Digitale signaturer gir tillit til elektronisk kommunikasjon

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.

Innhold

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

---

Rådet for IT-sikkerhet

Digitale signaturer gir tillit til elektronisk kommunikasjon

Forslag til tiltak for aksept og utbredelse

Digitale signaturer for tillit til elektronisk kommunikasjon. Forslag til tiltak.

Del i: »En forberedende utredning»

1. Innledning

1.1 Bakgrunn

Denne rapporten er laget på oppdrag fra Rådet for IT-sikkerhet (RITS). Rådet for IT-sikkerhet er primært et forum der myndigheter utveksler informasjon og kan foreslå tverrsektorielle tiltak om informasjonssikkerhet knyttet til informasjonsteknologi (IT). Berørte virksomheter kan inviteres etter behov. Rådet ligger under Nærings- og handelsdepartementet (NHD), flyttet fra daværende Planleggings- og samordningsdepartementet ved årsskiftet 1997-98. Bakgrunnen er at Nærings- og handelsdepartementet fra dette tidspunktet fikk ansvaret for den overordnede samordningen av regjeringens IT-politikk, herunder samordning knyttet til IT-sikkerhet som berører politikkområder under ulike departementer og samfunnet som helhet. Arbeids- og administrasjonsdepartementet har fortsatt ansvaret for samordning av IT i statsforvaltningen, inkludert IT-sikkerhet. Fagdepartementenes linjeansvar i IT-politikken forblir uforandret.

Tidligere arbeider i regi av RITS er:

- Infrastruktur for sikker kommunikasjon - TTP-tjenester og offentlig engasjement, NR-notat OMNI/01/97, 3 april 1997 (bakgrunnsnotat, ikke rådsbehandlet)
- Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner, Sluttrapport 13 november 1997 (rådsbehandlet og oversendt NHD)

- Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk, Forsvarets overkommando/Sikkerhetsstaben 10 november 1997 (rådsbehandlet og oversendt NHD)

De to sistnevnte arbeidene er oversendt NHD med Rådets kommentarer, tilslutning og anbefalinger, for videre saksbehandling på ordinær måte.

I St prp nr 1 1998-99 for Nærings- og Handelsdepartementet 5.10.98 foreslår Regjeringen å etablere to nye sertifiseringsordninger: en for sertifisering av IT-sikkerhet i produkter og systemer og en for sertifisering av IT-sikkerhet i organisasjoner. For 1999 er det foreslått avsatt 5 millioner kroner over NHDs budsjett til etablering og drift av de to nye sertifiseringsordningene for IT-sikkerhet.

Denne rapporten føyer seg inn i rekken ovenfor, og supplerer disse arbeidene. Det anbefales å se rapportene i sammenheng. Til sammen utgjør de deler av en helhet som fokuserer på ulike tiltak som anses nødvendige for å fremme tillit til elektronisk informasjon i informasjonssamfunnet.

RITS ønsket primo 1998 å få nærmere klargjort spørsmål som knytter seg til organisering og bruk av digitale signaturer og tjenester fra såkalte tiltrodde tredjeparter (TTP) for å legge til rette for sikker elektronisk kommunikasjon. Rådet ønsket derfor en arbeidsgruppe til å lage en forberedende utredning, som grunnlag for en anbefaling fra Rådet om behovet for konkrete handlinger eller ytterligere utredninger/avklaringer på området, og hvilke hensyn som bør ivaretas.

1.2 Mandat og sammensetning av arbeidsgruppe

Et oppnevningsbrev ble sendt fra Nærings- og handelsdepartementet 05.02.98 til det som ble arbeidsgruppen for utredning om digitale signaturer. Departementet viste til at Rådet for IT-sikkerhet har anbefalt at det settes i gang et slikt arbeid.

Mandatet gjengis i sin helhet nedenfor, i kursiv:

Rådet for IT-sikkerhet 28.01.98

Sekretariatet

Mandat og sammensetning for arbeidsgruppe for å utrede problemstillinger vedrørende digitale signaturer mv.

Bakgrunn

Rådet for IT-sikkerhet ønsker å få nærmere klargjort spørsmål som knytter seg til organisering og bruk av digitale signaturer og tjenester fra såkalte tiltrodde tredjeparter (TTP) for å legge til rette for sikker elektronisk kommunikasjon. Rådet nedsetter derfor en arbeidsgruppe til å forestå en forberedende utredning. Det legges til grunn at utredningen skal tjene som grunnlag for en anbefaling fra rådet om behovet for konkrete handlinger eller ytterligere utredninger/avklaringer på området, og hvilke hensyn som bør ivaretas. Arbeidsgruppen skal gi en oversikt over området, avklare problemstillinger og presentere dem på en lettfattelig måte, uten å gå i dybden på de enkelte punktene.

Utredningens innhold

Arbeidsgruppen skal avklare sentrale problemstillinger som reises i forbindelse med alminnelig, sivil bruk i samfunnet av digitale signaturer og tjenester fra tiltrodde tredjeparter. Nedenfor følger momenter som ønskes belyst.

1. *Kort oversikt over generelle behov og bruksområder for digitale signaturer og TTP-tjenester. Hvilke TTP-tjenester er aktuelle, - i hvilke sammenhenger?*

2. *Hvilke initiativer og konkrete forsøk med digitale signatur/TTP finnes i Norge og internasjonalt?*

3. *Foreliggende og evt alternative teknologiske løsninger for digital signatur og TTP, herunder konkrete produkter og tjenester som nå er på markedet, eller er i ferd med å bli etablert som tilbud i markedet.*

4. *Hva er nødvending infrastruktur og rammebetingelser for alminnelig utbredelse av sikker elektronisk kommunikasjon med bruk av digital signatur, - teknisk, organisatorisk, juridisk, evt annet, såvel nasjonalt som internasjonalt? Hva finnes i dag, og hva må evt skapes, og av hvem? Hva kan markedet og brukerne selv gjøre, og hva kan eller bør sentrale myndigheter gjøre?*

Dette innebærer vurdering av blant annet følgende punkter:

- *eksisterende eller kommende nasjonale og internasjonale krav som digitale signaturer og TTP-tjenester må, bør, eller kan tilfredsstille nøkkeladministrasjon med tilhørende tjenester, herunder sertifisering*
- *kryssertifisering, inkludert kryssertifisering mot aktører i andre land*
- *ansvarsspørsmål, og andre rettslige spørsmål typer av roller i markedet, herunder tjenesteleverandørenes, sentrale myndigheters*

- *forholdet til området for innholdskryptering,*
- *koordineringsrolle nasjonalt og i forhold til andre land, brukere, mm.*

Arbeidsgruppen bør også vurdere om det finnes alternative måter å sikre tillit til autentisering og integritet enn gjennom nasjonale og internasjonale sertifiseringsstrukturer. Situasjonen i andre land bør omtales.

Sammensetning

Gruppen sammensettes slik:

1. *Amund Eriksen, Rådet for IT-sikkerhet (RITS), sekretariatet*
2. *Knut Erik Sæther, Justisdepartementet, Lovavdelingen*
3. *Rolf Riisnæs, Institutt for rettsinformatikk (IRI), Universitetet i Oslo*
4. *Olav Torvund, Institutt for rettsinformatikk (IRI) , Universitetet i Oslo*
5. *Torbjørg Hogsnes, Sosial- og helsedepartementet*
6. *Jens Nørve, Arbeids- og administrasjonsdepartementet*
7. *Arne Økstad, Kommunal- og regionaldepartementet*
8. *Endre Grøtnes, Statskonsult*
9. *Lars Gunnarson, Forsvarets overkommando/sikkerhetsstaben*
10. *Jørn A. Arnesen, Datatilsynet*
11. . *Finn-Olaf Berg, Posten SDS*
12. *Harald Rønning, Telenor Bedrift*
13. *Asbjørn Hovstø, Norsk EDIPRO*
14. . *Knut Kvalheim, Bankenes standardiseringskontor*
15. . *Petter Christensen, Næringslivets sikkerhetsorganisasjon*
16. . *Leif Nilsen, Thomson-CSF Norcom (tidligere Alcatel Telecom Norway)*
17. *Ole Snerte, Norsk Hydro*

Administrative forhold

- *Sekretæren i RITS leder gruppen.*
- *Gruppen velger selv arbeidsmåte og organisering.*
- *Arbeidsgruppen gis et driftsbudsjett.*

- *Delutredninger kan innhentes, innenfor rammene av driftsbudsjettet.*
- *Arbeidsgruppens medlemmer honoreres etter satsene for utvalgsarbeid i staten. Oversikt over medgåtte timer utfylt på skjema for utvalgsarbeid sendes rådets sekretær.*
- *Reiser til utlandet skal forelegges departementet før de utføres.*
- *Arbeidsgruppen avleverer rapport til Rådet for IT-sikkerhet innen 15 mai 1998.*

Det vises bl.a. til følgende arbeider, som vedlegges:

- *Digitale signaturer og tiltrodde tredjeparter, versjon 1.0, desember 1996, prosjektrapport i regi av Norsk EDIPRO og Norges forskningsråd. Med sammendrag av høringsuttalelser.*
- *Infrastruktur for sikker kommunikasjon - TTP-tjenester og offentlig engasjement, april notat utarbeidet av Norsk Regnesentral, Jon Ølnes, på oppdrag fra Rådet for IT-sikkerhet.*
- *Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk, Rådet for IT-sikkerhet, FO/S 1997-11-10.*
- *OECD: OCDE/GD(97)204: Cryptography Policy: the Guidelines and the Issues*
- *EU: COM (97) 503: Towards a European Framework for Digital Signatures and Encryption.*

Kommentarer til sammensetningen:

Amund Eriksen sluttet som sekretær for Rådet for IT-sikkerhet i oppdragsperioden, og gikk pr 1.6 over til Aksjon 2000, et prosjekt i regi av Nærings- og handelsdepartementet.

Jens Nørve ble fra 1.8.98 ny sekretær for Rådet for IT-sikkerhet, og fortsatte som deltaker i arbeidsgruppen på det grunnlaget.

Ny deltaker fra Arbeids- og administrasjonsdepartementet i sluttfasen ble Katarina de Brisis. Hun ledet samtidig en gruppe under Forvaltningsnettprosjektet som bl a utformet kravspesifikasjon for sertifiseringstjenester og systemer for digitale signaturer og innholdskryptering, parallelt med arbeidet i denne digital-signatur arbeidsgruppen.

1.3 Om arbeidet og mandatet

Første møte ble holdt 18.2. 1998. I tillegg til plenumsmøtene organiserte arbeidsgruppen seg i fire grupper, fordelt på temaene næringsliv, forvaltning, teknikk og jus. Representanter fra hver temagruppe har sammen med arbeidsgruppens leder utgjort et redaksjonsutvalg. Temagruppene har holdt møter mellom plenumsmøtene. Det er avholdt en rekke møter, hvorav 8 i den fulle arbeidsgruppen. Alle grupper og personer har bidratt med et antall skriftlige innspill, med vesentlige bidrag fra Leif Nilsen, Asbjørn Hovstø og Rolf Riisnæs i sluttfasen.

Olav Torvund, Institutt for rettsinformatikk, og Rune Hagen, Bankenes Standardiseringskontor, har bidratt som kvalitetssikrere.

Den opprinnelige tidsrammen ble av flere grunner overskredet. Departementet og arbeidsgruppen ble enige om opplegget for gjennomføringen innenfor en ny(e) tidsramme(r).

Området er omfattende og i rask utvikling. Vi har prøvd å gi en kortfattet, pedagogisk oversikt på et overordnet nivå, for lettere å formidle bakgrunnen for de tiltak vi foreslår. Dette går ut over presisjonsnivået, men er ment å etterleve oppdraget gitt i mandatet.

Ut fra dette har arbeidsgruppen forsøkt å besvare mandatets hovedspørsmål, som vi mener ligger i punkt 4, om hva som er nødvendig infrastruktur og rammebetingelser for alminnelig utbredelse av sikker elektronisk kommunikasjon med bruk av digital signatur, - teknisk, organisatorisk, juridisk... så vel nasjonalt som internasjonalt. Med begrepet infrastruktur forstår vi de forhold, den oppbygging, eller den sammensetning, av underliggende karakter, som man er avhengig av for å oppnå målsetningen om alminnelig utbredelse. Disse underliggende forholdene kan bestå av både tekniske, organisatoriske og juridiske elementer.

Det er noen spørsmål i mandatet vi ikke har svart på, eller har besvart knapt. Forhold rundt kryssertifisering er blitt meget kort besvart. Det både kunne og burde ha vært sagt mer. Det som sies er nærmest at det er mye som gjenstår på området for kryssertifisering, ikke minst fordi de aktuelle grunnlag for kryssertifisering ikke er kommet spesielt langt. Videre er det i mandatets punkt 3 sagt at vi skal si noe om »alternative teknologiske løsninger for digital signatur og TTP», ikke bare de foreliggende løsninger. Vi bes til slutt i mandatet om å »vurdere om det finnes alternative måter å sikre tillit til autentisering og integritet enn gjennom nasjonale og internasjonale sertifiseringsstrukturer».

Det er arbeidsgruppens opplevelse at det pr i dag ikke foreligger reelle alternativer med tilsvarende funksjonalitet og sikkerhet, uten at vi kan påberope oss å ha gjennomført et omfattende arbeid for å undersøke saken. Synspunktet er basert på hva gruppens generelle kunnskaper tilsier. Begrepet »elektronisk» signatur rommer åpenbart muligheten for alternativer til det som pr i dag er en veldefinert teknologi under navnet »digital» signatur, men vi kjenner ikke til at alternative teknikker nå skulle være konkurransedyktige mht sikkerhet og funksjonalitet i forhold til digitale signaturer. Biometriske teknikker for identifisering av individer finnes, men er kommet kortere i utviklingen, og har neppe sammenlignbar sikkerhet, og ikke sammenlignbar funksjonalitet eller bruksområde. Det er heller ikke noe som tyder på at dette vil forandre seg med det første. Selv om biometriske metoder og produkter snart skulle bli billige, effektive og utbredte på markedet, vil de ikke kunne bidra til annet enn å identifisere personer, kanskje som en av flere komponenter i en fremtidig løsning som også inkluderer bruk av digitale signaturer. De biometriske metodene kan ikke koble avsenderens identitet til innholdet i meldingen på en sikker måte. Applikasjoner, servere og diverse utstyr vil dessuten fortsatt måtte identifiseres ved andre teknikker, der digitale signaturer i en overskuelig fremtid etter all sannsynlighet er det som er best egnet.

På den annen side: utviklingen går generelt fort, og »fremtiden» kjenner vi lite til før den har vært her en stund. Vi minner om at grunnlaget for offentlig nøkkel-kryptografi, som digitale signaturer (og denne rapporten) bygger på, ble presentert allerede i 1976, [1] og at metoden for en sentral algoritme for digitale signaturer (RSA) ble publisert i en artikkel i 1978 av forfatterne Rivest, Shamir og Adleman. Og nå begynner det hele snart å virke.....!

1
Med Stanford University, Hellman, Diffie og Merkle som sentrale aktører.

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Rådet for IT-sikkerhet

Digitale signaturer gir tillit til elektronisk kommunikasjon

Forslag til tiltak for aksept og utbredelse

---

2. Sammendrag

Rapporten er delt inn i fire hoveddeler:

- »En forberedende utredning» (del I)
- Behovet for sikkerhetstjenester (del II)
- Hva er nødvendig infrastruktur og rammebetingelser for »alminnelig» utbredelse? (del III)
- Anbefalinger om tiltak (del IV)

I tillegg kommer utfyllende vedlegg: ordliste, forkortelser og referanser (vedlegg 1), behov uttrykt gjennom forsøk og initiativer i Norge (vedlegg 2), kort oversikt over standarder (vedlegg 3), kort oversikt over aktuelle produkter og TTP-tjenester i Norge (vedlegg 4), oversiktsscenario - elektronisk samhandling - potensiale og utfordringer (vedlegg 5). Som lesetips til de med minst tid til disposisjon peker vi på følgende: Hvert av kapitlene 3 til og med 9 avsluttes med kortfattede kommentarer og en konklusjon (se innholdsfortegnelsen for oversikt). Sammen med dette sammendraget og tiltakskapittel 9 gir lesing av dette den raskeste og letteste måten å få oversikt over rapporten på. Mest og best informasjon får man imidlertid selvfølgelig ved å lese hele rapporten!

Del I inneholder de vanlige opplysninger om opprettelse, mandat, sammensetning og tolkning av mandat, samt en presisering av noe av det som ikke besvares særlig mye i forhold til mandatets krav. Rapportens inndeling og innhold for øvrig er et forsøk på nettopp å besvare mandatet. Mandatet går ut på å gjøre et forarbeid, - peke ut hvilke biter av helheten det etter arbeidsgruppens mening er viktig å arbeide videre med eller få på plass. Rapporten er vårt råd til Rådet for IT-sikkerhet, RITS, som er vår oppdragsgiver. Målet er ikke rapporten i seg selv, men de aktivitetene den kan føre til.

Del II: Behovet for sikkerhetstjenester, starter i kapittel 3 med spørsmålet: hva snakker vi om? De mest sentrale begrepene på sikkerhetsområdet forklares. Begrepet sikkerhetstjenester brukes som et teknologinøytralt fellesbegrep på en rekke forhold eller behov (3.1), som kan ivaretas av teknologibaserte mekanismer eller teknikker (3.2). I en åpen verden med mange aktører som trenger å kommunisere tillitsfullt med hverandre uten å kjenne hverandre på forhånd, er det nødvendig å organisere disse teknikkene slik at de passer sammen. Til det trenger man det som kalles en infrastruktur (3.3). Slik infrastruktur kan bestå av tekniske, organisatoriske, rettslige og politiske elementer. I kapittel 3.3 er det fokus på de tekniske

sidene (elektroniske nøkler som skal være offentlig tilgjengelige for alle i »den åpne verdenen»), omtrent som telefonnumre (som ikke er så anvendelige hvis de er utilgjengelige, eller ikke passer sammen på tvers av grenser mellom leverandører, bransjer, forvaltninger og nasjoner). Utviklingen er i høy grad teknologidrevet. Det er også en grunn til å interessere seg for hva som skjuler seg bak noen av de mest sentrale tekniske begrepene på området.

Etter denne lille innføringen peker rapporten på områder der behov for de omtalte løsningene er blitt uttrykt på ulike måter. Vi begynner i den delen av utlandet som må sies å ha størst betydning for oss, EU jf. EØS-avtalen, samt OECD. Deretter ser vi på våre hjemlige behov slik de er formulert av de to siste regjeringene i Norge. EUs og OECDs sterke vektlegging og satsing, og måten både regjeringen Bondevik og regjeringen Jagland har formulert meget klare begrunnelser og mål for dette området på, er gjengitt i kapitlene 4.1 og 4.2. Den politiske bevisstheten i EU, OECD og i Norge om behovene må kunne sies å være meget høy, og viljen til å få frem løsninger er sterk.

Stort klarere »marsjordre» for å få frem sikre elektroniske løsninger enn det de to siste norske regjeringene har gitt, skal en lete lenge etter. Her er det ingen tvil om at man ser sterke behov for sikre elektroniske løsninger både nasjonalt, regionalt (f eks europeisk) og globalt. Det er grunn til å minne om at man arbeider i store deler av verden med å dekke tilsvarende behov som de vi gjennomgår. For våre formål anser vi det imidlertid tilstrekkelig å begrense oss til EU, OECD og Norge. Hva så med markedet på offentlig og privat sektor for disse forholdene? Er man opptatt av de samme tingene i »det virkelige livet»? Trenger oljeindustrien, handelslivet, betalingsformidling, helsesektor og offentlig forvaltning løsninger for sikker kommunikasjon i den elektroniske verdenen? Dette gir vi eksempler på i kapittel 4.3 (noe utdypet i vedlegg 2).

