavn	Forekomst	;Kommentar
version	M	=2 (for X.509 v.3)
serialNumber	M	RFC 2459 stiller svært få krav unntatt at serienummeret må være numerisk og entydig. Den enkelte utsteder er ansvarlig for at serienummerne sikres entydighet
signature	M	En av disse to signatur-algoritmene skal benyttes: – ;md5WithRSAEncryption – ;sha-1WithRSAEncryption
issuer	M	Følgende attributter skal benyttes: – ;*countryName* (Landkode =NO) – ;*organizationName* (Registrert navn (fra Brønnøysundreg.) ;for utstedende organisasjon myndighet etc.) – ;*serialNumber* (Organisasjonsnummer (fra Brønnøysundreg.)) – ;*commonName* (Navn som utstederen er kjent under) *countryName organizationName* og *serialNumber* skal til sammen være tilstrekkelig for å gi en unik identitet som ifølge kravene i *Qualified Certificate*-profilen skal være en *unmistakable identity* hvilket innebærer at identiteten skal være opplagt for avhengige parter. *commonName* skal inneholde et alminnelig navn som utstederen er kjent under f.eks. Kbank.
validity	M	Gyldighetsperiode Fra – til i samsvar med RFC 2459
subject	M	Følgende attributter skal benyttes: – ;*countryName* (Landkode =NO) – ;*serialNumber* (Kodet verdi som entydig refererer til en person) – ;*commonName* (f.eks. Hans Olsen) Disse tre attributtene skal entydig definere personen som er sertifikatinnehaver. *serialNumber* skal ikke være sertifikatinnehavers fødelsnummer men en numerisk eller alfanumerisk verdi som sertifikatutsteder (eller en operatør på vegne av utsteder) kan oversette til fødselsnummer ved hjelp av tabelloppslag eller konverteringer. serialNumber blir i dette sertifikatet et «uniqueSubjectNumber».

Feltnavn	Forekomst	;Kommentar
version	M	=2 (for X.509 v.3)
		subject kan i tillegg inneholde andre attributter men disse skal ikke være nødvendige for å identifisere personen. *common name* skal inneholde et navn som personen vil bli identifisert med. Det skal være mulig å «undertrykke» uønskede mellomnavn etc.
subjectPublicKeyInfo	M	– ;I sertifikater for autentisering eller ikke-benekting skal dette ;være rsaEncryption – ;I sertifikat for kryptering skal dette være rsaEncryption eller ;Diffie-HellmanKeyExchange
issuerUniqueIdentifier	---	Brukes ikke
subjectUniqueIdentifier	---	Brukes ikke

Tabell V2.8 Standard utvidelser for offentlig personsertifikat

Feltnavn	Må sjekkes	Forekomst	Kommentar
authorityKeyIdentifier	Nei	M	Gir mulighet til å identifisere den offentlige nøkkel som hører sammen med den private CA-nøkkel som er brukt til å signere sertifikatet.
subjectKeyIdentifier	Nei	M	Gir mulighet til å identifisere den offentlige nøkkel som er i sertifikatet.
keyUsage	Ja	M	Informasjon om «keyUsage» skal finnes. Om *nonRepudiation* er valgt tillates ingen annen «Usage».
privateKeyUsagePeriod		---	Brukes ikke
certificatePolicies	Nei	M	
policyMappings		---	Brukes ikke
subjectAltName	Nei	O	Det er mulighet til å legge inn to typer informasjon i subjectAltName: – ;E-post adresse – ;Fullt navn for personen slik dette er registrert ;i folkeregisteret E-postadresser skal kodes som IA5-strenger.
issuerAltName		---	Brukes ikke
subjectDirectoryAttributes		---	Brukes ikke
basicConstraints		---	Brukes ikke i sluttbrukersertifikatene
nameConstraints		---	Brukes ikke

Feltnavn	Må sjekkes	Forekomst	Kommentar
policyConstraints		---	Brukes ikke
cRLDistributionPoints	Nei	M	
extKeyUsage		---	Brukes ikke

Tabell V2.9 Private utvidelser for offentlig personsertifikat

Feltnavn	Må sjekkes	Forekomst	Kommentar
AuthorityInfoAccessSyntax	Nei	O	
biometricInfo	Nei	O	
qcStatements	Nei	O	Anbefales å legge inn OID til «egenerklæring» for utstedere av kvalifiserte sertifikater
cardNumber	Nei	O	

2.5 Profesjonssertifikat

Profesjonssertifikatet skal baseres på RFC 2459 og spesifikasjonene for kvalifiserte sertifikater. I tillegg har Forvaltningsnettsamarbeidet spesifisert krav til og innhold i profesjonssertifikater gjennom FSP-1.

Profesjonssertifikater er personlige sertifikater som knytter en person til et bestemt yrke/utdanning og til en eventuell autorisasjon eller godkjenning fra en myndighet eller en organisasjon.

Profesjonssertifikatene skal ha et unikt nummer som angir profesjonsrettigheten samt et tittelfelt som gir en tekstlig (menneskelig lesbar) beskrivelse av profesjonen.

Et profesjonssertifikat kan betraktes som en kombinasjon av identitetssertifikat og autorisasjonssertifikat.

Profesjonssertifikatet er spesifisert uavhengig av valgt lagringsmedium for nøkler.

Profesjonssertifikatet skal inneholde et «profesjonsnummer» som definerer innehaveren unikt innenfor en nærmere angitt mengde «profesjonelle» f.eks. innenfor alt registrert helsepersonell i Norge. Profesjonssertifikatet gir således vedkommende en unik identifikasjon innenfor innehaverne av et gitt yrke men ikke en unik identifikasjon som person hele befolkningen tatt i betraktning.

Elektronisk profesjons-ID kan bestå av tre sertifikater:

- Sertifikat for ikke-benekting (elektronisk signatur) med *non-repudiation*-biten satt i keyUsage-feltet
- Sertifikat for autentisering med *authentication*-biten satt i keyUsage-feltet

- Kryptering og transport av sesjonsnøkler med bitene *keyEncipherment* og/eller *dataEncipherment*satt i keyUsage-feltet.

Anvendelse av tre sertifikater kan være vanskelig for enkelte typer programvare spesielt på klientsiden men også på utstedersiden.

Som en del av diskusjonen rundt profesjonssertifikater bør det avklares i hvilken grad innehaveren skal ha anledning til å benytte sertifikatene og nøklene til rent privat bruk.

Som et alternativ til å definere profesjonssertifikater kan det brukes identitetssertifikater eller ansattsertifikater og man kan i stedet lagre informasjon om innehavers profesjon og rettigheter i et sentralt tilgjengelig register. Imidlertid må det da finnes klientprogramvare som klarer å kombinere informasjon i sertifikatene med informasjon i det andre registeret.