Mandatet spør om hva som er nødvendig infrastruktur og rammebetingelser for alminnelig utbredelse av sikker elektronisk kommunikasjon med bruk av digital signatur, - teknisk, organisatorisk og juridisk. Det er et stort spørsmål. Behovskapitlet omtalt foran gjengir noen av grunnene til at spørsmålet er stilt.

I del III: Hva er nødvendig infrastruktur og rammebetingelser for »alminnelig» utbredelse?, ser vi på de bitene i puslespillet som til sammen vil utgjøre svaret: I Kapittel 5 pekes det kort på viktige områder der vi pr i dag finner ulike standarder (med henvising til vedlegg 3 for mer utfyllende oversikt). I kapittel 6 ser vi på noen av de mest sentrale oppgavene som organisatorisk må ivaretas av ulike aktører. Deretter nærmer vi oss jussen. I kapittel 7 gis det en oversikt over noe av det som allerede er gjort i Norge (hvilket er fort gjort) og ikke minst i utlandet, på området for rettslige og policy-messige initiativer og vedtak. Dette er viktige utgangspunkter for en del av vår hjemlige tenkning. I kapittel 8 blir de mest sentrale rettslige spørsmålene identifisert og diskutert. I dette kapitlet ligger grunnleggende bidrag til diskusjonen om hva vi bør gjøre for å »få dette på plass», og diskusjonen er for så vidt ikke begrenset til jussen. Siden jussen ikke lever isolert fra »den virkelige verden», vil fremstillingen her også angå/berøre spørsmål knyttet til de andre delene av nødvendig infrastruktur - både teknologiske og organisatoriske forhold.

Del IV inneholder arbeidsgruppens anbefalinger til tiltak. I kapittel 9 finner vi tiltak knyttet til rettslige og andre rammebetingelser, delt inn i visse undergrupper. Et hovedspørsmål angår den rettslige likestillingen av elektroniske dokumenter og signaturer (kap 9.2), et annet tilrettelegging for etablering og drift av TTP-tjenester (kap 9.3). Det tredje hovedområdet

gjelder tiltak for å vinne konkret erfaring og kunnskap, bl a gjennom tverrgående pilotprosjekt (kap 9.4).

Del II: Behovet for sikkerhetstjenester

I denne delen besvares spørsmålet om behov ved først å gi en oversikt over de generelle behovene som ligger bak de ulike begrepene på området informasjonssikkerhet og sikkerhetsteknikker (kapittel 3). Deretter gis det oversikt over hvordan det etterspørres løsninger for å dekke disse behovene, med en spennvidde fra det politiske livet i EU, OECD og i Norge til de praktiske behov som konkret finnes på dagens marked (kapittel 4).

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Rådet for IT-sikkerhet

Digitale signaturer gir tillit til elektronisk kommunikasjon

Forslag til tiltak for aksept og utbredelse

DEL II: BEHOVET FOR SIKKERHETSTJENESTER

I denne delen besvares spørsmålet om behov ved først å gi en oversikt over de generelle behovene som ligger bak de ulike begrepene på området informasjonssikkerhet og sikkerhetsteknikker (kapittel 3). Deretter gis det oversikt over hvordan det etterspørres løsninger for å dekke disse behovene, med en spennvidde fra det politiske livet i EU, OECD og i Norge til de praktiske behov som konkret finnes på dagens marked (kapittel 4).

3. Hva snakker vi om?

3.1 Informasjonssikkerhet - sentrale begreper

Utviklingen av det moderne informasjonssamfunnet har skapt en elektronisk hverdag der de fleste former for informasjon skapes, behandles og utveksles i digital form. Nasjonale og internasjonale infrastrukturer har åpnet for nye måter av elektronisk samhandling. Utviklingen innebærer at prosedyrer forankret i papirbasert saksbehandling i stadig flere tilfeller må finne nye og «digitale» former. Bruk av digitale signaturer er eksempelvis en teknikk som kan benyttes til å «signere» digital informasjon på samme måte som en håndskreven signatur benyttes til å undertegne et papirdokument. Teknikken får dermed betydning for jussen, og i alle de sammenhenger hvor det å »skrive under» spiller en rolle.

Samtidig med den teknologiske utvikling er det skapt et stort og voksende behov for å integrere sikkerhetsløsninger i systemene.

Fagfeltet informasjonssikkerhet har til oppgave å utvikle metoder og teknikker som kan bidra til en trygg og sikker elektronisk hverdag. Et informasjonssystem vil sikres ved at vi anvender veldefinerte sikkerhetstjenester som skal beskytte informasjonen mot identifiserte trusler, og bidra til å realisere muligheter som uten sikkerhetstjenesten ville vært vanskelig eller umulig.

Sikkerhetstjeneste er i denne sammenheng en overordnet betegnelse på en egenskap eller ytelse som vi ønsker eller trenger i et system, og sier ikke noe om hvilken teknologi som benyttes for å realisere løsningen. Sikkerhetstjenester realiseres eller implementeres ved hjelp av spesifikke sikkerhetsmekanismer eller sikkerhetsteknikker. Noen av de viktigste sikkerhetstjenestene er:

- Integritet

Integritet betyr at informasjon ikke er endret under lagring eller transport. Dersom det er en fare for at skade kan oppstå ved at innholdet av en melding blir endret, vil det være behov for å benytte en integritetstjeneste. 2 Eksempel: Uten en form for integritetsbeskyttelse vil det være mulig å endre en transaksjonsmelding mellom en minibank og banken slik at et uttak på 5000 kroner blir registrert som et uttak på 500 kroner på konto. På tilsvarende måte vil man ved overføring av elektroniske resepter kunne endre en forskrivning på 10 til 100 tabletter.

Sekvensintegritet innebærer å sikre at en meldingsutveksling har foregått i riktig rekkefølge, f eks at en faktura er mottatt før det kan sendes en betalingsmelding. Tjenesten er med på å støtte duplikatkontroll. Eksempel: Dette er aktuelt ved forhåndsautorisert direktedebitering, der nummeret angir forhåndsdefinert rekkefølge for meldinger.

- Autentisering

En autentiseringstjeneste skal sikre at en enhet (person/prosess) virkelig er den som vedkommende gir seg ut for å være. I forbindelse med utveksling av elektroniske meldinger vil autentisering innebære å skaffe seg hensiktsmessig sikkerhet for at avsenderen av en melding er den vedkommende gir seg ut for å være og knytte avsenderen til meldingens innhold.

Eksempel: Bruker-autentisering av personer som logger seg på et elektronisk datasystem er spesielt viktig og danner grunnlaget for at vi kan stole på andre sikkerhetstjenester.

Behovet for autentisering vil avhenge av hvilken type melding det er tale om å utveksle. I de fleste transaksjoner vil det være ønskelig eller nødvendig å få etablert tilfredsstillende autentisering, f eks av hensyn til økonomiske verdier, korrekt saksbehandling, personvern, mv.

- Sporbarhet

Denne sikkerhetstjenesten skal sikre at viktige hendelser i systemet kan spores til ansvarlige personer eller prosesser. Autentiseringstjenester er ofte nødvendig for sporbarhet.

- Ikke-benekting

Med ikke-benekting forstås den egenskap at mottakeren av et dokument har sikkerhet for (kan sannsynliggjøre) at den angitte avsender ikke senere kan nekte å ha sendt dokumentet. På

samme måte må avsenderen av et dokument sikre seg mot at mottakeren på et senere tidspunkt kan nekte å ha mottatt dokumentet.

- Autorisering

En autoriseringstjeneste skal på sikker måte gi opplysninger om hvilke rettigheter en person har i tilknytning til et IT-system.

- Tilgjengelighet

Krav til tilgjengelighet skal sikre oss at informasjon og ressurser er tilgjengelig for brukere som har rettmessig adgang til informasjon når de har behov for det, ikke minst når de har dårlig tid f eks ved anvendelse av elektroniske meldinger/telemedisin i pasientbehandlinger.

- Konfidensialitet

Konfidensialitet er den sikkerhetstjenesten som skal sikre at informasjon ikke blir gjort tilgjengelig for uvedkommende. Det betyr at informasjon er beskyttet mot innsyn under transport og lagring. Krav til konfidensialitet kan finnes dels i lovgivningen, eksempelvis ved taushetsplikter i helselovgivningen, dels i avtaler mellom partene.

Eksempel: Forvaltningsloven pålegger taushetsplikt om »noens» personlige forhold og konkurranseutsatte opplysninger, uten å si hvordan plikten skal ivaretas, utover kravet om at det skal være »på betryggende måte». I staten finnes det noen instrukser som gir konkrete regler for sikker behandling av slike opplysninger. 3 Tilsvarende har næringslivet behov for å skjerme sine forretningshemmeligheter, og private behov for å skjerme bl a sin personlige korrespondanse.

3.2 Sikkerhetsmekanismer

Realisering av sikkerhetstjenester skjer ved innføring av sikkerhetsmekanismer eller sikkerhetsteknikker som kan være av fysisk, organisatorisk eller logisk (systemteknisk) karakter. Tradisjonelt har vi løst konfidensialitet ved bruk av forseglede konvolutter og kurerpost, mens elektronisk kommunikasjon blir beskyttet ved hjelp av kryptering. Kryptering forvrenger det digitale signalet slik at bare rettmessig avsender og mottaker ser det opprinnelige innholdet. Kryptografi er et omfattende og teknologisk fagfelt, men de grunnleggende idéene er enkle. For å forstå de underliggende organisatoriske, politiske, juridiske og tekniske problemstillingene som rapporten drøfter, gir vi her en kortfattet framstilling av noen sentrale begrep.

3.2.1 Symmetrisk krypto

Forsvar og diplomati har i århundrer gjort brukt av kryptering for å sikre kommunikasjon. Figuren under viser hva som skjer med bruk av moderne teknikk.

Figur 4: Kryptering av dataforbindelse

Avsenderen har et dokument M i lesbar form, ofte kalt klartekst. For å sende dette over til mottakeren vil klarteksten gå inn i en krypteringsfunksjon, der den blandes med en krypteringsnøkkel K_E. Resultatet blir en uforståelig melding, chiffertekst (C i figuren), som uvedkommende ikke kan tyde. Bare den rettmessige mottakeren sitter på den korrekte dekrypteringsnøkkelen K_D, som gjør det mulig å omforme C tilbake til klarteksten M. Det er derfor helt avgjørende for sikkerheten i systemet at ikke uvedkommende får tak i denne nøkkelen.

I konvensjonelle eller symmetriske kryptosystemer benyttes samme nøkkel til kryptering som til dekryptering, i den forstand at de er like. Vi har altså at $K_E = K_D$. Det betyr at kryptonøkler må distribueres på en sikker måte til begge parter før den krypterte forbindelsen kan skje. Slik nøkkelfordeling stiller store organisasjonsmessige og sikkerhetsmessige krav og er derfor en kostbar og krevende løsning dersom antall brukere blir stort.

Selve krypteringsfunksjonen skjer ved hjelp av en kryptoalgoritme som beskriver på en eksakt måte hvordan klartekst og nøkkel skal blandes sammen. Det finnes mange ulike algoritmer som er kommersielt tilgjengelig, men ingen felles internasjonal standard på området. Den amerikanske standarden DES (Data Encryption Standard) benyttes mye, men denne er over 20 år gammel og arbeidet med å ta fram en erstatning til denne er nå i gang.

Krypteringsnøklene består av en rekke mer eller mindre tilfeldige enere og nuller og antall forskjellige nøkler i systemet vil være en indikator på hvor sikker algoritmen er. Siden antall mulige nøkler henger sammen med lengden på nøkkelen, har reguleringer rundt bruk og eksport av krypto ofte vært knyttet til nøkkellengden. Det må imidlertid sterkt understrekes at det ikke er noen automatikk i at en algoritme med stor nøkkellengde er en sikker algoritme. For DES er nøkkellengden 56 bits [4] og det er i dag et faktum av at dette er i minste laget for systemer med høye sikkerhetskrav. En oppfatning er at med en utvidelse til 80-100 bits nøkkellengde, vil de fleste kommersielle systemer ha god beskyttelse i lang tid.

3.2.2 Asymmetrisk krypto

I et asymmetrisk eller offentlig nøkkel kryptosystem (eng. public key cryptosystem) er det ikke lenger noen enkel sammenheng mellom krypteringsnøkkel og dekrypteringsnøkkel. I figuren over betyr det at det ikke lenger er noe krav om at krypteringsnøkkelen K_E skal holdes hemmelig. I slike systemer vil hver bruker i systemet lage sitt nøkkelpar (K_E, K_D). Den offentlige nøkkelen K_E kan nå fritt distribueres til alle som vil sende krypterte meldinger til denne brukeren. Kravet til hemmelighold av denne vil nå bli erstattet av et krav om ekthet eller autentisitet av krypteringsnøkkelen.

Dette betyr at asymmetrisk krypto er best egnet til å løse problemene knyttet til nøkkelfordeling. Men det kreves store organisasjonsmessige og tekniske løsninger for å etablere den infrastruktur som skal til for å distribuere offentlige nøkler på en god måte. Bruk av nøkkelsertifikater og katalogtjenester blir viktig for å få til dette.

I praksis er alle asymmetriske kryptosystemer for langsomme til å kryptere store mengder av data eller trafikk i sanntid. Det er derfor vanlig å lage blandingssystemer der man benytter det asymmetriske systemet til å fordele trafikknøkler som går inn i symmetrisk kryptering av selve meldingen.

Det mest utbredte asymmetriske kryptosystemet kalles RSA, men det finnes en rekke andre teknikker som særlig benyttes til å etablere en felles, hemmelig nøkkel mellom de kommuniserende partene.

Teknologien i asymmetriske systemer er helt forskjellig fra symmetriske og kravene til nøkkellengder vil vært helt forskjellige. En kan derfor ikke sammenligne nøkkel-lengder mellom DES og RSA. En god egenskap ved mange asymmetriske løsninger er at de enkelt kan skaleres opp til et ønsket sikkerhetsnivå.

3.2.3 Digitale signaturer

Krypto slikt det er omtalt over beskriver hvordan teknikkene brukes for å oppnå konfidensialitet. Digitale signaturer er eksempel på en teknologi innenfor området kryptering (asymmetrisk krypto), men dette er en teknikk med hovedoppgave å realisere tjenester som integritet, autentisering og ikke-benekting.

Figuren illustrerer hvordan et digitalt signatursystem system fungerer.

Figur 5: Bruk av digitale signaturer

Avsenderen i et slikt system genererer et nøkkelpar som består av en hemmelig signeringsnøkkel S_A og en offentlig verifiseringsnøkkel V_A. Når avsenderen ønsker å «signere» et elektronisk dokument M, sendes M sammen med signeringsnøkkelen S_A inn i en signeringsfunksjon. Resultatet av denne prosessen er en signert melding S(M). I de fleste signatursystemene består den signerte melding av den opprinnelige meldingen etterfulgt av et signaturfelt. Signaturen er igjen en komplisert blanding av M og S_A.

Når mottakeren får en slik signert melding, vil han i utgangspunktet ha direkte tilgang til selve M. For å verifisere at dette virkelig er en «ekte» melding fra avsenderen, vil han sende M sammen med den offentlige verifiseringsnøkkelen V_A til avsenderen inn i en verifikasjonsfunksjon. Resultatet av denne prosessen vil være et godkjent/ikke-godkjent utfall. Ved et godkjent utfall vil mottakeren vite følgende:

- M kommer virkelig fra Avsenderen siden det bare er hun som besitter den hemmlige signaturnøkkelen som må til for å lage den digitale signaturen. Vi har altså meldingsautentisering.
- Meldingen eller signaturfeltet kan ikke bevisst eller ubevisst ha blitt endret under overføringen. Det betyr at krav om integritet er oppfylt.
- Avsenderen kan ikke i ettertid nekte for å ha sendt meldingen. Mottakeren kan bevise overfor en tredjepart (domstol) at det var avsenderen som signerte meldingen, ved gjentatt demonstrasjon av verifikasjonsfunksjonen. Den digitale signaturen gir derfor en ikke-fornektingstjeneste.
- Signaturen beskytter også mot at mottakeren endrer meldingen og prøver å få den akseptert som en ekte melding. Mottakeren kjenner ikke signeringsnøkkelen S_A som er nødvendig for å lage en signatur som passer på den modifiserte meldingen.

For et digitalt signatursystem vil det være nødvendig å etablere en infrastruktur som sikrer at alle parter får tilgang til de nøklene som trengs. Alle skal ha tilgang til alle verifiserings-nøkler. Kort oppsummert kan vi si:

I et signatursystem er det kun en person som kan signere ved hjelp av den hemmelige signeringsnøkkelen, men det er mange som kan verifisere signaturen ved hjelp av den offentlige verifiseringsnøkkelen. I et offentlig nøkkel kryptosystem er det mange som kan kryptere meldinger ved hjelp av den offentlig krypteringsnøkkelen, men det er kun en som kan dekryptere ved den tilhørende dekrypteringsnøkkelen.

3.3 Infrastruktur for offentlige nøkler (Public key infrastructure, PKI)

3.3.1 Sertifikater

Offentlige nøkler gir ingen informasjon om en brukers identitet. Til dette formålet benyttes entydige navn, tildelt av en »navneautoritet». Det entydige navnet og den tilhørende offentlige nøkkelen koples sammen ved hjelp av et offentlig nøkkelsertifikat. Dette utføres ved at en sertifikatautoritets (se 3.3.2 nedenfor) private (hemmelig) nøkkel brukes til å signere koplingen mellom en brukers offentlige nøkkel og vedkommendes entydige navn. Dette kan selvsagt utføres av hvem som helst, men koplingen blir verdiløs dersom ikke brukerne av dette nøkkelsertifikatet kjenner identiteten og den offentlige nøkkel på vedkommende som har signert sertifikatet. En trenger en uavhengig enhet/tredjepart, hvis offentlige nøkkel og identitet er allment kjent. Denne må selvsagt også drives på en forsvarlig måte, slik at den private nøkkelen, som er brukt til å signere offentlige nøkkelsertifikat, ikke kan misbrukes eller komme på avveie. Denne tredjeparten blir kalt for en TTP (Tiltrodd Tredjepart) 5. Det er grunn til å tro at det blir mange som vil tilby TTP-tjenester i forbindelse med offentlig nøkkel-håndtering og digitale signaturer. Både i næringslivet og i det offentlige kan det vokse frem løsninger på enkeltområder (pr bransje, pr forvaltningsområde/stat/departement/kommune).

3.3.2 Tiltrodde Tredjeparter (TTP)

En TTP kan ha mange roller, men vi konsentrerer oss her om rollen som sertifikatutsteder. Denne rollen kalles sertifiseringsautoritet (SA), på engelsk Certification Authority (CA). Hvis bruker A ønsker et nøkkelpar, kan han ta med legitimasjon og gå til en TTP. Der får han et (elektronisk) sertifikat som kobler hans identitet opp mot en offentlig nøkkel. En tiltrodd tredjepart har også et nøkkelpar som består av en hemmelig og en offentlig nøkkel. Sertifikatet signeres med TTP-ens hemmelige nøkkel. Alle skal ha tilgang på TTP-ens offentlige nøkkel. Det er viktig at alle parter stoler på at TTP-en faktisk sjekker identiteten til brukerne før de utsteder sertifikater, og at TTP-en oppbevarer sin hemmelige nøkkel på en slik måte at ingen uvedkommende får tak i den. En TTP kan også tilby verdiøkende tjenester som tidsstempling, arkivering av meldinger og mellommannstjenester.