Det foreslåtte profesjonssertifikatet skiller seg fra forslaget i FSP-1 ved at den ansattes fullstendige navn slik dette er registrert i folkeregisteret er fjernet fra subjectAltName. Det burde ikke være nødvendig å ha med mellomnavn som aldri brukes etc. i et slikt sertifikat.

I stedet åpnes det for at man i feltet subjectAltName kan legge inn e-postadresse eller web-adresse til den institusjonen som har autorisert sertifikatinnehaver (f.eks. Statens helsetilsyn).

Et annet avvik fra FSP-1 er at attributtet SerialNumber brukes i subject til å angi den unike referansen (f.eks. et unikt nummer) som angir profesjonsrettighetene for innehaveren.

Tabell V2.10 Forslag til grunnleggende sertifikatfelter fra X.509 for profesjonssertifikat

Feltnavn	Forekomst	;Kommentar
version	M	=2 (for X.509 v.3)
serialNumber	M	RFC 2459 stiller svært få krav unntatt at serienummeret må være numerisk og entydig. Den enkelte utsteder er ansvarlig for at serienumrene sikres entydighet
signature	M	En av disse to signatur-algoritmene skal benyttes: – ;md5WithRSAEncryption – ;sha-1WithRSAEncryption
issuer	M	Følgende attributter skal benyttes: – ;*countryName* (Landkode =NO) – ;*organizationName* (Registrert navn (fra Brønnøysundreg.) for ;utstedende organisasjon myndighet etc.) – ;*serialNumber* (Organisasjonsnummer for denne (Brønnøysundreg.)) – ;*commonName* (Navn som utstederen er kjent under) *countryName organizationName* og *serialNumber* skal til sammen være tilstrekkelig for å gi en unik identitet som i følge kravene i *Qualified Certificate*-profilen skal være en *unmistakable identity* hvilket innebærer at identiteten skal være opplagt for avhengige parter. *commonName* skal inneholde et alminnelig navn som utstederen er kjent under f.eks. Kbank.
validity	M	Gyldighetsperiode Fra – til i samsvar med RFC 2459
subject	M	Følgende attributter skal benyttes: – ;*countryName* (Landkode =NO) – ;*commonName* (Navn som vanligvis benyttes på personen) – ;*organizationName* (Alminnelig brukt navn for organisasjonen ;hvor sertifikatinnehaver er registrert og autorisert til å inneha sin ;profesjon og organisasjonsnummer for denne) – ;*serialNumber* (unikt nummer som identifiserer vedkommende ;innenfor innehaverne av den aktuelle profesjonen) – ;*title* (tekstlig beskrivelse av profesjonen f.eks. «lege spesialist ;indremedisin») Kombinasjonen av disse attributtene skal entydig beskrive personens

Feltnavn	Forekomst	;Kommentar
version	M	=2 (for X.509 v.3)
		profesjonsrettigheter og opprette en logisk forbindelse mellom personens navn og entydige profesjonsrettigheter. Av praktiske grunner plasseres både organisasjonens navn og org.nr. i ett og samme attributt. *subject* kan i tillegg inneholde andre attributter. *common name* skal inneholde et navn som personen vil bli identifisert med. Det skal være mulig å «undertrykke» uønskede mellomnavn etc.
subjectPublicKeyInfo	M	– ;I sertifikat for autentisering eller ikke-benekting skal dette være ;rsaEncryption – ;I sertifikat for kryptering skal dette være rsaEncryption eller ;Diffie-HellmanKeyExchange
issuerUniqueIdentifier	---	Brukes ikke
subjectUniqueIdentifier	---	Brukes ikke

Tabell V2.11 Standard utvidelser for profesjonssertifikat

Feltnavn	Må sjekkes	Forekomst	Kommentar
authorityKeyIdentifier	Nei	M	Gir mulighet til å identifisere den offentlige nøkkel som hører sammen med den private CA-nøkkel som er brukt til å signere sertifikatet.
subjectKeyIdentifier	Nei	M	Gir mulighet til å identifisere den offentlige nøkkel som er i sertifikatet.
keyUsage	Ja	M	Informasjon om «keyUsage» skal finnes. Om *nonRepudiation* er valgt tillates ingen annen «Usage».
privateKeyUsagePeriod		---	Brukes ikke
certificatePolicies	Nei	M	OID til den policy sertifikatet er utstedt under.
policyMappings		---	Brukes ikke
subjectAltName	Nei	R	Det anbefales å legge inn sertifikatinnehavers e-postadresse. E-postadresser skal kodes som IA5-strenger. I tillegg kan det legges inn en e-postadresse eller web-adresse for autoriserende organisasjon.
issuerAltName		---	Brukes ikke
subjectDirectoryAttributes		---	Brukes ikke
basicConstraints		---	Brukes ikke i sluttbrukersertifikatene

Feltnavn	Må sjekkes	Forekomst	Kommentar
nameConstraints		---	Brukes ikke
policyConstraints		---	Brukes ikke
cRLDistributionPoints	Nei	M	
extKeyUsage		---	Brukes ikke

Tabell V2.12 Private utvidelser for profesjonssertifikat

Feltnavn	Må sjekkes	Forekomst	Kommentar
AuthorityInfoAccessSyntax	Nei	O	
biometricInfo	Nei	O	
qcStatements	Nei	O	Anbefales å legge inn OID til «egenerklæring» hvis man utsteder kvalifiserte sertifikater
cardNumber	Nei	O	

Vedlegg 3

Brev til utvalget

3.1 Brev fra Skattedirektoratet Statistisk sentralbyrå og Brønnøysundregistrene 10. mai 2000

Innspill om det offentliges behov for entydig identifikasjon ved bruk av digitale signaturer

Bakgrunn

Brønnøysundregistrene (BR) Skattedirektoratet (SKD) og Statistisk sentralbyrå (SSB) samarbeider om en felles satsing innenfor området elektronisk innrapportering fra næringslivet. Det forventes å gi innsparinger og bedre resultater både internt og eksternt. Samarbeidet organiseres i en samarbeidsgruppe sammensatt av deltakere fra de tre etatene. Deltakerne representerer de ulike satsinger innenfor området fra hver enkelt etat. Samarbeidsgruppens styrende organ er Samordningsforum som består av de tre etatenes toppledere.

Så langt har den felles satsingen resultert i utvikling av en såkalt «avgiverløsning» for elektronisk innrapportering via diverse skjema. Dette er en EDI-løsning basert på EDIFACT-standarden elektroniske skjema e-post og med sikkerhetsløsninger for kryptering og digitale signaturer. For store deler av de data det er tale om er det behov for å ha sikkerhet for hvem avgiver er at data eller signatur ikke er endret under transporten eller etter ankomst til mottaker og at dette kan bevises i ettertid. Deler av datasendingen må av diskresjonshensyn også krypteres.