3.3.3 PKI-infrastrukturer og kryssertifisering

En Public Key Infrastructure (på halv-norsk/smør-på-flesk: PKI-infrastruktur), eller på hel-norsk: en infrastruktur for offentlige nøkler, kan sees på som de forhold, støttefunksjoner og -tjenester som må være til stede for å realisere digitale signaturer og øvrige kryptografiske tjenester, både lokalt, regionalt og globalt. Tjenestene som en PKI skal gi nettbrukeren er blant annet håndtering av nøkler, utstedelse av sertifikater, tilbakekalling av sertifikater, verifisering (bekreftelse) av nøkler og sertifikater.

Infrastrukturen omfatter underliggende oppbygging eller sammensetning av komponenter og/eller forhold som anses nødvendige for å oppnå det som er hensikten med offentlige nøkler. Kort og upresist: »det som skal til».

En PKI kan sees på som et formelt samarbeid mellom ulike TTPer/sertifiseringsautoriteter (SAer) slik at nøkler signert og godkjent av en TTP blir godtatt av alle andre TTPer i en PKI. Dette gir brukerne et bedre grunnlag for tillit. Det er grunn til å tro at det vil oppstå mange PKI'er, bransjevis, sektorvis, i kommunal, fylkeskommunal og statlig forvaltning.

I noen sammenhenger er man mer avhengig av et kvalifisert grunnlag for tillit. Ved behov for et litt høyere sikkerhetsnivå enn »vanlig», kan slik »ekstra tillit» til en (eller flere) PKI være basert på at TTPene som deltar i infrastrukturen er godkjent av en sentral myndighet og at det er stilt krav til driften og administrasjonen av TTPene ut fra anerkjente kriterier. Spørsmål om »noen» skal godkjenne en TTP eller om det skal være et fritt marked, eller om det skal være en blanding, ut fra hvilke kriterier det eventuelt skal godkjennes, hvilket ansvar skal en TTP ha, hvem utsteder TTPenes nøkler, osv er policyspørsmål som det må tas stilling til, både i Norge og i andre land.

Kryssertifisering er en mekanisme som innebærer at to eller flere TTP'er (SA'er) tilhørende forskjellige PKI'er gir hverandre sertifikater for å stadfeste et tillitsforhold. Denne fremgangsmåten skiller seg fra den strengt hierarkiske modellen der tillit flyter nedover langs fast definerte "stier" i et hierarki. Det er ikke snakk om kryssertifisering innenfor en PKI/et PKI-domene (område). For å oppnå kryssertifisering må en rekke også ikke-tekniske forhold være på plass, bl a at TTP'en har organisert seg og drives på et forutsatt sikkerhetsnivå iht aksepterte (helst internasjonale) normer/kriterier, herunder sertifiseringspolicy/regelverk og -praksis (Certification policy and -practice statement) og at bilaterale eller multilaterale avtaler kan inngås på bakgrunn av slike felles utgangspunkter/premisser, som er det som gir grunnlag for tillit.

Et spesielt spørsmål er om politi- og påtalemyndighet ut fra lovlige etterforskningsformål skal ha mulighet for avlytting eller nøkkelregenerering (key recovery) på en eller annen måte. Dette siste berøres ikke i denne rapporten, fordi vi her er opptatt av sikkerhetstjenester som autentisering, integritet og ikke-benekting. Disse kan ivaretas av den teknologien innenfor området offentlig nøkkelkryptering som kalles digital signatur. Disse tjenestene representerer ikke problemer etterforskningsmessig, ettersom de ikke skjuler noe innhold.

3.4 Forholdet mellom kryptering og signering

Dersom en har behov for både beskyttelse av integritet og konfidensialitet, kan digital signatur kombineres med påfølgende kryptering av innholdet i dokumentet eller informasjonen (innholdskryptering). Valg av tjenester må gjøres ut fra den verdien informasjonen har og de truslene eller mulighetene vi står overfor.

Innholdskryptering vil ikke bare hindre uvedkommende innsyn i en kommunikasjon, med det kan også vanskeliggjøre eller umuliggjøre etterforskning og avlytting i regi av politi og myndigheter. Dette griper inn i forhold som kan ha med nasjonal sikkerhet å gjøre. De fleste land fører derfor en streng eksportkontroll med teknologi som kan benyttes til kryptering. I mange dataprogrammer som selges fra USA er kryptofunksjonalitet blitt fjernet eller sterkt redusert. Andre land fører også en streng regulering med nasjonal bruk av krypterings-

teknologi. Konfidensialitet er derfor et område der det er langt vanskeligere å komme fram til internasjonale løsninger enn for digitale signaturer og rene autentiseringstjenester.

Problemstillingene rundt bruk og regulering av krypto er tidligere behandlet i en egen arbeidsgruppe 6 i regi av Rådet for IT-sikkerhet og disse problemene vil i liten grad bli berørt i denne rapporten. Det er imidlertid overlappende problemstillinger, siden det finnes asymmetriske kryptosytemer som også kan benyttes som signatursystemer. Den infrastruktur som må etableres for å få systemene til å spille sammen er lik fra land til land, og det må tas hensyn til at sikker elektronisk kommunikasjon ofte krever at begge tjenestene er på plass.

3.5 Begrepet »elektronisk signatur»

I enkelte sammenhenger brukes begrepet »elektronisk signatur» som et mer generelt begrep, der digital signatur kan inngå som ett av flere tenkelige underbegrep (biometrisk baserte teknikker kan være et annet). Betegnelsen sikker elektronisk signatur brukes av mange om en digital signatur fra et asymmetrisk signatursystem.

3.6 Kommentar og konklusjon

Overskriften til kapitlet spør »hva snakker vi om»? Har vi svart på en forståelig måte? Det er ikke godt å si. Begrepene er teknisk orienterte, vanskelige å overskue innholdet av, de er mange, de står i bestemte forhold til hverandre, og for de fleste av oss tar det tid å skjønne noe av dette. Kanskje lang tid. Vi har lært at informasjonssikkerhet gir trygghet i den elektroniske hverdagen, ikke minst ved kommunikasjon over usikre nettverk som Internett, og at sikkerhetstjenester som autentisering, integritet og ikke-benekting kan ivaretas av sikkerhetsteknikker som kryptering og digitale signaturer. Dette er bygget på det som kalles offentlige nøkkelkryptografi, der hjelp fra tredjeparter kan inngå. Dermed kan vi identifisere oss sikkert for hverandre og for systemer, vi kan være sikre på om det vi sender kommer frem uten »riper i lakken», og vi kan være sikre på at verken mottaker eller avsender kan nekte for det de har gjort/det som er skjedd. For det kan bevises!

Som brukere trenger vi ikke skjønne hvordan teknikken gjør dette for oss. Det er nok at vi klarer å bruke den. Det er mange tekniske innretninger som er i god, effektiv og nyttig bruk, uten at brukerne nødvendigvis skjønner selve innholdet i teknikken. Bil, radio, TV og telefon er noen eksempler. Det krever ikke spesiell teknisk innsikt å bruke disse teknologiene. Alle gjør det. Tilsvarende er det med digitale signaturer og innholdskryptering. For brukerne blir dette muligheter man velger med den største letthet på skjermen, og alt det tekniske som er forklart foran skjer automatisk via systemet. Forutsatt at visse ting er på plass. Det er noen av disse viktige tingene resten av rapporten handler om. For beslutningstakere er det nyttig og nødvendig å skjønne hovedtrekkene i hva dette dreier seg om, for å kunne bidra på et best mulig opplyst grunnlag.

En generell konklusjon er at både folk flest og brukere/beslutningstakere i offentlig og privat virksomhet mangler informasjon om digitale signaturer og andre sikkerhetsteknikker som må på plass og i alminnelig bruk. Det er grunn til å tro at det er mye usikkerhet om hva dette er for noe, hva teknikken kan gjøre for oss, om det er til å stole på og om det er rettslig holdbart å ta det i bruk. Det er et stort behov for formidling av allmennkunnskap på området.

2 Dataintegritet må ikke forveksles med datakvalitet som er knyttet til riktigheten av de opplysninger som er formidlet. Dataintegritet kan være i behold selv om opplysningene objektivt sett er uriktige, dersom det var disse opplysningene avsenderen faktisk sendte.

Sikring mot forsinkelse eller tap av meldinger er heller ikke omfattet av begrepet dataintegritet.

3 Dette er bl a Sikkerhetsinstruksen og Beskyttelsesinstruksen, samt Datasikkerhetsdirektivet. Hvis man etter en vurdering merker et dokument med gradering f eks iht Beskyttelsesinstruksen, fordi det »kan skade» om uvedkommende ser det taushetsbelagte dokumentet, kommer man inn under virkeområdet til Datasikkerhetsdirektivet. Dette stiller krav om at taushetsbelagt/gradert informasjon som overføres utenfor eget kontrollert område skal konfidensialitetsbeskyttes ved hjelp av godkjent kryptoutstyr. Forsvarets overkommando/sikkerhetsstaben er godkjenningsmyndighet.

4 Det betyr at det totalt finnes 256 eller omtrent 72. 000 milliarder nøkler i systemet.

5 Begrepet Tiltrodd Tredjepart (TTP) er upresist og generelt. Begrepet og de rollene/oppgavene som knyttes til begrepet er forklart kort nedenfor i 3.3.2 og 3.3.3, og mer utførlig i kapittel 6. En tiltrodd tredjepart kan ha mange roller. Og det kan være mange TTP'er.

6 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.

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Forslag til tiltak for aksept og utbredelse

---

4. Hvilke behov?

4.1 EU og OECD vil ha sikker elektronisk kommunikasjon

EU har interessert seg for informasjonssikkerhet og herunder elektroniske/digitale signaturer i mange år. Det er gjort svært mye for å belyse temaene, engasjere europeisk næringsliv og ulike kompetansemiljøer, samt for å fremme politisk forståelse og satsing. EU's Ministerråd vedtok program for ivaretakelse av informasjonssikkerhet for perioden 1992 til 1994 (INFOSEC-programmet, Information Security). 7 Det ble gjennomført en rekke relevante prosjekter for temaet. Dette ble fulgt opp av nye program som i stadig større grad viet oppmerksomheten utelukkende mot digitale signaturer og tiltrodde tredjeparter. En såkalt grønnbok, med gjennomgang av hele området, ble lagt frem i 1994. Teorier ble omsatt i praktiske utprøvende prosjekter, blant annet med sikker kommunikasjon på tvers av landegrensene. Dette har gitt verdifullt erfaringsmateriale. 8 På en slik bakgrunn er nye initiativer kommet på stadig høyere nivå i EU (se kap 7.2.1). Man er i ferd med å gå fra utredninger og utprøvinger til vedtak av overordnet rammeverk. Det er åpenbart at både Kommisjonen, Ministerrådet og Parlamentet nå legger avgjørende vekt på å få til

hensiktsmessige løsninger for digitale signaturer og tiltrodde tredjeparter. Man ser klart for seg at jo mer divergerende medlemslandenes tekniske og rettslige tilnærminger er eller blir på dette området, dess verre hinder vil dette representere for det indre marked, og hele EU som sådan. Derfor legges det avgjørende vekt på å få til en EU-policy eller rammeverk for å få til sikkerhet og tillit knyttet til elektronisk kommunikasjon. Kommisjonen understreker at EU ikke har råd til et splittet rettslig landskap på et område som er så viktig for økonomien og samfunnet. Man er selvfølgelig også opptatt av at europeiske løsninger har behov for å inngå som deler av globale løsninger.

Kommisjonen peker på at de problemer man kan ha med hensyn til krypto for å skjule innholdet (innholdskryptering), ikke gjør seg gjeldende i forhold til krypto som anvendes for digitale signaturer. Siden digitale signaturer ikke hindrer at man kan lese informasjonen på en helt åpen måte, utgjør de ingen fare for å være til hinder for rettslig etterforskning av alvorlige forbrytelser, slik som innholdskryptering kan være. Det er tvert i mot slik, sier Kommisjonen, at digitale signaturer kan være til hjelp for eventuell etterforskning, ved sin klare sammenknytning av identiteter og informasjon/handlinger. Det gjøres til et poeng at både kommunikasjonen »A European initiative in Electronic Commerce (COM (97)157 final, 16.4.97) og OECDs »Guidelines for Cryptography Policy» av 27.3.97 skiller mellom på den ene siden autentiserings og integritets-tjenester som digitale signaturer bidrar til, og på den andre siden det som kalles konfidensialitetstjenester som innholdskryptering bidrar til.

Også **Ministererklæringen fra Bonn** i juli 1997 slo klart fast behovet for et rettslig og teknisk rammerverk for digitale signaturer på et europeisk plan. I tillegg slo erklæringen fast betydningen av tilgang på det som ble kalt sterk kryptoteknologi for å dekke behovene på området elektronisk handel.

EU-kommisjonens utkast til direktiv om elektroniske signaturer er på denne bakgrunn det siste leddet i en lang utviklingskjede. Nærmere omtale av utkastet finnes i kap 7.2.1, samt er omtalt en rekke steder der det er relevant i forhold til det enkelte temaet som diskuteres. Hvis direktivet blir vedtatt, vil det bli førende for utviklingen også i Norge, gjennom vårt EØS-medlemskap.

OECD avholdt en ministerkonferanse om elektronisk handel i Ottawa i oktober 1998 med 800 delegater fra de 29 medlemslandene, samt 12 observatørland. 9 Delegatene representerte landenes myndigheter, industrien og forbruker- og arbeidstakerorganisasjoner og andre interesseorganisasjoner. Videre var en rekke internasjonale organisasjoner representert. Målet for konferansen var å komme videre med løsninger knyttet til autentisering og sikker identifisering med elektronisk signatur, personvern, forbrukervern og skatt og avgiftshåndtering ved elektronisk handel. Videre var målet å avklare den internasjonale arbeidsdelingen mellom ulike organisasjoner for å unngå dobbeltarbeid. Det var enighet om en rekke hovedkonklusjoner. Siden digitale signaturer for autentiseringstjenester, integritet og ikke-benekting etter arbeidsgruppens mening må anses som noen av de grunnleggende byggeklossene for elektronisk handel, og elektronisk handel på den annen side sannsynligvis er den sterkeste drivkraften for etterspørsel og bruk av slike tjenester ved hjelp av digitale signaturer mv, gjengir vi nedenfor noen av konklusjonene:

- Elektronisk handel gir radikalt nye muligheter for forretninger og handel, og er en potensiell drivkraft for økonomisk vekst og utvikling i verden.

- Det må oppmuntres til samarbeid mellom alle deltakere (myndigheter, forbrukere, næringslivet, arbeidstakere og offentlige institusjoner) i det enkelte land og i internasjonale organisasjoner i arbeidet med å utforme politikk for elektronisk handel.
- Myndighetene må arbeide for konkurransefremmende omgivelser for e-handel, arbeide for å redusere og fjerne unødige hindere, og iverksette tiltak der det er nødvendig for å sikre beskyttelse av samfunnsmessige interesser i den digitale som i den fysiske verdenen.
- Myndighetsinngrep når nødvendig, må være rimelige, åpne, konsistente og forutsigbare, samt teknologinøytrale.
- Myndighetene må anerkjenne viktigheten av fortsatt samarbeid i næringslivet om standardisering innenfor internasjonale frivillige og konsensusbaserte omgivelser
- Næringslivet må spille en nøkkelrolle i utvikling og implementering av løsninger på en rekke sentrale områder av betydning for utvikling av e-handel, og samtidig anerkjenne og ta i betraktning grunnleggende samfunnsinteresser, økonomiske og sosiale mål og arbeide nært sammen med myndighetene og andre aktører.

Ottawakonferansen betraktes som en milepæl i det globale arbeidet med e-handel, og landene ble bl.a. enige om felles retningslinjer på områdene skatt/avgifter, personvern og autentisering. Ministerdeklarasjonene 10 på disse områdene danner en viktig bakgrunn for det videre arbeidet i Norge:

- Det var enighet om at man i alle land må gå gjennom lover og regelverk og justere bestemmelsene slik at elektroniske signaturer kan sidestilles med tradisjonelle signaturer. Det videre arbeidet internasjonalt med lov- og regelverksutforming for elektroniske signaturer og autentisering vil skje i UNCITRAL. OECD vil følge opp dette arbeidet.
- Det var enighet om at man erkjenner betydningen av autentisering for elektronisk handel, og at det må gjennomføres en rekke nærmere angitt tiltak for å fremme utviklingen og bruken av autentiseringsteknologier og -mekanismer. Dette må inkludere arbeid på internasjonalt nivå, i samarbeid med næringsliv, industri og brukerrepresentanter.
- Det var enighet om at prinsippene i OECDs retningslinjer for beskyttelse av personopplysninger fra 1980 fortsatt har gyldighet og er relevante for beskyttelse av personvernet på Internett. OECD vil følge opp hvordan disse implementeres i landene mhp elektronisk handel.
- Det var enighet om å utarbeide felles retningslinjer for forbrukervern i løpet av 1999.

4.2 Norske regjeringer vil ha sikker elektronisk kommunikasjon

I **Voksenås-erklæringen** fra oktober 1997 slår Kristelig Folkeparti, Senterpartiet og Venstre fast at en sentrumsregjering vil samle det politiske ansvaret for den strategiske satsing på informasjons- og kommunikasjonsteknologi både innen næringsutvikling, utdanning, distriktspolitikk samt satsing på IT innen offentlig sektor. Ansvaret for samordningen av regjeringens IT-politikk vil bli lagt til Nærings- og handelsdepartementet. Dette ble senere gjennomført. I erklæringen heter det videre at *»på alle områder i samfunnet skaper informasjonsteknologien muligheter som var utenkelige for bare få år siden. Samtidig er drivkreftene i den digitale revolusjonen så kraftige at utviklingen uten styring kan føre til et samfunn med ujevn fordeling og sterk sentralisering av makt, kompetanse og bosetting.»*En rekke tiltak skisseres der bruk av informasjonsteknologi anses sentralt for å oppnå de politiske målene. Styrking av personvernet fremheves ved at den enkelte i størst mulig grad skal ha

anledning til å bestemme over bruk og gjenbruk av informasjon om en selv, samt sikring av muligheten for anonymitet i en stadig mer elektronisk hverdag der de fleste etterlater elektroniske spor. Det slås også fast at en sentrumsregjering vil få fortgang i arbeidet med å etablere *»et eget sertifiseringorgan for sikre dataløsninger».*

I **IT-politisk redegjørelse** 1998 fra april la næringsministeren frem for Stortinget en videreføring av disse tankene. Den store veksten i Internett-bruk understrekes, og den store samfunnsmessige betydningen av dette, sammen med utviklingen i den øvrige IT- og kommunikasjonsteknologen. Det understrekes at dette berører på en sentral måte alle politikkområder. Elektronisk handel fremheves som et av de mest spennende områdene, der det *»er behov for å lage rammebetingelser som sikrer en forsvarlig handel på nettet. Det er privat sektor som må gå foran og ta i bruk elektronisk handel. Myndighetenes rolle er å legge til rette gjennom lov og regelverk.» IT-politisk redegjørelse peker på fire innsatsområder: at flest mulige kan bruke de nye handlemulighetene, at brukere og forbrukere kan ha tillit og tiltro til at elektroniske overføringer er sikre, også ved handel over landegrensene, at usikkerhet omkring regelverket kan reduseres, samt reduksjon av problemer forbundet med betaling og levering.*

Næringsministeren presiserte at *»en arbeidsgruppe under Rådet for IT-sikkerhet vil komme med forslag om hvordan digitale signaturer og tiltrodde tredjepartstjenester bør realiseres », et utsagn som sikter til vår arbeidsgruppe, og det forarbeidet vi gjør gjennom denne rapporten.*

Redegjørelsen peker på at elektronisk handel skaper nye muligheter også for statlig eide virksomheter, med Posten som ett eksempel. Offentlige innkjøp er på ca 165 milliarder kroner i året. Elektronisk handel kan gi betydelig drahjelp i utviklingen. Regjeringen vil bruke informasjons- og kommunikasjonsteknologi til å fornye, forbedre og modernisere alle sider ved offentlig sektor. Den peker på at etableringen av tverrsektorielle nett og felles infrastruktur har skapt grunnlag for løsninger på tvers av virksomheter, og at elektronisk saksbehandling, tilrettelagte informasjonstjenester, elektroniske skjema og datautveksling er sentrale områder i forvaltningsutviklingen. Samtidig understreker regjeringen at det må legges vekt på konsekvensene, og de verdivalg som forvaltningen bygger på. Det heter i redegjørelsen at det er *»et mål at hele forvaltningen tar i bruk Internett som kanal i sin informasjonsstrategi».* Samtidig understrekes det at trygg bruk av Internett er et særskilt problem, med adresse til ulike typer uønsket innhold på nettet.