Entydig identifikasjon av personer og organisasjoner

I samhandlingen mellom det offentlige og borgerne i Norge benyttes fødselsnummer som entydig identifikasjon av enkeltpersoner. I overgangen til elektronisk samhandling mener vi det vil ha mange fordeler dersom det fortsatt kan være slik at fødselsnummeret benyttes som entydig identifikasjon. Pålitelighet enkelhet kostnader markedsuavhengighet er stikkord for noen av fordelene. For at dette skal være mulig må sertifikater som utstedes til borgerne kunne knyttes til fødselsnummeret. Slike sertifikater kan kalles borgersertifikater.

Forvaltningsnettsamarbeidet (FNS) sine sertifikater baserer identifiseringen av individer på tilknytningen til en organisasjon. Det er generelt ikke mulig å knytte denne identifiseringen sammen med fødselsnummer.

Det er i det norske markedet flere aktører som ønsker å tilby nasjonale Tiltrodd Tredje Partstjenester (TTP). For at man skal kunne velge fritt mellom disse aktørene må det være mulig å verifisere sertifikater utstedt av andre TTP'er enn den man har avtale med. Slik verifisering løses ved at TTP'ene inngår avtale om såkalt kryssertifisering.

Ved manglende kryssertifisering av borgersertifikater hos de TTP'er som skal operere i det norske markedet vil man favorisere de TTP'er som velges av landsdekkende forvaltningsenheter. Dette fordi det da vil være et krav at borgerne får utstedt sertifikat fra den TTP som er valgt av den forvaltningsenheten man skal ha elektronisk samhandling med. Det begrenser borgernes frihet til å velge sin egen TTP-tjenesteleverandør.

Den avgiverløsningen som i dag er under utprøving baserer seg på bruk av borgersertifikater. De har foreløpig vært utstedt av Posten SDS. Så langt har man trodd at disse sertifikatene vil kunne benytte seg av den kryssertifiseringsavtalen som er inngått gjennom FNS.

Det viser seg imidlertid at den kryssertifiseringen av TTP'er som skjer gjennom FNS ikke løser de samarbeidende etaters behov.

Vi ber derfor om at utvalget i sin utredning tar hensyn til etatenes behov for å kunne identifisere enkeltindivider. Dette kan gjøres ved at det stilles krav til TTP'er om at de skal koble personlige sertifikater

med fødselsnummer og at alle TTP'er skal inngå avtale om kryssertifisering av denne type sertifikater (borgersertifikater).

Norge er i den heldige situasjon at det er bygget opp to nummerserier som entydig identifiserer hhv. alle personer og organisasjoner i landet nemlig fødselsnummer og organisasjonsnummer. Vi mener det vil være nærliggende å benytte forvaltningsenhetene for disse nummerseriene (Det sentrale folkeregisteret og Enhetsregisteret) som navneautoritet i en nasjonal infrastruktur for PKI (Public Key Infrastructure).

Oslo 10. mai 2000

For BrønnøysundregistreneErik Fossum Direktør For Skattedirektoratet Bjarne Hope Skattedirektør For Statistisk sentralbyrå Svein Longva Adm. direktør

3.2 Brev fra Lånekassen 29. juni 2000

Borgerkort for studenter i Norge

I tilknytning til utvalgets arbeid vil Lånekassen benytte anledningen til å komme med noen innspill på områder som vil ha stor betydning for virksomhetens videre utvikling.

Med en aktiv kundegruppe på ca. 700 000 kunder stilles det bl.a. store krav til Lånekassens evne til informasjon og kommunikasjon. Utfordringen understrekes ved begrensede bemanningsressurser og ved erfaringen at manuelle løsninger som telefon- og skrankebetjening samt brev og masseutsendelser i stadig mindre grad vil dekke opp for økte kundekrav om servicetilgjengelighet.

Til nå har Lånekassen kunnet tilby en løsning ved kassafon/kontofon hvor kundene hele døgnet har kunnet hente ut en del personlige kundeopplysninger. I disse dager tilbys nå samme tjeneste via en nettsvarløsning. Strategien for videre modernisering vil være å kunne tilby kundene ytterligere muligheter via internett bla. gjennom innsending og behandling av søknader innbetalings- og utbetalingsordninger støttetjenester for egen beregning/simulering av lånevilkår. Sikkerhetsspørsmål og personlig identifisering gjennom digitale signaturer står her sentralt.

I den forbindelse kan nevnes noen forhold som utvalget kan ta i betraktning i sitt videre arbeid.

Gjennom samarbeidet med de nordiske «lånekasser» er vi kjent med forslaget og planene om å gi en «digital» signatur til alle unge i Danmark. I Finland er noe tilsvarende i gang ved utstedelse av såkalte «borgerkort».

Lånekassen er ofte den første offentlige virksomhet som de unge inngår personlige langvarige kontrakter med. Denne aldersgruppen er i tillegg meget aktiv i bruk av internett og har forventninger om elektroniske tjenester. Det er ønskelig at de unge mellom 16 og 25 år får muligheter for sikker samhandling med Lånekassen gjennom bruk av PKI og kvalifiserte digitale signaturer.

Det vil være ønskelig at utstedelse av «borgerkort» inkluderer de unge og gjerne at denne gruppen blir prioritert og får tildelt et «borgerkort» som et fellesløft fra staten. Det vises spesielt her til utvalgets mandat pkt. 7 om «behovet for elektronisk ID- kort i samband med offentlig tjenesteyting».

Dersom ressurser stilles til rådighet kan allerede aktuelle løsninger kjøpes fra flere leverandører.

Lånekassen vil ellers uttrykke generell støtte til det arbeidet som utvalget utfører.

Med vennlig hilsen

Viktor Valnes

Underdirektør

Kopi: Utvalgsleder Katarina de Brisis

Arbeids- og administrasjonsdepartementet

Postboks 8004 Dep

0030 Os1o

Vedlegg 4

Forklaringer og forkortelser

Applikasjon Brukerprogram

Anvendelse Et brukerprogram eller et datasystem i forvaltningen som benyttes til å løse bestemte oppgaver.

Asymmetriske nøkkelpar Asymmetrisk kryptering benytter to matematisk relaterte men ulike nøkler (en privat og en offentlig nøkkel). Det skal ikke være mulig å utlede den private nøkkelen fra den offentlige.

Attributt En egenskap knyttet til den som eier et sertifikat. De ulike feltene i sertifikatet kan inneholde ett eller flere attributter.

Autentisering En prosess som har som mål å bekrefte en påstått identitet.

Autentisk Ekte.

Autorisere 1) Bemyndige; 2) sanksjonere gjøre rettsgyldig hjemle; 3) tillate; 4) berettige [11].

Avansert elektronisk signatur En elektronisk signatur som

a) Er entydig knyttet til undertegneren

b) Kan identifisere undertegneren

c) Er laget ved hjelp av midler som bare undertegneren har kontroll over og

d) Er knyttet til det elektroniske dokumentet på en slik måte at alle etterfølgende endringer av innholdet i dokumentet kan oppdages.

BI Beskyttelsesinstruksen.

BS 7799 En engelsk standard for administrasjon av informasjonssikkerhet. Del 1 av standarden ble ISO-standarden IS 17799 i 2000 [45].

CA Certification Authority. I denne utredningen brukes begrepet i hovedsak om sertifikatutstedere.

CRL Certificate Revocation List se tilbaketrekkingsliste.

Dataintegritet En egenskap ved data som gjør det mulig å oppdage om data har blitt endret på en uatorisert måte eller pga. feil.

DES Data Encryption Standard – en symmetrisk kryptoalgoritme utviklet i USA.

Digital signatur Et dataelement som følger en elektronisk melding eller et dokument og som binder dokumentet til et individ en maskin eller et datasystem. Det tillater mottakeren å bevise hvor dokumentet kommer fra og om dokumentet er forfalsket.

Dokument En avgrenset og sammenhengende informasjonsmengde framstilt for et bestemt formål. Informasjonen kan bestå av en kombinasjon av tekst data

grafikk bilder og multimedia. Et dokument kan også bestå av flere dokumenter (sammensatte dokumenter).

DSA Digital Signature Algorithm en amerikansk algoritme for digitale signaturer.

EDI Electronic Data Interchange – elektronisk datautveksling.

EESSI European Electronic Signature Standardization Initiative.

Elektronisk ID Et sett med sertifikater og tilhørende private nøkler for hhv. signering autentisering og kryptering.

Elektronisk ID-kort Et smartkort som inneholder en elektronisk ID og har fysisk identifikasjon på forsiden.

Elektronisk saksbehandling En måte å behandle saker på der hele eller deler av prosessen kan utføres med støtte av informasjonsteknologi.

Elektronisk signatur Data i elektronisk form som er knyttet til andre elektroniske data og som brukes til å kontrollere at disse stammer fra den som fremstår som undertegner [52].

ETSI European Telecommunications Standards Institute europeisk standardiseringsorganisasjon innen telekommunikasjonsområdet.

FNS Forvaltningsnettsamarbeidet et samarbeid mellom staten og kommunenene for å tilby forvaltningen løsninger for enkel pålitelig og kostnadseffektiv elektronisk informasjonsutveksling innad i forvaltningen og til forvaltningens brukere.

Formkrav Krav i regelverk om hvordan noe skal gjøres f.eks. ved krav om skriftlighet for å informere oppnå gyldighet oppnå rettsvern og/eller for å oppnå rettsvirkning.

FSP-1 Forvaltningsnettsamarbeidets SertifiseringsPolicy – Nr 1. En sertifikatpolicy utarbeidet av FNS i forbindelse med rammeavtale om digital signatur med tilhørende tjenester.

Hash-algoritme En matematisk metode som beregner en konkret verdi (hash-verdi) ut fra et dokument slik at det er umulig å gjenskape dokumentet ut fra resultatet.

Hash-verdi Et tall som er et resultat av å bruke en hash-algoritme på et elektronisk dokument. Man skal ikke kunne konstruere et annet dokumentet som gir den samme verdien. Man kan si at en hashverdi representerer et elektronisk dokument på en i praksis unik måte.

Hierarki Institusjon organisasjon med fast organisert og strengt ordnet rangfølge.

IDA Interchange of Data between Administrations et EU-program for utvikling av telematikkløsninger mellom medlemslandenenes forvaltninger.

Identifisere 1) Kjenne igjen fastslå identiteten av påvise identitet mellom eller med [6];

2) Regne seg som ett (med) ha samfølelse (med);

3) Påvise identitet mellom (to eller flere ting) bringe under samme begrep [10].

IETF Internet Engineering Task Force et standardiseringsorgan for Internett-utvikling.

Ikke-benekting Uavviselighet. En mekanisme som kan knyttes til elektronisk samhandling og som er slik at de deltakende partene ikke kan benekte å ha deltatt i deler av eller hele samhandlingen.

IKT Informasjons- og kommunikasjonsteknologi.

Infrastruktur Grunnleggende strukturer og systemer som er nødvendige for en organisasjon en samling av organisasjoner eller et land for å fungere på en effektiv måte.

Innholdskryptering En prosess som fører til forvrenging av innholdet i et dokument slik at bare mottaker med riktig nøkkel kan få det fram og lese det.

Integritet se dataintegritet.

ISO International Organization for Standardization.

Key recovery se nøkkelgjenoppretting.

Kryptering se Innholdskryptering.

Kryptografi Hemmelig skjult skrift. Disiplinen som samler prinsippene midlene og metodene for transformasjon av data for å gjemme informasjonsinnholdet hindre uoppdagete endringer og/eller hindre uautorisert bruk.

Kryssertifisering En prosess som fører til at to sertifikatutstedere utsteder sertifikater for hverandres offentlige nøkler. Slike sertifikater kalles kryssertifikater. Utstedelse av kryssertifikater indikerer at utstedere stoler på sertifikater utstedt av den andre.

Kvalifisert elektronisk signatur En avansert elektronisk signatur som er basert på et kvalifisert sertifikat og som er framstilt av et sikkert signaturframstillingssystem.

Noark-standarden Standard spesifikasjon for arkivsystemer i forvaltningen. Fastsettes og forvaltes av Riksarkivaren [57].

Nøkkel En sekvens av symboler som kontrollerer operasjonene for kryptering og dekryptering. Signaturframstillingsdata eller signaturverifiseringsdata.

Nøkkeladministrasjon Generering lagring distribusjon arkivering og anvendelse/bruk av nøkler i samsvar med et regelverk (policy).

Nøkkelgjenoppretting Hente fram en kopi av en krypteringsnøkkel. Dette kan brukes i forvaltningen der man av tjenstlig grunn trenger tilgang til et kryptert dokument. (eng. Key recovery).

OCSP On-line Certificate Status Protocol En metode for kontinuerlig sjekking av status på et sertifikat.

Offentlignøkkel- Teknologi som involverer asymmetrisk kryptering ved bruk av offentlige og

teknologi private nøkler.

OID Object identifier – et unikt nummer på global basis som entydig kan identifisere et dokument et dataelement en meldingstype eller liknende.