Personvern understrekes som et viktig aspekt regjeringen er opptatt av å styrke. I redegjørelsen for Stortinget heter det: *» For å forenkle vurderingen av IT-sikkerhetsnivået bl.a. med hensyn på personverninteressene, er det utarbeidet et forslag til IT-sikkerhets-sertifisering av henholdsvis produkter og organisasjoner. Forslaget har vært på høring, og Regjeringen vil vurdere forslaget på bakgrunn av høringsuttalelsene.»*

Næringsministeren avsluttet med å hevde at hovedutfordringen er å *»påvirke retningen på utviklingen og redusere folks opplevelse av avmakt og usikkerhet i forhold til den nye teknologien.» Det er markedet som driver frem den digitale revolusjonen, og* »den er bare i noen grad politisk styrt.» Han lovet imidlertid at mulighetene til å påvirke utviklingen på sentrale områder skal bli aktivt brukt.

Våren 1998 la regjeringen også frem Norge - en utkant i forkant, Næringsrettet It-plan 1998-2001. Visjonen er at avansert bruk av informasjonsteknologi skal bli et av de største

konkurransefortrinn for norsk næringsliv i nær framtid. For å møte næringslivets utfordringer beskriver planen 40 tiltak som berører sentrale områder. Overordnede mål er å styrke norsk næringsliv gjennom effektiv utvikling og anvendelse av IT, samt å stimulere til nyskaping og vekst i IT-næringen.

I forbindelse med elektronisk handel fremheves det som en utfordring *»å utnytte de globale nettene som markedskanal for økt handel og kommunikasjon».* Det pekes på at bruk av Internett fjerner krav om nærhet til markedene, - det er det globale markedet som åpner seg, med et enormt potensiale. Det hevdes at næringslivets konkurranseevne i stor grad vil bli berørt av bedriftenes evne til å utnytte mulighetene i en tidlig fase av utviklingen, og av *»den offentlige tilretteleggingen for at elektronisk handel skal kunne skje på en sikker og effektiv måte.»* Det må eksistere tillit til at den nye måten å gjøre handel på er like sikker som tradisjonell handel. Det understrekes at myndighetsansvaret ligger i å lage *»gode rammebetingelser og et nasjonalt, globalt tilpasset lov- og regelverk for handel over elektroniske nett», i en nær dialog mellom offentlige og private aktører.* Videre heter det: »Næringslivet og forbrukernes tillit til elektronisk handel vil være nært knyttet til løsningen av problemstillinger rundt sikkerhet, betalingsordninger, digitale signaturer, personvern, opphavs- og forbrukerrettigheter, samt skatter og avgifter. Regjeringen vil derfor prioritere arbeidet med å utforme det nødvendige lov- og regelverket som skal til for å skape tillit til den elektroniske markedsplassen.»

Planen går så over til å erklære følgende mål: *»Handel over elektroniske nett skal bli en like vanlig handelsform som tradisjonell handel».* Ved siden av tilpasninger i lov- og regelverk og deltakelse internasjonal regelverksutforming, vil myndighetene bruke informasjon og bevisstgjøring som virkemidler. Som tiltak nevnes igangsetting av pilotprosjekter for å påskynde utviklingen av elektronisk handel i Norge, etablering av et forum for elektronisk handel, samt i løpet av 1998 å vurdere nødvendige tilpasninger i lov- og regelverk, inkludert løsninger for digitale signaturer og tiltrodde tredjeparter.

Den norske IT-veien. Bit for bit. I rapport fra Statssekretærutvalget for IT fra januar 1996 ble det slått fast en rekke politiske mål i forbindelse med IT og IT-utviklingen i samfunnet.

I pkt 3.3.6 uttales det:

»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 presiseres det at man må avklare en rekke forhold og utvikle nye fellesordninger med klar ansvarsplassering.

Dette punktet kommenteres av arbeidsgruppen for kryptopolitikk. 11 Gruppen hevder 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 tiltakspunkt 3.3.6d erklæres det i rapporten fra statssekretærutvalget:

»Myndighetene og næringslivet må samarbeide om ordninger som gir tilfredsstillende sikkerhet i IT-systemene og i de elektroniske informasjonsnettene»

De kommenterer dette selv ved å understreke at dersom sikkerheten i nettene ikke er god nok, vil brukerne være tilbakeholdne med å bruke elektronisk kommunikasjon. Felles løsninger skal bidra til å skape tillit hos brukerne til at informasjonen de mottar er autentisk, sikre at sensitiv informasjon bare er tilgjengelig for autorisert bruk, og at uautoriserte brukere ikke kan få tilgang til, endre eller ødelegge informasjon. Videre sies det at norske myndigheter skal samarbeide innbyrdes og med privat sektor for å få frem og ta i bruk sikkerhetprodukter og -løsninger. Det heter at *»Akkreditering av sertifiseringsorganer og sertifisering av produkter og tjenester er aktuelle virkemidler for å oppnå ønsket informasjonssikkerhet», og at dette bør samordnes med tilsvarende internasjonale ordninger.*

Tiltak 3.3.6e: *»Det bør utredes hvilke felles administrative oppgaver som må ivaretas når åpne informasjonsnettverk skal bygges i sektorer og bransjer»*

Under dette tiltakspunktet pekes det på at man trenger å samordne viktige fellesoppgaver, herunder løsninger for digitale signaturer og administrasjon av krypteringsnøkler. Dessuten understrekes det at slike ordninger krever samordning over landegrensene for å sikre at norske brukere kan delta internasjonalt, og at ordningene også har betydning for brukervennligheten og fleksibiliteten i informasjonsnettverkene.

Det finnes mange initiativer i utlandet som tilsvarer det de to siste norske regjeringene har gjort. For nærmere oversikt viser vi til kap 7.2 og 7.3. Fokus der tar utgangspunkt i rettslige aspekter, men angår et bredere knippe spørsmål.

4.3 Behov uttrykt gjennom konkrete forsøk og initiativer

En kartlegging av behov for informasjonssikkerhet/meldingssikkerhetble gjennomført i 1994, 12 og er forsøkt ajourført på en del områder i denne rapporten. Det understrekes at det ikke tas sikte på å gi en fullstendig oversikt, men heller noen sentrale eksempler for å illustrere behovet. Dette er et område i rask vekst, og det skjer relativt mye.

Effektiv utnyttelse av de muligheter IT-utviklingen gir blir en stadig viktigere konkurransefaktor for norsk næringsliv. De siste årene har så vel små som store bedrifter og offentlig forvaltning fått tilgang til åpne elektroniske nettverk (for eksempel Internett). Gjennom dette er det blitt stadig mer vanlig å sende informasjon av ulik karakter over disse åpne nettverkene.

Både for næringslivet og forvaltningen ligger det et betydelig effektiviseringspotensiale i å utnytte Internett og andre nettverk. Potensialet foreligger i grenseflatene mellom:

- *Bedrift til bedrift og offentlig til offentlig*
Generell elektronisk post, handelsprosesser, saksbehandling, intranett og ekstranett, m.v.

- *Bedrift til offentlig og offentlig til bedrift*
Generell elektronisk post, handelsprosesser, innsamling og utveksling av skattedata (elektroniske selvangivelser, regnskap, m.v.)

- *Bedrift til privat og offentlig til privat*
Generell elektronisk post, handelsprosesser, hjemmekontorløsninger, m.v.

- *Privat til bedrift og privat til offentlig, samt ikke minst privat til privat* Generell elektronisk post, bruk av internett til å finne informasjon og få kontakt, søknader, selvangivelse, handelsprosesser, banktjenester, private brev m.v.

Det generelle sikkerhetsnivået med tanke på autentisering og konfidensialitet i f. eks. Internett tilfredsstiller pr. i dag ikke næringslivets behov når virksomhetskritisk informasjon skal formidles. Heller ikke forvaltningens behov, når informasjon trenger sikker autentisering, integritet og konfidensialitet av hensyn til forsvarlig saksbehandling og utveksling av informasjon, og transaksjoner av en viss økonomisk størrelse. Også for privat kommunikasjon er det grunn til å tro at det er behov for tjenester med et høyere sikkerhetsnivå enn det som pr nå tilbys i vanlige standardprodukter.

TTP-tjenester (se kapittel 6 for nærmere omtale) er sett fra både næringslivets og forvaltningens side en god generisk sikkerhetsløsning som kan bidra til at næringsliv og forvaltning effektivt kan utnytte de store investeringer som legges ned i IT-infrastruktur i Norge i dag.

Ved å legge til rette for fremveksten av gode TTP-tjenester kan det offentlige bidra til redusert skjemavelde, raskere og tryggere kommunikasjon, mer effektiv offentlig saksbehandling, og redusert bruk av ressurser både i næringsliv og offentlig forvaltning.

Nedenfor følger en kort gjennomgang av ulike områder og virksomheter, der fellesnevneren er at man i det praktiske liv nå faktisk tar i bruk (eller planlegger å ta i bruk) de sikkerhetstjenestene og mekanismene som er omtalt i teorien foran. Teoriene er i ferd med å bli praksis, men ofte en noe kaotisk praksis, som trår sine første barnesko. Ved siden av å dokumentere behovene for sikker elektronisk kommunikasjon og lagring, gir denne praksisen verdifull erfaring, som vi i fellesskap bør bygge videre på. Dette er også en praksis som gir innspill til diskusjonen om hva som kan være myndighetsroller på området, og hva markedet best gjør selv.

De enkelte områdene er noe fyldigere omtalt i vedlegg 2.

4.3.1 Handel

Det foregår for tiden en enorm internasjonal fokusering på elektronisk handel med initiativer fra bransjer, nasjoner, regioner, standardiseringsorganisasjoner, WTO, FN (UNCITRAL) og OECD. Store aktiviteter skjer i nasjoner som USA, Canada, Japan, Singapore, Malaysia, Australia og Europa. En kommunikasjon datert 16.4.1997 fra Kommisjonen til Rådet og Parlamentet er »A European Initiative in Electronic Commerce», COM(97)157. Dette er den første policy-uttalelsen fra Kommisjonen der bruken av kryptering og digitale signaturer i forbindelse med elektronisk handel er et sentralt tema. Se til orientering websiden til EU, med oversikt over området. 13 På våre hjemlige trakter har Næringsdepartementet høsten 1998 etablert et fellesforum for elektronisk handel i samarbeid med eforum.no, Norsk EDIPRO, Næringslivets Hovedorganisasjon og Handelens og Servicenæringenes Hovedorganisasjon. Etableringen kommer som en oppfølging av Regjeringens Næringsrettede IT-plan, jf omtalen foran i kap 4.2.

I en åpen internett-verden er det behov for åpen handel hvor alle skal kunne handle med alle, individer, bedrifter, mv. Man vil ikke lenger være begrenset til lukkede brukergrupper eller forhåndsinngåtte avtaler mellom partene, selv om slike også vil fortsette sine aktiviteter, gjerne ved hjelp av ny teknikk. Ulike sikkerhetsteknikker anses avgjørende for at både konvensjonell handel over åpne nettverk, men ikke minst »helelektronisk» handel over Internett på global basis skal kunne bli trygg nok. Kryptering og digital signatur basert på offentlig nøkkel-teknologi vil spille en *»nøkkelrolle».*

Nærings- og handelsdepartementet har det overordnede ansvar for å stimulere til og tilrettelegge for elektronisk handel i Norge, men privat sektor må lede utviklingen. I Næringsrettet IT-plan 1998-2001 er elektronisk handel et sentralt område. Et viktig tiltak er å vurdere nødvendige tilpasninger i lov- og regelverk, inkludert løsninger for digitale signaturer og tiltrodde tredjeparter. Et eget grunnlagsdokument 14 er utarbeidet som ledd i oppfølgingen av dette tiltaket. Statssekretærutvalget for IT har ved en rekke anledninger drøftet ulike sider ved e-handel, og Regjeringen har slått fast prinsippene, hovedinnretningen og prioriteringene for arbeidet med rammebetingelser for elektronisk handel.

4.3.2 Betaling

Banktjenester er i stor grad et spørsmål om tillit. For betalingsformidling og andre banktjenester vil behovene for sikkerhetstjenester i et produkt være avhengig av forhold til de verdier som skal beskyttes, og de risiki man ser for forskjellige typer angrep.

For betalinger er det naturlig å skille mellom det å sikre tilgangen til konto eller betalingsinstrumenter, og sikring av betalingstransaksjonene.

I mange betalingssystemer er det bygget inn sikkerhetsmekanismer som gjør at innehaver av kort eller konto må identifisere seg slik at uautorisert aksess ikke forekommer. Data som autentiserer en kontoinnehaver må enten beskyttes mot innsyn eller være av en slik art at de ikke er forutsigbare for en eventuell angriper.

Betalingstransaksjonene må også beskyttes, bl a mot manipulering av transaksjonsbeløp og kort / kontonummer. Fjerning av transaksjoner eller innsetting av falske transaksjoner må kunne oppdages. Verifisering av at en transaksjon eller en forespørsel kommer fra en kjent og godkjent kommunikasjonspartner (autentisering av opphav) er viktig. Behov for konfidensialitet kan knytte seg til deler av en transaksjon. Det er også viktig at meldinger kommer fram i tide, at betaling skjer innen en tidsfrist - og at både avsender og mottaker får melding om at betaling har skjedd. Disse meldingene må kunne lagres slik at de kan brukes med beviskraft ved eventuelle disputter.

Innenfor feltet elektronisk betalingsformidling er man opptatt av å få avklart digitale signaturers rettslige beviskraft. Dette leder i sin tur til at det er ønskelig å ha retningslinjer for utstedelse av nøkler og sertifikat og krav til tiltrodde tredjeparter.

4.3.3 Petroleumsbransjens elektroniske markedsplass: Secure Oil Information Link (SOIL)

0 En samarbeidsgruppe bestående av Statoil, Saga, Norsk Hydro, BP Norge, Shell, Amoco, Philips, og Oljedirektoratet ble etablert høsten 1997. Det ble utført en markedsundersøkelse i november - januar `98. Deretter ble det kjørt formell forespørsel i februar - juni '98. Fellesdata er valgt som leverandør. Løsningen har fått navnet SOIL - Secure Oil Information Link. Test

av tjenester og utprøving av pilot løsninger har foregått siden aug. '98 og en forventer at SOIL vil være i drift før årsskifte.

SOIL er ment som en markedsplass og teknisk infrastruktur for oljebransjen og baseres på bruk av internasjonale standarder (ref. IETF 15). Et høykapasitets bredbåndsnett danner basis i løsningen. Sikkerhet er hovedkriteriet for måten dette er utformet på. Mange teknikker og metoder er brukt for å forhindre uautorisert tilgang.

Tjenestene er delt i to grupperinger, for henholdsvis tilgang (access) og tjenester (services).

Tjenesten for sikker e-post benytter sertifikat 16 utstedt av Fellesdata i rollen som tiltrodd tredjepart. En vil benytte følgende sikkerhetsgrad på sertifikatene: Sterk autentisering 17, konfidensialitet 18, integritet og ikke-fornektelse 19 .

4.3.4 Norsk EDIPRO

En rapport fra Norsk EDIPRO i 1996, Digitale signaturer og tiltrodde tredjeparter, inneholder konkret utformete forslag på tre av de antatt viktigste områdene, - overordnede retningslinjer for en sikkerhetspolicy for TTP-tjenester, et forslag til det som kalles en *»standard» i Norge for sertifikatformat, samt et forslag til en sikker navnestruktur. Rapporten fremhevet at formålet med å etablere det den kalte en sikker meldingsinfrastruktur basert på TTP-tjenester er å dekke viktige behov i forhold til autentisering, konfidensialitet, integritet og ikke-benekting. Det ble understreket at TTP-er må være tiltrodd evnen til upartisk å levere tjenester med en høy grad av funksjonell og teknisk tillit (sikkerhet) i forhold til elektronisk meldingsutveksling.*

4.3.5 Offentlig innkjøp

Når det offentlige står for innkjøp av varer og tjenester er det i motsetning til næringslivet en del overordnede prinsipp som må ivaretas:

- åpenhet - kunngjøring og elektronisk informasjon må være tilgjengelig for hele verden
- likeadgang - 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 dokument 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. Arbeids- og administrasjonsdepartementet (AAD) planlegger et eget program for elektronisk handel ved offentlige innkjøp som vil forfølge sentrale problemstillinger.

Et tilbud er konfidensielt for alle, inklusive innkjøper, fram til et bestemt åpningstidspunkt som er senere enn innleveringstidspunktet for tilbudet.

4.3.6 Statskonsult

Statskonsult har gjennom flere år jobbet med området elektronisk saksbehandling, elektronisk innrapportering og IT- standardisering. Det er laget en rekke rapporter og notater som direkte eller indirekte har tatt for seg temaer rundt digitale signaturer og TTPer. Blant de seneste er Elektronisk saksbehandling (Statens generelle kravspesifikasjon), Statskonsult 1998 og Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering, Statskonsult rapport 1998:13.

Statskonsult har etablert et brukerforum for elektronisk saksbehandling hvor offentlige etater kan ha en møteplass for utveksling av erfaringer med elektronisk saksbehandling og man kan få Statskonsult til å ta opp konkretet problemstillinger som brukerne måtte ha. Dette forumet er en del av et større program om elektronisk saksbehandling som Statskonsult er ansvarlig for. Programmet er flerårig og delfinansiert av AAD.

4.3.7 Arbeids- og administrasjonsdepartementet og rammeavtaler i offentlig sektor

Forvaltningsnettprosjektet ble startet i 1996 etter initiativ fra Arbeids- og administrasjonsdepartementet (AAD) i samarbeid med Kommunenes sentralforbund (KS). Det skal 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. I tillegg skal prosjektet etablere en rekke andre typer fellestjenester som er nødvendige for en helhetlig og velfungerende elektronisk infrastruktur. Digital signatur med tilhørende sertifiseringstjeneste er et prioritert område for offentlig sektor med et dokumentert behov hos ulike offentlige virksomheter for denne type tjenester.

Enkelte etater er allerede gått ut med forespørsler om leveranse av løsninger for digital signatur og sertifiseringstjenester med tanke på prøveprosjekter for elektronisk dokumentutveksling. Det er imidlertid et problem at teknologien (og sertifiseringstjenestene) ikke er godt nok standardisert og det kan oppstå situasjoner der to aktører ikke vil være i stand til å kommunisere med hverandre på grunn av at de har valgt forskjellige teknologiske løsninger og ulike sertifiseringstjenester.

Virksomheter (eller privatpersoner) som skal samhandle elektronisk med flere offentlige etater kan derfor komme i en situasjon der det kan være ulike krav til løsninger for digital signatur og sertifisering fra de ulike offentlige etater.

AAD ønsker avtaler der det forutsettes mulighet for såkalt kryssertifisering, dvs. at de valgte leverandørene skal godkjenne hverandres tekniske løsninger, rutiner for og organisering av sertifikat- og nøkkelutstedelse. Det kan også bli aktuelt med forpliktende samarbeidsavtaler dem i mellom. Dette for å unngå situasjonen beskrevet ovenfor, med ikke-samspillende løsninger for digital signatur.

Arbeids- og administrasjonsdepartementet vil i tillegg til arbeidet under Forvaltningsnett-prosjektet iverksette et eget utredningsarbeid med spørsmål knyttet til utstedelse av et nasjonalt elektronisk ID-kort («borgerkort») og et enhetlig elektronisk ID-kort for de offentlig ansatte (med ID-kort menes her smartkort som både fungerer som fysisk identifikasjon og som en bærer av eierens elektroniske signatur- og krypteringsnøkler).

4.3.8 Kommunal- og regionaldepartementet - pilotprosjektet EDNA

Kommunal- og regionaldepartementet og Husbanken gjennomfører pilotprosjektet EDNA - Elektronisk Dokumentutveksling i Norsk Administrasjon.

Ved prosjektstart i 1995/96 ble det klart at det ennå ikke forelå tilbud om tilfredsstillende teknologiske løsninger på markedet. En utviklingsavtale måtte inngås, ut fra kravspesifikasjon og scenarier knyttet til offentlig saksbehandling, med de tilhørende spesifikke sikkerhetstiltak 20. Som industripartner ble Posten SDS kontraktmotpart for en utviklingsavtale støttet av Statens Nærings- og distriktutbyggingsfond (SND). En norsk sikkerhetsapplikasjon, SecApp (SecurityApplication) er utviklet. Den er basert på åpne løsninger iht internasjonale standarder, implementert og utprøvd, og har vært i daglig bruk i en periode. Måten implementeringen av sikkerhetskravene er gjennomført på er evaluert og kvalitetssikret.

EDNA kan sies å være et pionerprosjekt på forvaltningsområdet ikke bare i nasjonal, men også i internasjonal sammenheng. Det er etablert helt konkrete operative løsninger for å ivareta krav til bl a signatur og konfidensialitet. Løsningene og erfaringene fra dette prosjektet har klar eksempel- og overføringsverdi for offentlig sektor. Prosjektledelsen i EDNA ser det som både ønskelig og nødvendig at det videre arbeidet på området skjer i samarbeid med næringslivet og sivile organisasjoner. Dette anses påkrevet fordi det i nær fremtid vil bli behov for elektronisk kommunikasjon med disse. Allerede i dag skjer det (som nevnt nedenfor) en del innrapportering fra privat til offentlig sektor. Privatpersoner og næringsliv vil i stadig større grad komme i direkte elektronisk kontakt med førstelinjetjenester fra for eksempel Husbanken og Skattedirektoratet. Da er det viktig at løsningene som legges til grunn er omforente.

4.3.9 Innrapportering til og i det offentlige, mv.

Statskonsult har i sin rapport om Elektronisk datautveksling og innrapportering, 1998:15, gitt en generell oversikt over området og innføring i problemstillingene.

*Skattedirektoratet*s 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, full sporbarhet/ikke-benekting, og i noen tilfeller konfidensialitet må møtes. En formidlingssentral vil være ansvarlig for nøkkeladministrasjon for de som benytter digital signatur og det kreves at den blir tilpasset en nasjonal infrastruktur når denne er på plass. Skattedirektoratet ønsker ett sikkerhetssystem for alle prosjekter med innrapportering og ber en formidlingssentral om støtte.

Når det gjelder innrapportering til *Statistisk sentralbyrå* (SSB) og KOSTRA (kommune-stat innrapportering) er det lagt spesielt vekt på kryptering av sensitive data. Det er bare noen svært få innberetninger som krever signatur, KOSTRA vil imidlertid kreve dette etter hvert. Det legges heller ikke vekt på ikke-benekting.

Når det gjelder innrapportering til *Brønnøysundregistrene*, gjelder det offentlig tilgjengelig informasjon (regnskap) og er således ikke konfidensielle. Her er det derimot krav om signatur og ofte flere enn en signatur.

Fiskeridirektoratet har et prosjekt på gang med innrapportering av bl.a. fangstmeldinger og passivmeldinger fra skip via satellitt. Krav til sikkerhet er under vurdering, men det er i alle fall krav til riktig avsender og meldingsintegritet.

Statens vegvesen, Vegdirektoratet har utarbeidet en håndbok for elektronisk billettering med krav til samordning som myndighetene stiller overfor kollektivselskapene ved investering i elektroniske billetteringssystemer. Anonyme betalingsmåter som verdikort reduserer behovet for kontantbeholdning hos fører, men øker krav til sikkerhet og kryptering av informasjon på et chipkort. Det legges opp til at selskapene har ansvar for generering av sikkerhetsmoduler og utstedelse av egne kort til brukere.

Datatilsynet vil iht forslaget 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.

Riksarkivet utarbeider ny arkivstandard 21 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 dokument, samt ved arkivering.

4.3.10 Helsesektoren

I helsesektoren formidles store mengder informasjon innen administrativ saksbehandling og pasientbehandlingen. Årlig foretas ca. 12-16 millioner konsultasjoner i primærhelsetjenesten, 3 mill. polikliniske konsultasjoner i sykehus og 650 000 innleggelser i sykehus. 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 helse-personell å dokumentere sin virksomhet.

Regler for journalføring omfatter bl.a. krav til føring, innsynsrett, innhold, utlevering og lagring. En *elektronisk* pasientjournal i sykehus (helseinstitusjoner) er i dag ikke likestilt med papirjournal, og det kreves at pasientinformasjonen skal oppbevares *og lagres som papir eller mikrofilmet*. Oppbevaringsplikten varierer fra uendelig for noen opplysninger og 10 år for andre.

Overføring av sensitiv pasientinformasjon formidles daglig og er i tillegg til journalkopier, resepter, henvisninger, epikriser, prøvesvar , utdrag av pasientopplysninger fra journaler m.m. Som ved annen dokumentforsendelse er det behov for identifisering av avsender og beskyttelse mot ikke-autorisert innsyn.

Sosial- og helsedepartementet utarbeider ny lov om helsepersonell og ny lov om helseregistre og elektronisk behandling av helseopplysninger, der det legges opp til å likestille elektronisk og papirbasert pasientjournal, at nedtegninger i pasientjournalen skal signeres og at man i forskrifter vil gi nærmere regler for føring, langtidslagring, kodeverk, signering og

kommunikasjon. Det legges videre opp til at departementet kan gi bestemmelse om form og frist for innsamling av helsopplysninger til sentrale helseregistre, herunder pålegg om sikkerhet, bruk av standarder, kode og klassifikasjonssystemer m.m.

4.3.11 Forsvaret

Forsvarets overkommando/ Sikkerhetsstaben har gjennomført et arbeid med det mål å belyse problemstillinger omkring sikkerhet i endesystemer. Aktuelle områder som er vurdert er bl. a. bruk av digitale signaturer, TTP-tjenester, samt opprettelse av et domene for offentlig nøkkelkryptografi i Forsvaret. Det er fokusert på Forsvarets behov, men gruppen har også vurdert arbeidets konsekvenser og relevans for statsforvaltningen forøvrig. Arbeidsgruppen har utarbeidet en rapport som i tillegg til å komme med vurderinger, også anbefaler konkrete løsninger, samt skisserer behovet for videre arbeid. Gruppens anbefalinger og arbeid vil følges opp, og det vil sannsynligvis etableres et PKI-pilotprosjekt i løpet av 1998.

NATO har i lengre tid arbeidet med planer om å etablere en NATO PKI. Det er opprettet en gruppe (PKI Ad Hoc Working Group) som skal utrede aktuelle tekniske og operative løsninger. Målet med arbeidet er å få etablert et felles NATO PKI domene, med full interoperabilitet i hele domenet. De enkelte medlemsland bidrar med innspill til dette arbeidet. Flere av innspillene er basert på konkrete erfaringer ved bruk av allerede implementerte nasjonale løsninger. Dette dreier seg om PKI strukturer, varierende TTP-tjenester, og bruk av digitale signaturer.

Gruppen har utarbeidet et draft for hvilke mål og resultater som skal oppnås, samt frister for dette arbeidet. Det dreier seg om 5 hovedpunkter med tilhørende underpunkter. Disse er å: **A:** Etablere en arkitektur for et NATO PKI, **B:** Komme til enighet om en management struktur og tilhørende prosedyrer, **C:** Implementere et pilot PKI for å teste infrastrukturen og management prosedyrene, **D:** Dokumentere et felles rammeverk, og etablere en felles forståelse for ulike PKI-spesifikke begreper, samt **(E)**:Potensielle oppgaver.

4. 4.3.12 Norges forskningsråd

Programmet Nasjonalt informasjonsnettverk (NIN) er innrettet for igangsetting av et antall pilotprosjekter og demonstratorer for å oppnå økt elektronisk samhandling. ININ er etablert som en prosjektgruppering for å ta seg av felles infrastrukturspørsmål og kvartalsvise fagsamlinger skal samle ulike faglige støttemiljø for å ta del i erfaringsutvekslingen.

ININ har igangsatt en rekke fellesprosjekter for å etablere en infrastruktur mellom prosjektene, bl.a. ININ-K Implementering og initiell drift av en katalogtjeneste for NIN. Katalogtjenesten er i prøvedrift og kan nås via web på http://maxware.no/nin

Prosjektet har klarlagt hvilke type katalogopplysninger som er interessante internt i informasjonsnettverk og hva slags prosesser som er brukbare for å sikre oppdateringer og ønsket beskyttelse og eksponering med sporbarhet og autentitet. Det er åpent for demonstratorene i NIN å lage egne understrukturer i katalogen.

Sammen med Arbeids- og administrasjonsdepartementet er det tatt initiativ til å etablere et samarbeidsorgan som kan sørge for koordinering om kataloginformasjon og katalogtjenester, som epost- og edi-adresser, digitale sertifikater og annen kontaktinformasjon.

Det er videre etablert samarbeid med Forvaltningsnettprosjektet i AAD og Kommunenes Sentralforbund om å prøve ut kravspesifikasjonene i praktiske NIN-demonstratorer.

4.4 Kommentar og konklusjon

Gjennomgangen i dette kapitlet viser at både i henhold til EU, OECD, to norske regjeringer og de undersøkte praksisområdene er det behov for de sikkerhetstjenester og funksjoner som er nærmere forklart foran i kap 3.1. Det viser videre at behovene ikke er begrenset til den enkelte region, det enkelte land, eller sektor, men at de fleste aktører (også) vil bevege seg mellom regioner, land og sektorer. Behovene er med andre ord utpregede fellesbehov, selv om de kan og må ivaretas på litt ulike måter og med mulighet for å ta i bruk flere ulike sikkerhetsnivåer. Det er ikke slik at alle trenger det høyeste og dyreste sikkerhetsnivået.

Mer konkret: behovet for autentisering og integritet ser ut å være helt grunnleggende behov som vi finner overalt. Behovet for sporbarhet gjelder også alle områder, mens tidsstempling og (sekvens)integritet (duplikat-kontroll) ser ut til å være et behov særlig innen betaling, offentlig innkjøp, helse og handel. Ikke-benekting av bl a avsender og mottak går også ofte igjen som viktige behov i mange sammenhenger. For noen sektorer er det behov for konfidensialitet for informasjon som er sensitive i forhold til person-, produkt og firmaopplysninger, enten dette skyldes taushetsplikter eller andre skjermings-behov. Merk at dette ikke dreier seg om de høyeste sikkerhetsnivåer, som vi ofte forbinder med graderte opplysninger (av hensyn til rikets sikkerhet). Behovet for konfidensialitet på de lavere nivåene er et klart utviklingstrekk på sivil side i offentlig forvaltning, men ikke minst i næringslivet, i handel, og for privatpersoner. Merk også at en del ikke har behov for konfidensialitet, og kan oppleve at konfidensialitet på noen områder skaper mer problemer enn det løser.

De aktivitetene/løsningene fra det offentlige som kan bidra til at de nevnte fellesbehovene blir dekket, kan gi positive gevinster for samfunnet som helhet.

En konklusjon er at både EU's styrende organer, OECD og norske regjeringer har sagt i klartekst at det er sterke behov for at elektronisk underskrift, informasjon og kommunikasjon skal bli like akseptert og til å stole på som tilsvarende løsninger vi er vant til fra papirverdenen. Hensynet til både borgerne, offentlig forvaltning og næringsliv, i nasjonal og internasjonal kommunikasjon, krever at man finner gode elektroniske løsninger så raskt som mulig. Aktivitetene med konkrete initiativer og forsøk i Norge viser at dette ikke er politiske målsetninger uten rot i en virkelighet, - tvert om viser aktivitene at det finnes et raskt voksende bruksområde og marked innen offentlig og privat virksomhet som i praksis strever for å dekke nøyaktig de samme behovene som de politiske dokumentene etterlyser løsninger på. En konklusjon utover aspektet knyttet til behov er at den erfaringen som vinnes bør deles.

Og hva er så løsningen? Et sammensatt svar gis i del III, med forslag til tiltak i del IV.

Del III: hva er nødvendig infrastruktur og rammebetingelser for *»alminnelig» utbredelse?*

Mandatet spør om hva som er nødvendig infrastruktur og rammebetingelser for alminnelig utbredelse av sikker elektronisk kommunikasjon med bruk av digital signatur, - teknisk, organisatorisk og juridisk. Som arbeidsgruppens svar pekes det i kapittel 5 på behovet for standarder, i kapittel 6 på hvilke organisatoriske oppgaver som må ivaretas, i kapittel 7 på nasjonale og internasjonale rettslige initiativer som bl a kan gi føringer for norske løsninger,

og på bakgrunn av en slik sammensatt infrastruktur behandles i kapittel 8 de mest sentrale rettslige spørsmålene som må løses for å ha rammebetingelsene på plass, bl a i forhold til teknisk og organisatorisk infrastruktur.

---

7 Vedtaket finnes på websiden: http://www.cordis.lu/infosec/src/coundecs.htm

8 Mange av prosjektrapportene/arbeidene nevnt her er tilgjengelige på websiden: http://www.cordis.lu/infosec/src/down.htm

9 Se websiden om konferansen, med såkalte ministererklæringer: www.ottawaOECDconference.org

10 Se ministerdeklarasjonene på: http://www.ottawaoecdconference.org/english/homepage.html

11 Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk, Rådet for IT-sikkerhet, Forsvarets overkommando/Sikkerhetsstaben 1997-11-10

12 Norsk EDIPRO 1994 "Meldingssikkerhet - Tiltrodde tredjeparter og digitale signaturer".

13 Websiden til EU om elektronisk handel finnes på: http://www.ispo.cec.be/ecommerce/

14 Rammebetingelser for elektronisk handel. Problemområder og problemstillinger knyttet til lov og regelverk for elektronisk handel. Nærings- og handelsdepartementet, november 1998. Se dokumentet og delta i høringen frem til 15. januar 99 på følgende webside: http://www.dep.no/nhd/publ/1998/ehandel/html

15 Internet Engineering Task Force, IETF, en standardiseringsgruppe for Internett.

16 X.509 versjon 3

17 (2048 bit RSA)

18 (128 bit TripleDES)

19 («Non-repudiation»)

20 Til spesifisering av sikkerhetstiltakene knyttet man til seg Peter Landrock, Cryptomathic A/S. Han er i tillegg professor ved Århus universitet.

21 Riksarkivet har høsten 1998 NOARK 4 ute til høring på http://www.riksarkivet.no/nyheter.html

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Rådet for IT-sikkerhet

Digitale signaturer gir tillit til elektronisk kommunikasjon

Forslag til tiltak for aksept og utbredelse

DEL III: HVA ER NØDVENDIG INFRASTRUKTUR OG RAMMEBETINGELSER FOR "ALMINNELIG" UTBREDELSE?

Mandatet spør om hva som er nødvendig infrastruktur og rammebetingelser for alminnelig utbredelse av sikker elektronisk kommunikasjon med bruk av digital signatur, - teknisk, organisatorisk og juridisk. Som arbeidsgruppens svar pekes det i kapittel 5 på behovet for standarder, i kapittel 6 på hvilke organisatoriske oppgaver som må ivaretas, i kapittel 7 på nasjonale og internasjonale rettslige initiativer som bl a kan gi føringer for norske løsninger, og på bakgrunn av en slik sammensatt infrastruktur behandles i kapittel 8 de mest sentrale rettslige spørsmålene som må løses for å ha rammebetingelsene på plass, bl a i forhold til teknisk og organisatorisk infrastruktur.

5. Standarder - som bidrag til infrastruktur

5.1 Standarder - grunnlag for produkter og tjenester

Innføring av systemer for digitale signaturer og infrastruktur for offentlige nøkler må være basert på etablerte og omforente standarder. Dette er viktig (men ikke tilstrekkelig alene) for å sikre nødvendige krav til sikkerhet og interoperabilitet. Innenfor de etablerte standardiseringsorganisasjonene har det vært arbeidet med slike standarder i flere år.

Kort oppsummert kan en si at det finnes etablerte standarder på de fleste områder som må dekkes for å etablere en nasjonal infrastruktur for offentlige nøkler (PKI) for digitale signaturer. Dette innbefatter områder som:

a) Algoritmer for digitale signaturer med tilhørende kryptografiske hashfunksjoner. b) Sertifikatformater c) Signaturformater d) Offentlig nøkkel infrastruktur (PKI) og krav til interoperabilitet e) Tiltrodde Tredjepartstjenester (TTP) f) Programmeringsgrensesnitt (APIs) g) Kommunikasjonsprotokoller h) Smartkortteknologi i) Katalogtjenester j) Tidsstempling k) Evalueringskriterier
l) Administrasjon

Slike standarder kan finnes som internasjonale vedtatte standarder, som sektor/bransje-standarder, de facto standarder eller som pågående arbeid. På en del områder kan det eksistere overlappende standarder og det er ikke alltid tilfelle at to forskjellige implementasjoner av den samme standarden kan kommunisere seg i mellom.

En noe fyldigere oversikt over de antatt viktigste standardene for etablering av systemer for digitale signaturer framgår av vedlegg 3.

Standarder alene er ikke nok. Noen må også utvikle produkter og etablere tjenester i henhold til dem (såkalt implementere standardene). Helst på måter som passer sammen. Disse må så tilbys markedet. Det har ikke vært et mål å gi noen uttømmende oversikt. Dette er et marked i rask utvikling. I vedlegg 4 gis det en kort oversikt over enkelte produkter (og tjenester) på området. De tjenestene som ytes knytter seg til oppgaver som beskrives i kapittel 6 nedenfor.

Den største generelle drivkraften i den teknologidrevne utviklingen er uten tvil Internett og de mange anvendelsene der. Av disse igjen vil antakelig elektronisk handel og betalingsformidling bli sterke pådrivere for sikre løsninger, basert på internett-standarder på

området for offentlige nøkler og håndteringen av disse. Når større forbrukermarkeder kommer på nettet med vesentlig større volumer enn nå, f eks for å etterspørre produkter og tjenester fra ulike underholdningsindustrier, vil dette sannsynligvis være avhengig av at markedet for sikre tjenester blir/er blitt etterspurt tilsvarende. Og omvendt: markedene blir neppe store hvis man ikke finner effektive (også kostnadseffektive) løsninger på de elektroniske sikkerhetsteknikkene. Siden det er meget sterke krefter i sving både politisk og kommersielt kan dette komme på plass fortere enn man skulle tro. Trenden er helt klar: myndighetene verden rundt holder fingrene av fatet i forhold til utvikling av teknologien og de teknologisk orienterte løsningene, - dette er det åpenbare området for initiativ og satsing fra privat sektor. Industrier i mange land konkurrerer intenst på et voksende globalt marked. Siden handel og kommunikasjon går over landegrensene, må også utviklingen av sikkerhetsstandarder, produkter og -tjenester gjøre det samme. Myndighetenes rolle begrenses til å gi rammebetingelser og å legge forholdene til rette. I tillegg til rollen som storbruker.