PCMCIA Personal Computer Memory Card International Association. Et standardisert innstikkskort til PC-er.

PKI Public Key Infrastructure. En samling av sikkerhetstjenester sikkerhetskomponenter og aktører som gjør det mulig å benytte digitale signaturer i stor skala.

PKIX En arbeidsgruppe under IETF som utarbeider standarder for PKI-bruk på Internett.

Profil En presisering av en standard tilpasset et konkret anvendelsesområde.

Registreringsenhet. En organisasjon(senhet) som påtar seg korrekt å identifisere og autentisere en framtidig eier av offentlige og private nøkler med tilhørende sertifikater.

Rammepolicy Eksempel på et definert kvalitetsnivå for en sertifikatpolicy

Rolle En funksjon en person eller en organisasjon kan ha i en gitt sammenheng.

Rollesertifikat Et sertifikat som knytter en sertifikateier til en bestemt rolle.

RSA Rivest-Shamir-Adleman cryptosystem en bestemt asymmetrisk kryptoalgoritme.

SA Sertifikatautoritet. I denne utredningen brukes begrepet i hovedsak om sertifikatutstedere.

Samtrafikk Samspill mellom ulike sertifikatutstedere. Omfatter tillit til hverandres sertifikater og teknisk samvirke mellom PKI-løsninger som benyttes.

SEIS Sikker Elektronisk Informasjon i Samfunnet. En svensk interesseorganisasjon som bl.a. utarbeidet standarder for elektroniske ID-kort.

Sertifikat En elektronisk legitimasjon for eieren av en privat og en tilhørende offentlig nøkkel som viser at den offentlige nøkkelen tilhører henne.

Sertifikatbruker Den som mottar et digitalt signert dokument med et tilhørede sertifikat og som skal verifisere det mottatte materialet.

Sertifikateier Den som sertifikatet er utstedt til og som har den tilhørende private nøkkelen.

Sertifikatkjede En rekke av sertifikater som brukeren må benytte for å verifisere en signatur som baserer seg på et sertifikat som brukeren ikke kjenner utstederen til.

Sertifikatpolicy Et dokument som inneholder regler for hvordan sertifikater utstedes og behandles og som dermed definerer hvilken tillit man kan ha til sertifikatene. En sertifikatpolicy identifiseres unikt av en OID.

Sertifikatpraksis Et dokument som beskriver organisering ansvarsfordeling og rutiner hos sertifikatutstederen for å implementere regler i en sertifikatpolicy.

Sertifikatprodusent Certification Service Provider (CSP) en operativ enhet som faktisk produserer sertifikater.

Sertifikatutsteder En juridisk person som utsteder sertifikater iht. en sertifikatpolicy.

Sertifisere En prosess for å bekrefte samsvar mellom et produkt et system eller organiseringen av IT-sikkerheten i en organisasjon etter gitte standarder f.eks. IS 1508 Common Criteria eller IS 17799 BS 7799.

Signatur 1) Merke tegn; 2) navnetrekk underskrift [10].

SSL Secure Sockets Layer. Internett-standard for sikker tilkopling til en web-server.

Sporbarhet Et prinsipp i offentlig forvaltning som sikrer at behandlingen av en sak kan rekonstrueres i ettertid. Det skal være mulig å etterspore hva som har skjedd (audit trail).

Standard Normal vanlig. Å standardisere er å fastsette gjøre ensartet [10].

Tilbaketrekkingsliste En liste over sertifikater som ikke lenger er gyldige og som derfor ikke er til å stole på. Utstedes av sertifikatutstederen i gitte tidsintervaller.

Tillit En egenskap ved de tekniske og/eller organisatoriske systemene som samlet utgjør en sikkerhetstjeneste. Denne egenskapen sier noe om i hvor stor grad sikkerhet funksjonalitet og andre tekniske og organisatoriske aspekter er hensiktsmessige og tilstrekkelige i forhold til formålene ved sikkerhetstjenesten.

Tillitskjede Selv om A stoler på B som stoler på C som stoler på D er det ikke sikkert at A bør stole på D eller at D bør stole på B. For mange ledd gir ofte svakere tillit.

Tiltrodd tredjepart TTP-er en virksomhet som yter en eller flere sikkerhetstjenester og som to for hverandre ukjente kommuniserende parter har tiltro til. TTP-ens rolle er å øke tiltroen til at meldinger og transaksjoner overføres til den tilsiktede mottaker til rett sted og på en korrekt måte. I tilfelle tvister skal det finnes metoder for å generere bevis for hendelsesforløpet. TTP-tjenester kan f.eks. være sertifikatutstedelse eller tidsstempling.

Uavviselighet Se ikke-benekting.

UNCITRAL United Nations Commission on International Trade Law. FN's organ som anbefaler felles juridiske løsninger når det gjelder regulering av internasjonal handel.

Undertegner En person som disponerer et signaturframstillingssystem og som handler på vegne av seg selv eller på vegne av en annen fysisk eller juridisk person.

URL Uniform Resource Locator Internett-adresse.

Utvidelse Et tilleggsfelt i et sertifikat.

XML Extensible Markup Language. Standard måte å kode elektroniske dokumenter på slik at det er mulig å gjenkjenne innholdselementer og formater som dokumentet består av.