5.2 Kommentar og konklusjon

Vi er helt avhengige av gode standarder. Men ingen standarder løser »alle» problemer. Standarder kan være i innbyrdes motstrid, og en og samme standard kan brukes på ulike måter. Også på sikkerhetsområdet er standarder litt av en jungel, med mange farer og feller. Til tross for eksistensen av mange standarder som dekker de viktigste områdene, kan man neppe si at tilbudet av produkter og tjenester på grunnlag av standardene er kommet særlig langt. Det finnes få eller ingen »ferdige» løsninger i større skala pr i dag, verken i Norge eller andre steder. Mange er på vei. På noen områder er man ganske nær, på andre har man avgrensede løsninger, mens på atter andre er det langt igjen. Man er generelt sett fremdeles på et tidlig stadium i utviklingen på mange av de aktuelle områdene. Det er et inntrykk at markedet har litt vanskelig for å ta av. Grunnene kan være mange. Manglende kunnskap og tiltro er nevnt før, på etterspørselssiden. De forløsende fellesløsningene/fellesgrepene er ikke kommet på plass ennå på tilbudssiden. Det er antakelig mye arbeid som gjenstår. Mye må utredes videre, og mange praktiske erfaringer må høstes og deles, både nasjonalt og internasjonalt, før »alt kommer på plass».

Konklusjonen er at med den betydning standarder på sikkerhetsområdet har, er det svært viktig at vi fra norsk side holder oss så godt orientert om denne utviklingen som mulig, og deltar aktivt i den der det er mulig. Dette omfatter både de »gamle» organisasjonene for standardisering, men ikke minst den/de nye, knyttet til den førende utviklingen på Internet.

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Rådet for IT-sikkerhet

Digitale signaturer gir tillit til elektronisk kommunikasjon

Forslag til tiltak for aksept og utbredelse

---

6. Organisering - som bidrag til infrastruktur

6.1 Behovet for TTP-tjenester

Den teknologien som er nødvendig for signering og kryptering er kommentert i kapitlet foran, og noe utdypet og eksemplifisert i vedlegg 4. En del er på plass, men mye står igjen. Vi er i en tidlig fase av utviklingen. I åpne løsninger som Internett er et godt eksempel på, er tilgangen til kommunikasjonsmotpartens offentlige nøkkel sentral. Utfordringen ligger i hvordan man skal kunne distribuere den offentlige nøkkelen på en slik måte at mottakeren har rimelig grad av sikkerhet (kan stole på) for at nøkkelen tilhører den som hevder å være rette innehaver. Løsningen består trolig av det som kalles en offentlig nøkkel infrastruktur (også kalt Public Key Infrastructure, PKI) organisert av en såkalt Tiltrodd TredjePart ("TTP"). 22 Vi står ikke overfor et spørsmål om én offentlig nøkkel infrastruktur (PKI) og én tiltrodd tredjepart (TTP), men mange, og på høyst ulike nivåer og størrelser, nasjonalt og internasjonalt. Ordbruken kan være forvirrende. Den er ikke nødvendigvis så presis som en kan få inntrykk av, eller kunne ønsket. Begrepet TTP er et slikt upresist og generelt begrep, som på mange måter er en samlebetegnelse på en rekke forskjellige oppgaver, som gjennomgås nedenfor. Disse oppgavene kan løses av ulike organisasjoner. På et overordnet nivå er det likevel vanlig å snakke om »en TTP-tjeneste», eller »TTP'en», selv om en nærmere undersøkelse ville vise at det kan være snakk om ikke bare en, men flere aktører, i ulike typer samspill. Hver oppgave under TTP-paraplyen har egne navn/underbegreper. For enkelhets skyld går vi ikke inn på disse, men holder (stort sett) fast ved det generelle TTP-begrepet.

Et stykke på vei kan tilgangen til teknologi for digital signatur uten TTP sammenliknes med det å være i besittelse av en telefon uten at det finnes noen telefonkatalog eller nummeropplysning. For de fleste vil telefonen ha begrenset nytte hvis det bare kan ringes til de som har oppgitt sitt telefonnummer på forhånd.

Den enkelte kan naturligvis publisere sin offentlige nøkkel i avisen eller på sin egen Web-side, nøkkelen kan sendes med den første meldingen som utveksles mellom partene el. Problemet er at mottaker i alle disse tilfellene mangler sikkerhet for at nøkkelen virkelig tilhører den som hevder å være rette innehaver og at denne faktisk har den identitet vedkommende hevder å ha. Sikkerhet om nøkkelinnehaverens identitet er viktig fordi tjenestene først og fremst er beregnet på informasjonsutveksling der partenes identitet ikke er likegyldig - nemlig transaksjoner av stor økonomisk verdi eller som av annen årsak har et stort skadepotensiale.

Den alminnelig foreslåtte løsning på dette problem er å la en TTP administrere registreringen av og tilgangen til nøklene. Dette er ikke nødvendig hvis behovet for sikkerhet ikke er stort, eller behovet for å ha et kvalifisert grunnlag for sikkerheten ikke er stort. Veldig mye kan gjøres uten den formen for trygghet som TTP'er kan gi i en åpen elektronisk verden. Det er også åpenbart at for mange lukkede brukergrupper (i næringsliv eller forvaltning) kan det eksistere kontraktsforhold eller andre grunnlag, som gjør det mulig for dem å kommunisere med den ønskede sikkerheten til stede. Når det i denne rapporten videre argumenteres for å få på plass løsninger for sikker elektronisk kommunikasjon ved hjelp av TTP'er, er dette ment som tillegg til den delen av markedet som ikke trenger ekstra sikkerhet, og slett ikke til fortrengsel eller ulempe for dette markedet.

6.2 Identitetssertifikat og rollesertifikat

De offentlige nøklene legges inn i såkalte sertifikater. Sertifikatene er elektroniske meldinger (eller dokumenter om man vil) som inneholder opplysninger bl a om sertifikatinnehaverens entydige navn (som er en selvstendig utfordring), den offentlige nøkkelen, sertifikatets gyldighetsperiode (bl a pga teknisk foreldelse, saneringshensyn mv) og TTP'ens signatur (for å sikre integriteten og tilliten til sertifikatet).

Sertifikatene kan betraktes som «digitaliserte legitimasjonstegn». Det som imidlertid kjennetegner sertifikatene er at de bare gir mening når de benyttes i forbindelse med en på forhånd signert melding eller signerte "utfordringer". I motsetning til den håndskrevne signaturprøve, som kan etterliknes, kan ikke sertifikatet benyttes for å utgi seg for å være en annen.

Det er hensiktsmessig å skille mellom et »identitetssertifikat» og et »rollesertifikat».

Identitetssertifikatene identifiserer en person. Sertifikatet etablerer en forbindelse mellom personen og den offentlige nøkkelen som benyttes for å verifisere en melding vedkommende har signert.

I mange tilfelle er det imidlertid ikke identiteten man er interessert i, men om avsender er berettiget til å disponere over en konto eller opptre på vegne av en virksomhet. Hvilken enkeltperson som skjuler seg bak rollen vil i mange tilfeller være uten praktisk interesse.

Rollesertifikatene sier til forskjell fra identitetsertifikatene ikke nødvendigvis noe om hvem en aktør 23 er. Derimot gir rollesertifikatet uttrykk for en egenskap eller rolle vedkommende aktør har, f eks at innehaver av sertifikatet er berettiget til å disponere over en særskilt bankkonto eller er bemyndiget til å binde en virksomhet ved inngåelse av avtaler. Et rollesertifikat kan også knytte en identitet til rollen som lege, tannlege og veterinær som i medhold av helselovgivningen er autorisert til å foreskrive legemidler. Rollesertifikatet kan også være underlagt disposisjonsbegrensninger. Rollesertifikatene vil være gjenstand for hyppigere endringer enn identitetsertifikatene.

I motsetning til identitetssertifikatene vil rollesertifikatene ikke bare være et forhold mellom sertifikatinnehaver og -utsteder. Normalt vil også den virksomhet rollen er knyttet til, f eks en arbeidsgiver, bank eller autorisasjons-/tilsynsmyndighet, ha ønske om kontroll med rolleopplysninger som peker mot virksomheten.

Med en infrastruktur for identitetsertifikater i bunn vil det være mulig å la organisasjonene selv utstede rollesertifikater. Dessuten vil det antakelig være knyttet flere og mer direkte rettsvirkninger til rollesertifikatene.

Identitetsertifikatene benyttes til å dokumentere en knytning mellom en offentlig nøkkel og en aktør, og ved dette også en knytning mellom den elektroniske meldingen som er signert og en aktør. De rettslige virkninger av at nettopp denne aktør utferdiget den elektroniske meldingen, må søkes i de regler som gjelder for den aktuelle transaksjonstype, f eks spørsmålet om en medarbeider har stillingsfullmakt i forhold til bestilling av en bestemt type vare på bedriftens vegne, om en lege har rett til å foreskrive medikamenter og sende regning for pasientbehandling til Rikstrygdeverket. Hvis det derimot benyttes et rollesertifikat som nettopp gir uttrykk for vedkommende fullmakt eller i det minste knytter vedkommende til bedriften, kan situasjonen være en annen.

Fordeling av oppgaver og ansvar i forbindelse med rollesertifikater bør utredes videre og det anbefales å knytte kontakt med sektorvise utprøvingsprosjekter. Det samme gjelder de øvrige rettslige virkninger av å løsrive rollene fra den underliggende identitet, f eks i forhold til fullmektigens ansvar for overskridelse av fullmakter og rollesertifikatets posisjon i forhold til eksisterende fullmaktstyper som frasagnsfullmakten.

Dessuten bør det vurderes nærmere hvordan håndtere sertifikater som ikke er knyttet til noen enkeltperson, men som direkte identifiserer en virksomhet eller applikasjon. Et spørsmål er om man kan anerkjenne også slike sertifikater i forhold til formkrav om skriftlighet og signatur, eller om dette må reserveres for persontilknyttede signaturer. Et alternativ er å kun anerkjenne sertifikatenes (dvs signaturenes) identifiserende effekt, hvoretter man må vurdere de rettslige virkningene av meldingen separat, f eks ut fra synspunkter om innrettelsesrisiko mv. Praktisk sett vil virksomhets- og applikasjonssertifikatene få stor betydning og de rettslige virkningene av dette bør klarlegges.

6.3 TTP'ers oppgaver

TTP'ers tjenester er et resultat av en rekke funksjoner og oppgaver. Viktige tjenester kan stikkordsmessig oppsummeres som:

- registrering og identitetskontroll av brukere
- navnetildeling (fra navneautoritet), utstedelse av sertifikater
- utstedelse av krypteringsnøkler og adgangskoder
- drift og vedlikehold av sertifikatdatabase, inkl. varslingsberedskap og tilbakekallingslister

Oppgavene kan være fordelt på flere organisatoriske enheter/TTP'er, evt i samarbeid, og gjennomføringen av de ulike deler av tjenesten kan ofte utføres av underleverandører. I tillegg til operative funksjoner skal TTP'er forvalte de retningslinjer og sikkerhetspolicy som TTP-tjenesten drives under. Disse deles ofte inn i henholdsvis sertifiseringsregler (certification policy), som angir hvilket sikkerhetsnivå som er aktuelt for tjenesten, og sertifiseringspraksis (certification practice statements), som beskriver hvordan sertifiseringsreglene er etterlevd (implementert) for den enkelte, konkrete tjenesten 24. De aktuelle retningslinjer, sikkerhetspolicy og -praksis for gjennomføring av tjenesten er grunnlaget for den tillit som kvalifiserer tjenesteyteren som TTP. Hvorvidt TTP'er driver under en egenutviklet policy, eller er knyttet til en policy som omfatter flere tjenesteytere, vil variere. Her kan både nasjonale og internasjonale føringer være aktuelle.

6.4 Modeller for organisering

De oppgaver TTP'en skal løse kan realiseres gjennom ulike modeller. Se om dette blant annet i rapportene EDIPRO94 og EDIPRO96 25.

TTP'en kan, først og fremst gjennom egen organisasjon dekke opp alle de aktuelle oppgaver. Dette kan være praktisk dersom en virksomhet eller etat selv utsteder sertifikater til egne ansatte eller kommunikasjonspartnere. Men også i disse tilfellene kan det være aktuelt å sette ut f eks katalog- og varslingstjenesten av hensyn til driftsstabilitet og tilgjengelighet. Enkelte organisasjoner vil også gjennom sin konsernstruktur ha ønske om å kontrollere alle de relevante deler av tjenesten.

TTP'en kan velge å kontrollere sertifikathåndteringen og vedlikehold av katalogtjenestene, men sette ut registreringsarbeidet og den tekniske driften av katalogene til andre.

Det er grunn til å tro at det vil vokse frem en rekke ulike løsninger men at de fleste vil rette sine tjenester mot en avgrenset målgruppe. En åpen, generisk TTP-tjeneste, med et desentralisert nettverk av mulige registreringssteder, er en betydelig mer omfattende oppgave å organisere. Det arbeides imidlertid med slike løsninger i de andre nordiske land, og postverkene står nær til å løse en slik oppgave.

Et slik mangfold av løsninger innebærer utfordringer for forsøk på enhetlig regulering og kontroll med tjenestene.

6.5 Brukerregistrering og identitetskontroll

Tildeling av nøkkelsertifikater forutsetter et pålitelig system for registrering av nye brukere og kontroll med deres identitet eller »roller». Brukerregistreringen kan gjennomføres etter en rekke ulike modeller avhengig bl a av hvilket sikkerhetsnivå sertifikatet skal betjene.

For en bruker som opptrer som privatperson kan det være behov for tilgang til et registreringssted innenfor rimelig avstand. Dette kan f eks være en bank, et postkontor, politikammer, tinglysingskontor el. Disse registreringsstedene har ikke nødvendigvis status som sertifikatutsteder eller TTP, men opptrer på vegne av denne i forbindelse med registrering og identitetskontroll.

Et nærliggende alternativ for større virksomheter er at disse selv registrerer sine ansatte og formidler disse opplysninger videre til sertifikatutsteder. Etter omstendighetene kan en etat eller virksomhet også utstede egne sertifikater.

Registrering og kontroll reiser særlige ansvarsspørsmål.

6.6 Utstedelse av sertifikater

Når en bruker er registrert hos et registreringssted, overføres opplysningene til en sertifikatutsteder som gjennomfører nødvendige kontroller og utsteder nøkkelsertifikat.

Hvilke opplysninger som inngår i sertifikatet fremgår av vedlegg 3, i punktet om »Sertifikatformater».

Om den nøkkel som sertifiseres er generert av sertifikatutsteder, eller på forhånd er generert av bruker, vil kunne variere, bl a avhengig av hvilken teknologi som benyttes for nøkkeloppbevaring.

Sertifikatet signeres av sertifikatutsteder. Deretter gjøres sertifikatet tilgjengelig i en sertifikatkatalog.

6.7 Navnetildeling

Ved utstedelsen av sertifikater tildeles brukerne enkeltvis et entydig navn. Det er av stor betydning at det benyttes en navnestruktur og en politikk for navnetildeling som utelukker at et navn blir tildelt mer enn én gang. Dette kan oppnås enten ved at hver sertifikatutsteder

disponerer sitt eget »navnerom», hvilket kan være uheldig begrensende/bindende, eller ved etablering av en sentral, nasjonal tjeneste for navnetildeling (navneautoritet), hvilket kan være effektivt, rasjonelt og fullt mulig, ikke minst i et lite og oversiktlig land. En løsning som må vurderes er å bruke de veletablerte ordninger samfunnet har laget for tilsvarende problemstillinger tidligere. For personnavn kunne man bruke Folkeregisteret, med Sentralkontoret for folkeregistrering som navneautoritet. Det vises også til enhetsregisteret og foretaksregisteret hos Brønnøysundregistrene, og arbeidsgiver- og arbeidstakerregisteret hos Rikstrygdeverket.

Det anbefales omgående å vurdere hvilke parter som kan ha roller knyttet til navnetildeling.

6.8 Katalogtjenester, varsling og tilbakekalling av sertifikater

Katalog- og varslingstjenestene er helt sentrale for effektiviteten og påliteligheten i nøkkelinfrastrukturen.

Et pålitelig og tilgjengelig katalogsystem er nødvendig bl a for å finne frem til korrekt sertifikat dersom en brukers offentlige nøkkel skal benyttes til å kryptere en melding.

Dessuten vil opplysninger fra katalogtjenesten kunne være nødvendig for å identifisere den person som er innehaver av et sertifikat. Det såkalte »entydige navnet» som inngår i sertifikatet skal hindre forveksling med andre sertifikater og er en nøkkel mot sertifikatkatalogen og andre sertifikater, men vil ikke nødvendigvis inneholde de opplysninger som er nødvendige for at brukeren kan gjøre seg opp en mening om det er ønskelig å handle med sertifikatinnehaveren eller f eks å gå videre til entydig oppslag i en kredittopplysnings-database.

Den totale anvendeligheten av nøkkelsertifikatsystemet vil derfor stille like store krav til påliteligheten i katalogtjenesten som til innholdet i selve sertifikatet.

På samme måte er det av stor betydning at man for sertifikater som av en eller annen grunn skal trekkes tilbake har et effektivt varslingssystem tilgjengelig. Et sertifikat kan måtte trekkes tilbake fordi:

- En brukers hemmelige nøkkel antas å være kompromittert, slik at den tilhørende offentlige nøkkelen må gjøres ugyldig
- En brukers tilhørighet (f.eks arbeidssted) er endret, slik at rollesertifikatet ikke lenger er gyldig
- En brukers autorisasjon/lisens (eks. lege og tannlege) er endret
- En bruker skal ikke lenger sertifiseres av den samme sertifikatmyndigheten som tidligere
- Sertifikatmyndighetens sertifikat antas å være kompromittert (i så fall må alle sertifikater utstedt av denne myndigheten tilbakekalles)
- En bruker har brutt sertifikatmyndighetens sikkerhetspolicy

Rutinene for tilbakekalling av sertifikater, herunder hvem som er berettiget til å trekke et sertifikat tilbake, er kritiske for påliteligheten i systemet. Det samme gjelder tilgang til oversikter over tilbaketrukne sertifikater.

6.9 Oversettingstjenester

De brukere som opptrer i det elektroniske markedet må forholde seg til sertifikater utstedt av en annen TTP enn den de selv har avtale med. I praksis vil det imidlertid være vanskelig for den enkelte å forstå og vurdere holdbarheten av den policy vedkommende TTP driver under, og etter omstendighetene også hvilke begrensninger i sertifikatet. Brukeren vil derfor ha behov for veiledning fra sin egen TTP.

Denne type veiledning adskiller seg fra selve sertifikathåndteringen og bør adresseres særskilt i avtalen mellom partene. Dette gjelder både omfanget av veiledningstjenesten og det mulige erstatningsansvar TTP'en kan pådra seg i forbindelse med slik veiledning.

6.10 Tidsstempling mv

Ytterligere et krav til sikkerhetsfunksjonalitet er behovet for å kunne dokumentere at et dokument eksisterer, eller faktisk var i noens besittelse på et gitt tidspunkt, heretter kalt tidsstempling. Denne funksjon finner vi igjen blant annet i tinglysningssystemet [og i systemet med notifisering av skyldneren ved overdragelse av enkle fordringer].

Det kan være av betydning for mottakeren av en melding ikke bare å kunne dokumentere at han er i besittelse av en melding med et visst innhold avgitt av en viss avsender, men også at han faktisk hadde meldingen i sin besittelse på et gitt tidligere tidspunkt enn det tidspunkt det er aktuelt å legge meldingen frem. Meldingen kan f eks være en kvittering fra kommunikasjonsmotparten på at en tidligere oversendt melding faktisk var mottatt eller på at en bestemt melding var oversendt en bestemt tredjepart [deponering eller f eks anbud med innleveringsfrister og åpningstidspunkt] eller videresendt derfra.

En tidsstemplingstjeneste uten forankring i særskilte rettsregler vil imidlertid kun ha bevismessig betydning. Dersom tjenesten skal ha direkte virkning, f eks i forbindelse med løsning av prioritetskonflikter, må det regelendringer til.

6.11 Kommentar og konklusjon

I dette kapitlet har vi fremstilt ulike oppgaver og måter å organisere dem på, som ledd i en nødvendig infrastruktur for alminnelig, frivillig bruk av digitale signaturer. Oppgavene er mange og i gjensidige avhengighetsforhold til hverandre. De kan gjøres av mange organisasjoner, som med et fellesbegrep noe upresist kalles TTP'er. Begrepet indikerer at det dreier seg om tjenester fra noen som ikke er direkte part i kommunikasjonen, de er eksterne, som grunnlag for å gjøre det på en sikker måte. Et sentralt spørsmål er selvfølgelig hva som skal til for at de skal kunne smykke seg med betegnelsen »tiltrodd». Dette diskuteres i mange land. Noen vil at det skal ligge spesielle, internasjonalt anerkjente kriterier eller regler til grunn. Andre vil at tillit oppnådd ut fra vanlige markedsmekanismer bør være tilstrekkelig. Noe fasitsvar finnes ikke. Man må gjøre noen valg, jf forslaget til direktiv fra EU, som prøver å tilfredsstille begge disse syn. Hvilket er en klar internasjonal trend.

Det er offentlig nøkkelkryptografi som ligger til grunn, med sine krav til å gjøre de offentlige nøklene så tilgjengelige som mulig, og det motsatte for de private nøklene. Sentrale elementer er å få knyttet en sikker forbindelse mellom identitet og en offentlig nøkkel, slik at andre kan stole på dette. Dette gjøres ved at en tredjepart som »alle» kan stole på og kjenne til, utsteder en bekreftelse (et sertifikat) på at nøkkelen tilhører den oppgitte identiteten. Dermed kan vi være sikre på at »underskriften» hører til den personen. Sikrere enn ved håndtegnet underskrift på papir. I tillegg gir teknikken andre sikkerhetstjenester på kjøpet, som at

endringer i informasjonen/dokumentet ikke kan skje uten at vi kan oppdage det, og at den kommunikasjonen som skjer mellom avsender og mottaker kan bevises i ettertid (ingen kan nekte for det de har gjort). For å få til dette, må oppgaver på mange områder løses, nasjonalt og internasjonalt.

Fordi spørsmålene knyttet til jus, teknologi og organisering har så mange fellespunkter, er sentrale diskusjoner lagt til kapittel 8, for fellesbehandling, til en viss grad kamuflert som »bare» juridisk diskusjon. Men jus handler om normer knyttet til fakta, og faktagrunnlaget her er nettopp teknologi og organisering. Det er dermed naturlig å diskutere disse spørsmålene i sammenheng ett sted. Det er også liten tvil om at det er på regelverkssiden myndighetene må gjøre en grunnleggende innsats, både for å oppnå rettslig aksept der det trengs, men ikke minst sosial aksept. Et minimum av tilretteleggelse for markedet med ulike rettslige virkemidler vil gi et nødvendig grunnlag, også for de organisatoriske løsningene for sertifiseringstjenester.

Konklusjonen er at en sertifikat-basert infrastruktur for offentlig nøkkelhåndtering (også kalt PKI) kan sørge for de mekanismene som er nødvendige for å etablere tillitsforhold og tilgang til sikkerhetstjenester. Tillitsforholdene kan gå ut over eller på tvers av både organisatoriske og internasjonale grenser, til og med når partene er ukjente for hverandre. Mens de tekniske sidene ved en PKI i en viss grad er på vei fra det umodne til det noe mer modne nivået, er det nok generelt slik at de korresponderende operasjonelle temaene ikke er like godt forstått eller utprøvd. Det er grenser for hvor langt en kan komme i teoretiske tilnærminger til de organisatoriske spørsmålene. Det må nå legges betydelig vekt på å vinne praktiske erfaringer i større grad enn hittil både teknisk og operasjonelt, og på å spre de erfaringer som gjøres slik at de kan deles.

---

22 Med «offentlig» siktes her til den alment tilgjengelige nøkkelen, ikke at infrastrukturen skal drives av det offentlige. Her kan det være både offentlige og private aktører.

23 Begrepet "aktør" er her et samlebegrep for personer, virksomheter og informasjonssystemer når de opptrer som kommunikasjonspart ved elektronisk samhandling.

24 Disse begrepene kommer opprinnelig fra henholdsvis x.509 versjon3 sertifikat spesifikasjon og the American Bar Association Digital Signature Guidelines.

25 Norsk EDIPRO: Meldingssikkerhet - Tiltrodde tredjeparter og digitale signaturer, 1994; Digitale signaturer og tiltrodde tredjeparter, 1996.

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Forslag til tiltak for aksept og utbredelse

7. Rettslige rammebetingelser - hva er gjort i Norge og i utlandet?

7.1 Norske initiativ

Med unntak av enkelte endringer som er gjennomført i tolloven og sjøloven samt det pågående arbeid med revisjon av lovgivningen om behandling av personopplysninger, er det, etter det arbeidsgruppen kjenner til, ikke satt i verk tiltak for å tilpasse andre deler av norsk lovgivning til elektronisk samhandel.

Enkelte rettslige spørsmål i forbindelse med elektronisk samhandling er drøftet i rapporten EDIPRO94 26. Administrasjonsdepartementet ga i 1994 en arbeidsgruppe i oppdrag bl a å »vurdere forholdet mellom bruk av e-post og saksbehandlingsregler mv. for forvaltningen», som inkluderte sikkerhetsaspekter. Gruppen la frem sin rapport året etter 27, og mente bl a at man først måtte finne praktiske løsninger, som kan være »utgangspunkter for forslag til nye rutiner, konvensjoner og regler. Deretter når elementene til en mer samlet løsningsplattform foreligger, forutsettes en nærmere juridisk vurdering». Statskonsult initierte senere en juridisk kartleggingsstudie, publisert i 1997 28, der fokus ikke var begrenset til e-post, men favnet elektronisk saksbehandling generelt. Resultatene fra kartleggingen og en senere høringsrunde er dokumentert i en nylig utgitt rapport fra Statskonsult høsten 1998 29.

7.2 Internasjonale og regionale initiativ

På internasjonalt nivå, og i en rekke enkeltland, har spørsmål knyttet til rettslig regulering av elektronisk samhandel fått myndighetenes og lovgivers oppmerksomhet. Nedenfor følger hovedpunkter i noen utvalgte regulatoriske initiativ, i første omgang EU Kommisjonens utkast til direktiv om elektroniske signaturer, UNCITRAL Model Law on Electronic Commerce og utkastet til Uniform Rules on Electronic Signatures, OECDs initiativ samt en kort redegjørelse for situasjonen i bl a Danmark, Sverige og noen andre land.

7.2.1 EU Kommisjonens utkast til direktiv om «Electronic Signatures»

I mai 1998 la EU Kommisjonen frem et forslag til direktiv om elektroniske signaturer. 30 Direktivet var en oppfølging av kommisjonens tidligere kommunikasjoner: »A European Initiative in Electronic Commerce» 31 og »Ensuring Security and Trust in Electronic Communication - Towards a European Framework for Digital Signatures and Encryption» 32.

Som et forarbeid til direktivutkastet har Kommisjonen i regi av universitetet i Leuven i Belgia gjennomført en omfattende kartlegging av viktige juridiske forhold i de enkelte medlemsland og i EØS-landene 33.

I forbindelse med arbeidet med direktivet ble det arrangert en »eksperthøring» i København i april 1998 der representanter for Kommisjonen var tilstede for å få synspunkt før direktiv-utkastet 34 ble ferdigstilt. Kommisjonen har gitt FIPR i oppdrag å samle inn synspunktene som nå kan hentes fra en webside 35.

Direktivets formål er å skape rammebetingelser for sikker elektronisk handel og således stimulere den økonomiske aktiviteten i dette markedet. For å oppnå dette er det blant annet viktig å sikre rettslig anerkjenning av elektroniske signaturer i medlemslandene og unngå at varierende nasjonal lovgivning er til hinder for fri flyt av tjenester.

I direktivutkastet foreslås minimumskrav til elektroniske signaturer for å sikre et tilfredsstillende sikkerhetsnivå og fri flyt av tjenestene mellom medlemslandene. Videre foreslås minimumsregler for tjenesteleverandørens erstatningsansvar med hensyn til sertifikatenes innhold. Erstatningsreglene skal bidra til å sikre brukernes tillit til tjenestene og fremme utvikling av sikre løsninger.

Direktivet omfatter primært identitetssertifikater og stiller krav om ikke-diskriminering av elektroniske signaturer og at signaturer basert på sertifikater og tjenesteytere som oppfyller visse minstekrav 36 skal anerkjennes på samme måte som håndskrevne signaturer. Det legges opp til en teknologinøytral regulering som skal kunne omfatte mer enn digitale signaturer.

Det blir ikke adgang til å innføre krav om forhåndsautorisasjon for å tilby sertifiseringstjenester, men det vil være mulig for det enkelte medlemsland å etablere frivillige autorisasjonsordninger for å stimulere tjenester av høy kvalitet. Dessuten legges det vekt på hensiktsmessige ordninger for anerkjenning av sertifikater utstedt i tredjeland. Direktivets bestemmelser må gjennomføres i det enkelte medlemsland.

7.2.2 UNCITRAL's arbeider

UNCITRAL (United Nations Commision on International Trade Law) vedtok i 1996 sin «Model Law on Electronic Commerce». Modelloven omfatter mer enn det vi i dag vanligvis omtaler som «elektroniske meldinger», f eks er telex og telefax inkludert. Modelloven skal blant annet sikre at en elektronisk melding ikke diskrimineres bare på det grunnlag at den er elektronisk, og det nedfelles kriterier for å vurdere hvorvidt formkrav som skriftlighet, underskrift og original skal anses oppfylt. Videre skal det sikres at elektroniske meldinger kan føres som bevis. Modelloven har også til formål å bidra til harmonisering av rettstilstanden for å legge til rette for global elektronisk handel. Modelloven er utarbeidet med sikte på å kunne implementeres som selvstendig lov. Modelloven har ingen direkte virkning men må gjennomføres i hvert enkelt land. Det foreligger ingen folkerettslig forpliktelse til å gjennomføre den.

Etter vedtagelsen av modelloven har UNCITRAL nedsatt en arbeidsgruppe som skal utarbeide såkalte «Uniform Rules on Electronic Signatures». Et utkast fra desember 1997 ble diskutert under et møte i Wien i januar 1998 Et revidert utkast til Uniform Rules ble behandlet av arbeidsgruppen i juni/juli 1998. Rapporten fra dette møtet ble offentliggjort 21.8.98. 37 Det fremgår at det er delte meninger om hvordan slike regler skal utformes på en del sentrale punkter. En ny versjon av utkastet til Uniform Rules foreligger, og skal behandles på et nytt møte i arbeidsgruppen 8. - 19. februar 1999. 38

Våren 1998 fremmet USA forslag til UNCITRAL om at det skulle utarbeides et forslag til internasjonal konvensjon på området, bl a basert på den eksisterende Model Law on Electronic Commerce. Forslaget møtte imidlertid stor motstand i kommisjonen og ble ikke realitets-behandlet i arbeidsgruppen under deres sesjon i juni/juli 1998.

7.2.3 OECD Cryptography policy

I mars 1997 vedtok OECD anbefalinger til medlemslandene om retningslinjer for »kryptopolitikk» 39, som også er tilgjengelig på norsk fra Nærings- og handelsdepartementet. Medlemslandene anbefales å unngå umotiverte hindringer for bruk av krypteringsteknologi som kan hindre fremveksten av internasjonal handel og kommunikasjonsnettverk.

Retningslinjene innebærer bl a at brukerne fritt skal kunne velge mellom ulike teknologier 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 prinsipper. Dette innebærer bl a at man må skille mellom krypteringsteknologi benyttet for innholdskryptering og kryptering i forbindelse med signering og integritetsikring 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.

OECD har også utgitt en oversikt over det enkelte lands tilnærming til spørsmålet om autentisering og sertifisering. 40

7.3 Utenlandske nasjonale initiativ

7.3.1 Danmark - forslag til lov om digitale signaturer

Det danske Forskningsministeriet la i februar 1998 frem et utkast til lov om digital signatur.

Lovforslaget synes å være smalere i sitt anvendelsesområde enn direktivutkastet ved at det kun omtaler digitale signaturer. Lovforslaget går derimot lenger enn direktivutkastet når det gjelder reguleringsomfang ved at det behandler flere sider ved bruken av digital signatur.

Lovforslaget inneholder blant annet regler om autorisasjonsordning for nøkkelsentre (sertifikatutstedere), utløp og sperring av nøkkelsertifikater, begrensninger i anvendelsen av digital signatur, heftelse og ansvar ved bruk av digital signatur, regulering av formkrav om skriftlighet og underskrift samt plikt for offentlige myndigheter til å kunne motta digital kommunikasjon.

Forut for fremlegging av lovforslaget ble det gitt en redegjørelse for Folketinget i desember 1997. Redegjørelsen »Sikker digital kommunikation» tar bl a for seg behovet for sikkerhets-tjenester og rettslig klarhet og sikkerhet, se http://www.fsk.dk/fsk/div/digkomrd.html

I en pressemelding sommeren 1998 opplyser Forskningsministeriet at de første danske prosjekter med digital signatur skal settes i verk. Det er bevilget ca 15 millioner kroner til ni piloprosjekter som vil omfatte private, studenter, bønder og små og mellomstore virksomheter. 41Ved siden av de praktiske erfaringene pilotprosjektene vil gi, vektlegges det også at de vil legge et solid grunnlag for det videre arbeidet med lovgivningen om digital signatur, blant annet ved å belyse behovet for å likestille digital signatur og håndskrevet underskrift på forskjellige myndighetsområder.

7.3.2 Sverige - utredninger

I november 1997 gjennomførte Kommunikationsdepartementet, Närings- og handelsdepar-tementet og IT-kommisionen i samarbeid med SEIS og enkelte andre organisasjoner, en

høring om «identifiering och identitet i digitala miljöer». Rapporten fra høringen er publisert som IT-kommisionens rapport 4/98, SOU 1998:36.

Det fremgår av rapporten at man anser innføring av sikre systemer for digital identifisering som en forutsetning for realiseringen av elektronisk samhandel i åpne nett. Det anses avgjørende at de løsninger som innføres nyter stor tillit blant brukerne, og det hevdes at en skrittvis innføring er å foretrekke fremfor rask innføring av en kompleks helhetsløsning. I rapporten påpekes behovet for raskt å starte arbeidet med å vurdere utvikling av en nærings-rettslig lovgivning tilpasset det elektroniske marked, og det antydes et 4-5 års perspektiv for gjennomføringen av slike endringer.

Kommunikationsdepartementet har siden høsten 1997 arbeidet med en problem- og behovs-beskrivelse for digitale signaturer og støtte i lovgivningen. Resultatene er nylig fremlagt som Ds 1998:14 »Digitala signaturer - en teknisk och juridisk översikt». Rapporten gir anvisning på en rekke utredningsoppgaver som bør gjennomføres, herunder kartlegging og vurdering av formkrav i svensk lovgivning, mulig regulering av rettsvirkningen av digitale signaturer og organiseringen av sertifikatutstedere samt klargjøring av ansvarsspørsmål. Det er interessant å merke seg at man foreløpig ikke ser grunn til å gi særlige regler om digitale signaturers bevis-kraft eller mulighet for generelt å fastslå at digitale signaturer oppfyller lovgivningens mange formkrav.

Av tidligere arbeider kan det vises til IT-utredningen: «Elektronisk dokumenthandtering» (SOU 1996:40). Utredningen inneholder blant annet forslag til en rekke lovendringer for å legge til rette for elektronisk samhandel, herunder forslag til legaldefinisjoner for begreper som «digitalt dokument», «digital signatur» og «digitalt stämpel».

Delrevisjoner av lovgivningen er gjennomført bl a på toll- og skatteområdet.

7.3.3 Tyskland - lov om digital signatur

Tyskland vedtok i 1997 en «multimedialov» som blant annet inneholder en særlig regulering av digital signatur. I motsetning til øvrige initiativ på området regulerer den tyske loven ikke spørsmålet om når en digital signatur oppfyller lovbestemte formkrav, men fastsetter detal-jerte krav til hva som kan anerkjennes som en digital signatur iht loven, herunder krav til sertifikat-utstedere. I hvilke tilfeller den digitale signatur kan benyttes vil fremgå av annet regelverk. Det er opplyst at det nå arbeides (i Justisdepartementet) på lovgivning angående rettslig virkning og gyldighet knyttet til digitiale signaturer.

Formålet med den tyske loven er å gi betingelsene for hva som kan anses som en sikker infrastruktur for brukere av digital signatur i Tyskland. Loven tillater andre prosedyrer/opplegg for digitale signaturer, - den bygger på frivillighet. Loven ser ut til å være ment som en slags de facto standard for bruk av sikre digitale signaturer, men i lovs form.

I tillegg til loven finnes det en forskrift (Digital Signature Ordinance), der man i et visst omfang finner betydelig mer detaljerte regler.

7.3.4 Italia - lov om elektroniske dokumenter mv

I mars 1997 ble det i Italia vedtatt en lov som uttrykkelig tillegger elektroniske meldinger «gyldighet og relevans» i «enhver» rettslig sammenheng. Senere er det vedtatt detaljerte

bestemmelser for gjennomføring av prinsippene. Reguleringen favner både virkningen av å benytte elektroniske meldinger og digitale signaturer og krav til bl a sertifikatutstedere.

Bestemmelsene innebærer bl a at en elektronisk melding anses å oppfylle kravet til skriftlighet i rettslig forstand. Videre finnes regler om elektroniske meldingers beviskraft, noe som bl a vil avhenge av om det har vært benyttet digitale signaturer eller ei.

7.3.5 Storbritannia - utredninger

Våren 1997 la det britiske Handels- og Industridepartementet frem et såkalt «Consultation Paper» vedrørende mulig lisensiering av TTP'er. På bakgrunn av innkomne uttalelser til dette la departementet i april 1998 frem sin holdning i form av en såkalt «Secure Electronic Commerce Statement». 42

Det fremgår av uttalelsen at den britiske regjering legger stor vekt på utviklingen av elektronisk handel og at den anser sikkerhet og tillit som nødvendige forutsetninger. Det legges stor vekt på bruk av krypteringsteknologi som virkemiddel, men skilles skarpt mellom bruk for integritetssikring og innholdskryptering (konfidensialitet).

Regjeringen varsler at den vil innføre lovgivning på området og samarbeider med Kommisjonen for å sikre overenstemmelse med EU's løsninger. De varslede tiltak vil så langt som mulig være i overensstemmelse med OECD's Guidelines on Cryptography Policy, og arbeidet i UNCITRAL.

7.3.6 USA - delstatslovgivning og utredninger 43

Flertallet av statene i USA har vedtatt, eller vurderer, lovgivning om elektroniske og/eller digitale signaturer. Det er imidlertid store forskjeller i tilnærmingsmåten i de ulike delstater.

Det skilles i stor utstrekning mellom «elektronisk signatur» generelt og «digital signatur» basert på offentlig nøkkel kryptografi. Det er ingen felles oppfatning av hva som kvalifiserer som en «elektronisk signatur».