Vedlegg 5

Referanser

1. Adams Carlisle and Lloyd Steve: *Understanding Public-Key Infrastructure: Concepts Standards and Deployment Considerations*. Macmillan Technical Publishing 1999 ISBN 1-57870-166-x.
2. Arbeids- og administrasjonsdepartementet: *FSP-1:1.0. Forvaltningsnettsamarbeidets SertifiseringsPolicy – Nr. 1* Versjon 1.0 25/8 1999.
3. Arbeids- og administrasjonsdepartementet: *Implementing Public Key Infrastructure in Government. Report from an International Meeting in Oslo 25th – 26th May 2000* AAD 2000.
4. Arkivforskriften: *Forskrift om offentlege arkiv*. 1998-12-11 nr. 1193.
5. Arkivloven: Lov av 4. desember 1992 nr. 126 om arkiv.
6. *Aschehoug og Gyldendals Store norske leksikon* Kunnskapsforlaget 1980.
7. *Aschehoug og Gyldendals Store norske ordbok*. Kunnskapsforlaget 1992. ISBN 82-573-0312-7.
8. *Behov for elektronisk signatur og seritifikater i helsevesenet* Sosial- og helsedepartementet 30.10.2000. Notat til utvalget.
9. Bjerke Lucie og Haakon Søraas: *Engelsk-norsk ordbok* Aschehoug 1963.
10. *Bokmålsordboka* Universitetsforlaget 1997 ISBN 82-00-21763-9.
11. Brekne Tønnes: *Sikkerhet i distribuerte systemer* Unik 27. januar 1999.
12. Denning Dorothy E.: *Information Warfare and Security*. Addison Wesley 1999. ISBN 0-201-43303-6.
13. Deputy Secretary of Defense: *Department of Defense (DoD) Public Key Infrastructure (PKI)*May 6 1999 U07287/99.
14. DG III/B/6: *IDA Architecture Guidelines*. Brussels December 1998. www.ispo.cec.be/ida/ida.html
15. *Digitale signaturer og tiltrodde tredjeparter* Versjon 1.0. 31.12.96 Norsk EDIPRO ISBN 82-7813-004-3.
16. DLM-Forum: *Guidelines on best practices for using electronic information.* Office for official Publications of the European communities 1997. ISBN 92-828-2285-0. http://europa.eu.int
17. Eckhoff T.: *Forvaltningsrett*5. utg. s. 439.
18. *Elektroniska signaturer och elektronisk identifiering för myndigheters e-tjänster* Statskontoret 25. august 2000.
19. *Elektroniske signaturer – Myndighetsroller og regulering av tilbydere av sertifikattjenester* rapport fra utvalg oppnevnt av NHD Nærings- og handelsdepartementet 28. januer 2000.
20. *Elektronisk saksbehandling. Statens generelle kravspesifikasjon* Statskonsult november 1997 http://www.statskonsult.no/public/publiste/inform.htm#sksbeh [lest 23.11.98].
21. *eNorge 2.0. Handlingsplan 2000* Nærings- og handelsdepartementet K-0636B.
22. ETSI: *Baseline Qualified Certificate Policy for Certification Service Providers Issuing Qualified Certficates* ETSI STF 155 T1 Draft E 25 April 2000.
23. ETSI: *Policy requirements for certification authorities issuing qualified certificates* Draft ETSI TS 101 456 v0.015 (2000-11).
24. ETSI: *Qualified Certificate Profile* Draft ETSI TS 101 862 v0.02 (2000-10).

25.EU: *Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures* http://europa.eu.int/comm/internal_market/en/media/sign/index.htm.
26.Federal Bridge Certification Authority: *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)* December 27 2000 Version 1.12: http://csrc.nist.gov/pki.
27.Ford Warwick & Michael S. Baum: *Secure Electronic Commerce* Prentice Hall 1997 ISBN 0-13-476342-4.
28.Forvaltningsnettsamarbeidet: *Navn og identifikatorer i Forvaltningsnettsamarbeidet. Anbefalinger fra arbeidsgruppe (INA-gruppa)* Arbeids- og administrasjonsdepartementet og Kommunenes Sentralforbund 15. juni 1999.
29.*Gyldendals fremmedordbok*. Gyldendal 1969.
30.Hansen A. (UNINETT FAS) A. Lie og J. Ølnes (NR): *FEIDE: FElles Elektronisk ID for UoH-sektoren* Norsk Regnesentral 29. september 2000 ISBN 82-539-0467-3 http://www.nr.no/publications/rapport963.doc.
31.Hanseth Ole: *Information Technology as Infrastructure*. Göteborg Universitet Institutt for informatikk november 1996.
32.*Hantering av certificat och elektroniska signaturer inom statsförvaltningen* Riksskatteverket Rapport 2000:15.
33.Holst Per A.: *Datasikring – Metoder og Prinsipper* Per A. Holst Forlag 1995. ISBN 82-996820-9-0.
34.Hornby A.S.: *Oxford Advanced Learner's Dictionary of Current Engish* Fifth edition 1995. ISBN 0-19-431421-9.
35.Houseley R. W. Ford W. Polk and D. Solo: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* RFC 2459 January 1999 IETF http://www.ietf.org/rfc/rfc2459.txt.
36.http://www.whatis.com/authoriz.htm [sett 26.3.00].
37.IETF: *Internet X509 Public Key Infrastructure Certificate and CRL Profile RFC 2459* January 1999. http://www.ietf.org/rfc2459.txt.
38.*Innføring av elektronisk saksbehandling* Statskonsult 1998 ISBN 82-7483-080-6.
39.ISO/IEC FCD 9796-4 *Information technology – Security Techniques – Digital signature scheme giving message recovery – Part 4: Discrete logarithm based mechanisms* 1998.
40.ISO/IEC IS 9797-1: *Information technology – Security Techniques – Message authentication codes (MACs) – Part 1: Mechanisms using a hash-function* (Revisjon of IS 9797:1994) 1999.
41.ISO/IEC IS 9798-1: *Information technology – Security techniques – Entity authentication: Part 1: General* 1997.
42.ISO/IEC IS 10118-4: *Information technology – Security Techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic*1998-07-01.
43.ISO/IEC DTR 14516: *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*. December 2000.
44.ISO/IEC FD 15945: *Specification of TTP Services to support the application of Digital Signatures.* December 2000.
45.ISO/IEC IS 17799: *Information security management – Code of Practice for information security management* 2000.
46.JB Consult: *Elektroniske ID-kort* 3. oktober 2000.

47. *Kartleggingsprosjektet. Kartlegging av bestemmelser i lover forskrifter og instrukser som kan hindre elektronisk kommunikasjon* Nærings- og handelsdepartementet Prosjektrapport juni 2000 publikasjonsnummer K-0628 B. http://odin.dep.no/nhd/norsk/publ/rapporter/indeks-b-n-a.html.
48. Khare Rohit and Adam Rifkin: *Weaving a Web of Trust* WorldWideWeb Journal vol. II issue 3 summer 1997 http://www.w3journal.com/7/s3.rifkin.wrap.html [sett 13.3.00].
49. Kunnskapsforlagets blå ordbøker: *Engelsk-norsk*. Kunnskapsforlaget 1996. ISBN 82-573-0570-7.
50. Lie Anund og Gjertrud Pedersen: *Web-skjemaløsninger for digital signatur for SLN* Norsk Regnesentral Notat GEM/02/2000 14. april 2000. http://www.nr.no.
51. Lov 2000-04-14 nr 31: *Lov om behandling av personopplysninger (personopplysningsloven)* http://www.lovdata.no.
52. *Lov om elektronisk signatur* Innst. O. nr. 41 (2000–2001).
53. *Meldingssikkerhet: Tiltrodde tredjeparter og digitale signaturer* Norsk EDIPRO 7.12.94.
54. Menezes Alfred J. Paul C. van Oorschot & Scott A. Vanstone: *Handbook of Applied Cryptography* CRC Press 1996. ISBN 0-8493-8523-7.
55. Myers M. R. Ankney A. Malpani S. Galperin and C. Adams:*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* RFC 2560 June 1999 IETF http://www.ietf.org/rfc/rfc2560.txt.
56. Myrvang Per Harald: *An Infrastructure for Authentication Authorization and Delegation* Cand.Scient. Thesis in Computer Science Universitetet i Tromsø 22. mai 2000.
57. *NOARK-4 Norsk arkivsystem versjon 4. Del 1: Funksjonsrettet beskrivelse og kravspesifikasjon* Riksarkivaren 1999 Kommuneforlaget AS. ISBN 82-446-0628-2.
58. Nærings- og handelsdepartementet: St.meld. nr. 41 (1998–99) *Om elektronisk handel og forretningsdrift* http://odin.dep.no/nhd/norsk/publ/stmeld/index-b-n-a.html.
59. *Om lov om elektronisk signatur*Ot.prp. nr. 82 (1999–2000) Nærings- og handelsdepartementet: http://odin.dep.no/odin/norsk/publ/stprp/index-b-n-a.html.
60. PKI Consulting Services AS: *Samtrafikk mellom sertifikattjenester* 28.11.2000. http://www.statskonsult.no/prosjekt/pki/index.htm.
61. PKI Consulting Services AS: *Sertifikatprofiler* 17.1.2001.
62. Riisnæs Rolf: *Skisse til retningslinjer for bruk av digital signatur og kryptering i offentlig forvaltning – notat til PKI-utvalget* Institutt for rettsinformatikk Universitetet i Oslo 27.11.00. http://www.statskonsult.no/prosjekt/pki/index.htm
63. Rådet for IT-sikkerhet: *Digitale signaturer gir tillit til elektronisk kommunikasjon*: *Forslag til tiltak for aksept og utbredelse.* Rapport med forberedende utredning fra arbeidsgruppe oppnevnt av Nærings- og handelsdepartementet avgitt til Rådet for IT-sikkerhet 30.11.98.
64. Rådet for IT-sikkerhet: *Sertifisering av IT-sikkerhet i produkter systemer og organisasjoner* Sluttrapport 13. november 1997.
65. Rådet for IT-sikkerhet: *Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk* 10.11.97.
66. Seip Anne Karen Bonnevie: *Langtidslagring av digitalt signerte dokumenter* hovedfagsoppgave i informatikk Universitetet i Oslo 1999 http://www.nr.no/publications/annikken-oppg.ps.

67. Seipel Peter: *Documents Related to the Swedish EDI-system for Custom Authorities* s. 141 i Kilian Wolfgang & Wiebe Andreas (red.): *Data Security in Computer Networks and Legal Problems Proceedings of a Working Conference in Hannover/Germany* on September 23 24 1991 Beiträge zur juristischen Informatic Band 17 1992 S. Toeche-Mittler Verlag Darmstadt ISBN 3-87820-087-0.
68. SEIS-S10: *SEIS Certificate Policy* SEIS June 1998 http.//www.seis.se/
69. SESAM-prosjektet: *Sikker elektronisk samhandling på Aker sykehus* KITH Rapport 22/00. ISBN 82-7846-102-3.
70. Statssekretærutvalget for IT: *Den norske IT-veien. Bit for bit* Samferdselsdepartementet 1996. ISBN 82-7452-016-5.
71. *Stor engelsk-norsk ordbok* Cappelen 1988.
72. Stormorken Odd: *Nasjonalt ID-kort* Norsik 23.2.2000.
73. Thomas Stephen: *SSL and TLS Essentials. Securing the Web*. Wiley 2000. ISBN 0-471-38354-6.
74. UN/EDIFACT: http://www.c-lab.de/~aisch/edifact/edi/www.premenos.com/unedifact/untdid/d300_s.html [sett 29.10.99]
75. Wahl M. T. Howe and S. Kille: *Lightweight Directory Access Protocol (v3)* RFC 2252 December 1997 IETF http://www.ietf.org/rfc/rfc2252.txt.
76. Webster's *New World Computer Ordbok*. Schibsted 1984. ISBN 87-88165-13-2.
77. Wright Benjamin: *Electronic Signatures. Making Electronic Signatures a Reality.* Computer Law & Security Report Vol. 15 no. 6 1999. Elsevier Science Ltd.
78. http://www.whatis.com/pki.htm sett 27.4.00.
79. Ølnes Jon: *Behov for sertifikattjenester for norsk offentlig sektor*. Norsk Regnesentral NR Notat: OMNI/03/99 desember 1999.

Vedlegg 6

Stikkordregister

- Brønnøysundregistrene
- Canada
- CEN
- CEN
- Cloud Cover
- Common Criteria
- CRL
- Danmark
- Dataintegritet
- Datasikkerhetsdirektivet
- Datasikkerhetsdirektivet
- Datatilsynet
- Datatilsynet
- Dekryptere
- Den norske IT-veien
- Digitale signaturer
- Direktoratet for arbeidstilsynet
- DnB
- Domene
- Døgnåpen forvaltning
- Døgnåpen forvaltning
- døgnåpen forvaltning
- EAL 4
- EBASUS
- EDI
- EDI
- EDNA
- EESSI
- EESSI
- EESSI
- eEurope
- eEurope-paraplyen
- EID-kort

- EID-kort
- ELEKTRA
- ELEKTRA
- Elektronisk forvaltning
- Elektronisk innrapporteringKommune og statNæringslivet
- Elektronisk pass
- Elektronisk saksbehandling
- Elektronisk signatur
- Elektroniske identitetskort
- Elektroniske identitetskort
- Elektroniske identitetskort
- Elektroniske spor
- ELMER
- Engangsnøkkel
- Enhetsregisteret
- Enhetsregisteret
- Enhetsregisteret
- eNorge
- Entrust
- eRegel-prosjektet
- eRegel-prosjektet
- eRegel-prosjektet
- ErgoGroup
- ErgoGroup
- ErgoGroup
- ErgoGroup
- ETSI
- EU
- EU/EØS
- Finansdepartementet
- Finansdepartementet
- Finland
- Finland

- Finland
- FINUID
- FINUID
- FN
- Folkeregisteret
- Folkeregisteret
- Folkeregisteret
- Folkeregisteret
- Forum for digitale signaturer
- Forum for digitale signaturer
- Forum for digitale signaturer
- Forum for IT-sikkerhet
- Forvaltningsloven
- Forvaltningsnettsamarbeidet
- Forvaltningsnettsamarbeidet
- Forvaltningsnettsamarbeidet
- ForvaltningsnettsamarbeidetKryssertifiseringRammeavtaler
- ForvaltningsnettsamarbeidetRammeavtaler
- FSP-1
- FSP-1
- FSP-1
- Fødselsnummer
- Fødselsnummer
- Fødselsnummer
- Fødselsnummer
- Government Paperwork Elimination Act
- Hash-algoritme
- Helsepersonellregisteret
- Helsepersonellregisteret
- Helsesektoren
- Hierarkisk sikkerhetsmodell
- IDA-programmet
- Identifikatorer

- Identifisere
- IdentifisereSertifikateier
- IDENTRUS
- ID-kort
- ID-kort
- IDUN
- Ikke-benekting
- Ikke-benekting
- Ikke-benekting
- Ikke-benekting
- Integritet
- Japan
- Kartleggingsprosjektet
- Kartleggingsprosjektet
- Kartleggingsprosjektet
- Kataloger
- Kildeautentisering
- KITH
- Kommunal- og regionaldepartementet
- Kommunal- og regionaldepartementet
- Kommunal- og regionaldepartementet
- Kommunal- og regionaldepartementet
- Kommunenes Sentralforbund
- Kommunenes Sentralforbund
- Konfidensialitet
- Konfidensialitet
- Konkurransevridning
- KOSTIT
- KOSTRA
- KOSTRA
- Kryptere
- Kryptere
- Kryptere

- Kryptere
- Krypteringsnøkler
- KrypteringsnøklerTilgang
- Kryssertifisering
- Kryssertifisering
- Kryssertifisering
- Kryssertifisering
- Kryssertifisering
- Kryssertifisering
- Kryssertifisering
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifisert sertifikat
- Kvalifiserte elektroniske signaturer
- Kvalifiserte elektroniske signaturer
- Kystverket
- Langtidslagring
- LDAP
- Lov om elektronisk signatur
- Lånekassen
- Metakatalog
- Midt-Norsk helsenett
- Miljøverndepartementet
- Ministerrådet
- MVA 3

- Mykt sertifikat
- Navnerom
- Nederland
- NHD
- Norges vassdrags- og energidirektorat
- Norsk Hydro
- Norsk Hydro
- Norsk Hydro
- Norsk Tipping
- Norske Skog
- Nærings- og handelsdepartementet
- Nærings- og handelsdepartementet
- Nærings- og handelsdepartementet
- Nøkkel
- Nøkkelløst sertfikat
- Object IDentifier
- OECD
- OECD
- OECD
- Offentlig forvaltning
- Offentlig nøkkel
- Offentlig nøkkelTilgang til
- Offentlig personsertifikat
- Offentlig personsertifikat
- Offentlig personsertifikat
- Offentlige tjenester på Internett
- Offentlignøkkel-kryptografi
- Organisasjonsnummer
- Orkla
- Patentstyret
- Patentstyret
- Patentstyret
- Personopplysningsloven

- Personopplysningsloven
- Personvern
- Personvern
- Personvern
- Personvern
- Personvern
- PKI
- PKI
- Policy mapping
- Politikk
- POLK
- Post- og teletilsynet
- Post- og teletilsynet
- Post- og teletilsynet
- Post- og teletilsynet
- Post- og teletilsynet
- Posten SDS
- Posten SDS
- Privat nøkkel
- Profesjonssertifikat
- Profesjonssertifikat
- Profesjonssertifikat
- Profil
- Profil
- PSA
- Pseudonyme sertifikater
- Public Key Infrastructure
- Rammeavtaler
- Rammeavtaler
- Rammepolicy
- Registereringsenhet
- Riksarkivet
- Riksarkivet

- Rikstrygdeverket
- Rikstrygdeverket
- Risikovurdering
- Risikovurdering
- RITS
- RITS
- Rollesertifikater
- Rådet for IT-sikkerhet
- Samordningsfunksjon
- Samtrafikk
- Samtrafikk
- Samtrafikk
- Samtrafikk
- Samtrafikktjenester
- Samtrafikktjenester
- Schengen-samarbeidet
- Selvangivelse
- Sertifikat
- Sertifikat
- Sertifikatbruker
- Sertifikateier
- Sertifikathierarki
- SertifikatinnholdTolkning
- Sertifikatkjede
- Sertifikatkjede
- Sertifikatpolicy
- Sertifikatpolicy
- Sertifikatpolicy
- Sertifikatpolicy
- Sertifikatpraksis
- Sertifikatpraksis
- Sertifikattyper
- Sertifikatutsteder

- Sertifikatutsteder
- SESAM
- Sesjonsnøkkel
- Signaturframstillingsdata
- Signaturframstillingsdata
- Signaturframstillingssystem
- Signaturframstillingssystem
- Signaturframstillingssystem
- Signaturframstillingssystem
- Signaturframstillingssystem
- Signaturverfiseringsdata
- Sikkerhetsinstruksen
- Sikkerhetskomponenter
- Sikkerhetsloven
- Sikkerhetsloven
- Sikkerhetsnivå
- Sikkerhetsnivå
- Sikkerhetsnivå
- SikkerhetsnivåHierarkisk
- Sikkerhetstjeneste
- Skattedirektoratet
- Skattedirektoratet
- Skattedirektoratet
- Skattedirektoratet
- SLN-prosjektet
- SLN-prosjektet
- SLN-prosjektet
- Sosial- og helsedepartementet
- Sosial- og helsedepartementet
- SSB
- SSB
- SSL
- Statens bygningstekniske etat

- Statens dataforum
- Statens dataforum
- Statens kartverk
- Statens lånekasse
- Statistisk sentralbyrå
- Statistisk sentralbyrå
- Statoil
- Statoil
- Storbritannia
- Strålfors
- Strålfors
- Strålfors
- Svartelisting
- Sverige
- SWIFT
- Symmetrisk kryptografi
- Sårbarhet
- TAKISAI
- TAKISAI
- Teknisk samvirke
- Telenor
- Telenor
- Telenor
- Telenor
- Tidsinvariant
- Tidsinvariant informasjon
- Tilbaketrekkingsinformasjon
- Tilbaketrekkingsinformasjon
- Tilbaketrekkingslister
- Tilbaketrekkingslister
- TilgangKrypteringsnøkler
- Tilgang
- Offentlige nøkler

- TilgangTilbaketrekkingsinformasjon
- Tillit
- Tillit
- Tillitskjede
- Tillitsstrukturer
- Tillitsstrukturer
- Tilsyn
- Tilsynsmyndighet
- Tiltrodd tredjepart
- TolkeSertifikatinnhold
- Torvundutvalget
- Torvundutvalget
- TTP
- Unik identifikator
- Unik identifikatorTolke
- USA
- Utenriksdepartementet
- Utlendingsdirektoratet
- Varemerker
- Vegdirektoratet
- Vegdirektoratet
- Vegdirektoratet
- Verifisering
- VeriSign
- VeriSign
- Virksomhetssertifikat
- Virksomhetssertifikat
- Virksomhetssertifikat
- Virksomhetssertifikat
- WTO
- ZebSign