Omlag halvparten av statene som har eller vurderer lovgivning på området, ser på spørs-målene knyttet til digitale signaturer basert på en offentlig nøkkel infrastruktur. Der det er innført lisensieringsordninger er disse frivillige for sertifikatutstederen, men digitale signaturer basert på sertifikater fra lisensierte utstedere nyter særlig rettslig anerkjennelse. Et typisk trekk er at meldinger med digital signatur, i motsetning til elektroniske signaturer i sin alminnelighet, blir ansett som selv-autentiserende dokumenter. Det innebærer at den person som er knyttet til signaturen antas å ha signert dokumentet med mindre vedkommende fører motbevis.

7.3.7 Australia - utredninger

Australias justisminister la i april 1998 frem en rapport med tittelen «Electronic Commerce: Building the Legal Framework». Rapporten var utarbeidet av en ekspertgruppe og skal danne basis for regjeringens videre arbeid på området. Regjeringen legger stor vekt på utviklingen av elektronisk handel og rapporten er lagt ut til bred høring.

Ekspertgruppen baserte sitt arbeid med rapporten på to hovedprinsipper, henholdsvis å oppnå funksjonelt rettslig likestilling mellom papirbasert og elektronisk handel og ikke-diskriminering mellom ulike teknologier. I rapporten advares det mot innføring av for detaljerte regler, bl a på grunn av risikoen for løsninger som avviker fra markedets behov, og på grunn av den hurtige teknologiske utvikling.

I rapporten vurderes bl a UNCITRAL «Model Law on Electronic Commerce», og ekspertgruppen gir sin tilslutning til modellovens løsninger på en rekke punkter.

7.4 Kommentar og konklusjon

Aktivitetsnivået internasjonalt er høyt. De modeller og initiativer som det arbeides med i sentrale land og organisasjoner har stor verdi/betydning, også for Norge. Det er derfor om å gjøre å komme i posisjon til å vurdere nytten av og utnytte best mulig det arbeidet som skjer ute. Som et minimum bør vi løpende sørge for å følge så godt med i det som skjer at vi er ajour til enhver tid (ikke bare hver gang det nedsettes en arbeidsgruppe).

Konklusjonen er at der sentrale internasjonale organisasjoner er aktive, må Norge sørge for å ha aktiv deltakelse. Dette er den beste måten å tilføre landet nødvendige kunnskaper og kompetanse, samt en nødvendig måte hvis en vil påvirke løsninger, som i sin tur vil ha betydning nasjonalt. Så vidt arbeidsgruppen vet, deltar Norge i EU/EØS- og i OECD-sammenhenger på en aktiv måte, også i forhold til digital signatur og TTP-spørsmål. Deltakelse i UNCITRALs arbeider har vi derimot ikke. Dette må etter vår mening vurderes som en meget viktig arena å delta på. Norge må også sørge for å være ajour til enhver tid med kunnskaper om andre lands utvikling og erfaringer.

---

26 Meldingssikkerhet - Tiltrodde tredjeparter og digitale signaturer, Norsk EDIPRO 1994.

27 Elektronisk post i statsforvaltningen, Utredning fra arbeidsgruppe avgitt 9.juni 1995, Administrasjonsdepartementet.

28 Elektronisk saksbehandling, En kartlegging av juridiske problemstillinger som reises ved innføring av elektronisk saksbehandling i forvaltningen. Statskonsult notat 1997:3

29 Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering, Statskonsult rapport 1998:13.

30 COM(98)297 final, 13.05.98.

31 COM(97)157 final, 16.04.97.

32 COM(97)503 final, 08.10.97.

33 Websiden har denne adressen: http://www.law.kuleuven.ac.be/icri/projects/digisig_eng.htm

34 Forberedende materiale og rapport fra høringen finnes på: http://www.fsk.dk/fsk/div/hearing

35 Følgende webside: http://www.cl.cam.ac.uk/users/rja14/consultation.html

36 Se nærmere om direktivets forslag til minstekrav i punkt 12.2.6 nedenfor.

37 Rapporten heter REPORT OF THE WORKING GROUP ON ELECTRONIC COMMERCE ON THE WORK OF ITS THIRTY-THIRD SESSION (New York, 29 June-10 July 1998), A/CN.9/454, og finnes på adressen http://www.un.or.at/uncitral/en-index.htm

38 Det utkastet til Uniform Rules fra Uncitrals arbeidsgruppe som skal behandles på neste møte i februar 1999 finnes her: http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-79.htm

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

40 Outline and preliminary draft: Inventory of Approaches to Authentication and Certification in a Global Networked Society, 24 June 1998, OECD.

41 Digital signatur vil blant annet bli brukt til elektronisk selvbetjening i kommuner og i den danske Lånekassa for utdanning, til søknader og innrapporteringer fra virksomheter, til kommunikasjon av sensitive helseopplysninger. Mer enn 3000 brukere blir involvert. For å motta tilskudd fra Forskningsministeriet, må pilotprosjektene forplikte seg til å overholde bestemte krav til standarder for digitale signaturer. Dermed kan man få det første konkrete bidraget til en sammenhengende dansk infrastruktur for digital signatur. Se pressemeldingen og oversikt over pilotprosjektene på websiden: http://www.fsk.dk/fsk/presse/980630-1.html

42 http://www.dti.gov.uk/CII/ana27p.html

43 Oversikten er basert på Thomas J. Smedinghoff, Analyzing State Digital Signature Legislation, August 1997, hhttp://www.mbc.com/ds_rev.html. Se også http://www.mbc.com/ds_sum.html som inneholder en »summary of electronic commerce and digitial signature legislation» som i tillegg til USA omfatter internasjonale initiativer og mange andre lands lovgivningsaktiviteter på disse områdene.

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Rådet for IT-sikkerhet

Digitale signaturer gir tillit til elektronisk kommunikasjon

Forslag til tiltak for aksept og utbredelse

---

8. Rettslige rammebetingelser - hva må gjøres i Norge?

8.1 Regler om når digitale signaturer kan benyttes og hvilke virkninger de har

8.1.1 DS på områder uten lovbestemte formkrav

Utgangspunktet i norsk kontraktsrett er prinsippet om formfrihet. Det finnes ikke noe alminnelig krav om at avtaler skal inngås skriftlig eller bevises skriftlig. Videre bygger norsk rett på prinsippet om fri bevisføring og fri bevisvurdering. Dette innebærer at partene i alminnelighet er fri til å føre ethvert bevis de finner hensiktsmessig, og dommeren avgjør etter en samvittighetsfull prøvelse av hele saken hvilket faktum som anses sannsynliggjort og som derved legges til grunn for pådømmelsen. Der ingen formkrav finnes er partene altså fri til å

innrette seg slik de finner hensiktsmessig med tanke på den aktuelle transaksjonens betydning og muligheten for å sannsynliggjøre overfor en domstol hva som har funnet sted, jfr nærmere om bevisspørsmålene under punkt 8.1.3 nedenfor.

8.1.2 DS på områder med lovbestemte formkrav

Samtidig finnes det enkeltbestemmelser i lovgivningen (lov og forskrift) som stiller krav om at spesielle formkrav er fulgt, ved at særskilte dokumenter benyttes eller ved krav om underskrift. Hovedtyngden av disse bestemmelser finner vi innenfor forvaltningens område og i bestemmelser om meldinger til domstoler og offentlige myndigheter, men enkelttilfeller finnes også i privatretten. I disse tilfellene blir det spørsmål om den fremgangsmåte som er valgt er egnet til å oppfylle de formkrav som eksisterer, og om så ikke er tilfellet, hvilke effekter det eventuelt skal ha. Det er ingen automatikk i at manglende overholdelse av en formregel medfører ugyldighet. Resultatet kan etter omstendighetene f eks være at bevisbyrden endres dersom det er en ordensforskrift som oversittes eller at et annet regelverk kommer til anvendelse slik at noen forventede effekter uteblir eller andre oppstår.

Det er også grunn til å tro at begrunnelsen bak formkravene varierer fra lov til lov. En bedre innsikt og forståelse for hvilke hensyn som skal ivaretas i det enkelte tilfelle er nødvendig før man på forsvarlig måte kan si noe om i hvilke tilfeller elektroniske meldinger og digitale signaturer kan oppfylle formkravene.

Det er derfor ikke meningsfylt å drøfte generelt om en digital signatur er «gyldig». Spørsmålet er snarere om det, på det aktuelle området, foreligger noen formkrav, og i så fall hvorledes disse i det aktuelle tilfellet skal forstås, eventuelt hva som er virkningen av ikke å etterkomme dem.

For å kunne ta stilling til når elektronisk kommunikasjon kan eller bør kunne benyttes som alternativ til papirkommunikasjon, må man gjennomgå hvert enkelt av formkravene i norsk rett. Dette innebærer en kartlegging og systematisk gjennomgang av alle underskriftskrav i norsk lovgivning. En grov oversikt finnes i rapporten EDIPRO94 44.

Det blir imidlertid for snevert utelukkende å fokusere på kravet til underskrift. De behov og krav til funksjonalitet og sikkerhet som eksisterer i tradisjonell papirbasert kommunikasjon er et resultat av kombinasjonseffekter mellom papirets og den håndskrevne underskriftens egenskaper. Papiret som informasjonsbærer er et stabilt medium, det holder informasjonen samlet og informasjonsinnholdet er tilgjengelig uten hjelpemidler og over lang tid. Bruk av en virksomhets brevark vil av mange bli oppfattet som indikasjon på et representasjonsforhold. Konvolutten holder dokumentene samlet under overføring og gir mottakeren grunn til å stole på at alt kommer fra samme avsender. Den håndskrevne underskrift skal først og fremst knytte avsenderen til innholdet i meldingen. Det er alle disse funksjonene i kombinasjon vi forholder oss til når vi i normalsituasjonen aksepterer en skriftlig melding som etterrettelig.

Dette gjør vi til tross for at underskriften sjelden kan verifiseres før transaksjonen finner sted (med unntak av banktransaksjoner og andre tilfeller der prøve på avsenders signatur er tilgjengelig på forhånd). Etter at konvolutten er åpnet kan vi heller ikke i prinsippet dokumentere at ikke vedleggene til det signerte brevet i ettertid er endret eller at den midterste siden i brevet er byttet ut. Ofte vil det imidlertid være andre omkringliggende omstendigheter som gjør et saksforløp mer sannsynlig enn et annet.

Også den papirbaserte kommunikasjon har altså svakheter som vi hittil har kunnet leve med og som det ikke nødvendigvis er regningssvarende å løse ved overgang til elektroniske systemer. Vi skal imidlertid ikke undervurdere betydningen av at bruk av fortrykte dokumenter og formularer, svakheter ved kopieringsteknikken mv, hittil har vært en terskel for misbruk. Det kan synes som man i dag er i ferd med å erstatte fortrykte blanketter og brevark med utskrift i høykvalitets laserskrivere. Scanner-teknologien gjør etterfølgende manipulering lettere. På sikt vil muligens også papiret som medium oppleve et press mot troverdigheten basert på de samme betenkeligheter som mange i dag har i forhold til elektroniske meldinger.

Som vi har sett vil digitale signaturer med bruk av sertifikater tilfredsstille de fleste av de funksjoner papirdokumentet og underskriften har. Den viktigste egenskap den digitale signaturen ikke erstatter er papirdokumentets direkte tilgjengelighet, dvs den egenskap at man kan tilegne seg innholdet uten tekniske hjelpemidler. I tillegg er det knyttet særegne utfordringer til langtidslagring av elektroniske dokumenter. Riksarkivet tar opp i utkastet til den nye NOARK-4 standarden spørsmålet om langtidslagring av digital signatur og hevder der at måten verifisering foregår på betraktes som utenforliggende i forhold til NOARK-4 (ref kap 10.2.2 i NOARK-4), - dette gjelder også langtidsverifisering av sertifikater fra TTP-tjenester. 45 Det er pr i dag ikke avklart hvilke instanser som har ansvar for å definere krav til verifisering av langtidslagrete digitaliserte elektroniske dokumenter. Papirdokumentets direkte tilgjengelighet og stabilitet ved lagring er egenskaper som vil være av betydning når man skal vurdere om f eks forvaltningslovens krav til skriftlighet ved underretning om enkeltvedtak kan oppfylles ved hjelp av elektroniske meldinger. En må da også ta i betraktning at man kan klare seg helt uten papir med full tilgjengelighet dersom man bruker elektroniske hjelpemidler, og likevel være mer sikker på dokumenters og signaturers ekthet ved hjelp av digitale signaturer enn ved bruk av de tradisjonelle håndunderskrifter.

Når rettsreglene skal legge til rette for bruk av elektroniske signaturer mer generelt, blir det spørsmål om det bør gis en egen lov, eller om endringene best kan skje i de respektive regelverk. Det finnes gode grunner for begge løsninger. Noen endelig konklusjon er det neppe grunnlag for å trekke før kartleggingsarbeidet for formkravene er gjennomført. Dersom antagelsen om at papir/underskriftskravet i norsk rett har en rekke forskjellige funksjoner er riktig, vil det bli vanskelig å lage en dekkende generell lov. Dette er også den foreløpige konklusjonen i den svenske utredningen Ds 1998:14. Eksempler på argumenter for en egen lov kan imidlertid anføres: behovet for å skape klarhet og trygghet på et nytt og teknisk komplisert område av tverrgående samfunnsmessig betydning (herunder elektronisk handel), at det er snakk om å legge til rette for en trygg og effektiv overgang fra papirbasert til elektronisk kommunikasjon (som samfunnsfunksjoner i stor grad er avhengige av), at lovgivning både gjennom politisk og pedagogisk signaleffekt kan fremme overgangen på en gunstig måte, og til slutt at egen lov kan egne seg best i forhold til vår tilpasning til eventuelle EU-direktiv.

Det kan imidlertid være grunn til å vurdere nærmere den løsning som er foreslått bl a i Danmark. Forslaget legger opp til at det etableres tekniske løsninger som skal tilfredsstille visse minstekrav. Dersom kravene oppfylles vil det være grunnlag for å akseptere løsningen i forhold til en rekke nåværende formkrav, men vurderingen må skje særskilt for de enkelte deler av lovgivningen. Det er enda ikke tatt stilling til om dette skal skje gjennom en "velg inn", "velg ut" eller "kombinasjonsmodell". "Velg inn" modellen innebærer at den enkelte regelverksforvalter fatter beslutning om at et regelverk skal omfattes av loven om digitale signaturer. "Velg ut" modellen innebærer at alle lover omfattes med mindre

regelverksforvalter fatter beslutning om at et regelverk ikke skal omfattes. Kombinasjonsmodellen innebærer at man i en overgangsperiode benytter en "velg inn" modell, men at man fra et bestemt tidspunkt omfatter alle som ikke uttrykkelig er "valgt ut".

8.1.3 Beviskraft for elektronisk informasjon, herunder digitale signaturer

Dersom det ikke foreligger noen lovbestemte eller avtalte krav til hvilken form en melding (dokument, informasjon, e l) skal ha, er den enkelte i utgangspunktet fri til å velge kommunikasjonsform. I de fleste tilfelle vil dette innebære at formen må sikre at meldingen er tilgjengelig for mottaker, klarhet med hensyn til meldingens innhold, at mottaker har tillit til meldingen og at det i ettertid kan sannsynliggjøres at meldingen hadde det aktuelle innhold og utsteder.

Dette blir langt på vei et spørsmål om bevis og en elektronisk meldings beviskraft. Den alminnelige tillit til en kommunikasjonsform påvirkes av i hvilken grad man kan forvente at en domstol eller annen aktuell instans vil akseptere elektroniske meldinger som dokumentasjon for hva som har passert mellom partene. Det er grunn til å tro at også en del av formkravene i lovgivningen er helt eller delvis motivert av bevishensyn.

Næringslivets deltakere i arbeidsgruppen har fremholdt at det viktigste virkemiddel for å fremme utbredelsen av elektronisk samhandling i næringslivet vil være å gjøre det som skal til for å gi en elektronisk melding/digital signatur utvetydig, positiv beviskraft. Et tilsvarende behov finnes antakelig i offentlig forvaltning. Dette er neppe et stort problem verken i den enkelte bedrift eller i forvaltningen for den interne kommunikasjon, som sjelden eller aldri er gjenstand for tvil eller i verste fall domstolsbehandling. Ved kommunikasjon som krysser grensen mot omverdenen oppleves det derimot en sterkt hemmende usikkerhet mht hva som er status på dette punktet.

Spørsmålet blir imidlertid hvor langt man kan gå i å si noe generelt om en meldings eller digital signaturs beviskraft, hvilke premisser som må legges til grunn for at regelen skal komme til anvendelse og hvilke innvendinger som kan rettes mot regler eller generelle uttalelser om beviskraft.

Vi antar at en eventuell klargjøring, for å få den nødvendige gjennomslagskraft, må komme fra offisielt hold. Dette kan skje enten gjennom et lovgivningsinitiativ som f eks kan supplere de nåværende bestemmelser om papirdokumenters beviskraft i tvistemålsloven, eller gjennom en formell uttalelse fra Justisdepartementets lovavdeling. Et viktig skritt kan i tillegg være å legge til rette for, og instruere, domstolene til å benytte elektroniske meldinger og digitale signaturer i domstolens administrative kommunikasjon med departementet. Dette vil kunne bidra til å alminneliggjøre kommunikasjonsformen for domstolene og vil også virke positivt på den alminnelige tillit til elektroniske meldinger og digitale signaturer.

Innholdsmessig kan det neppe komme på tale med noen absolutt regel om at elektroniske meldinger skal legges til grunn for domstolenes avgjørelse (selv om alle meldinger kan legges frem til vurdering). Et slikt pålegg ville stride mot prinsippet om den frie bevisbedømmelse.

Derimot kan det vurderes å innføre en presumpsjonsregel vedrørerende autentiseringen, dvs en regel som legger meldingens/dokumentets innhold til grunn som avgitt av den oppgitte avsender, med mindre det føres motbevis. En slik regel innebærer altså at det er den som bestrider å være avsender som må føre bevis for dette. Dette er den modellen som er valgt for

papirdokumenter i tvistemålsloven § 262 som lyder: "Et privat dokument, som er egenhændig underskrevet med navn, og hvis indhold ikke gir særlig grunn til mistanke, avgir fuldt bevis for, at indholdet skriver sig fra den, som har underskrevet dokumentet. Motbevis er ikke utelukket." Bestemmelsen gir imidlertid neppe uttrykk for noe annet enn det som uansett ville følge av prinsippet om fri bevisbedømmelse.

Alternativet er at den som påberoper seg dokumentet må bevise at det faktisk er avgitt av den påståtte avsender.

Det vil antakelig være hensiktsmessig å begrense eller presisere en eventuell presumpsjonsregel til å gjelde bestemte egenskaper ved meldingen, f eks om meldingens integritet og avsender, men uten å ta stilling til virkningen av at meldingen er sendt. Det vil etter vår oppfatning være vanskelig i gi noen presumpsjonsregel som også tar opp i seg avsenders subjektive hensikt eller de materielle virkningene av at meldingen er sendt. Dette er spørsmål som normalt ikke hører hjemme i vurderingen av et dokuments "ekthet", men derimot selvstendige tema som i tid kommer etter at man har tatt stilling til "ektheten".

De nærmere vurderinger av omfang og gjennomføring av en uttalelse eller regel om beviskraftsvirkningen må utredes videre. Den usikkerheten som knytter seg til disse spørsmålene er antakelig en av de viktigste hindringene for alminnelig tillit til og utbredelse av elektronisk kommunikasjon som har en økonomisk eller annen verdi av en viss betydning. Næringslivet etterspør som nevnt konkrete løsninger så fort som mulig, for å få slått klart fast at digitale signaturer har uttrykkelig beviskraft. Forvaltningen har også behov for å få et godt nok grunnlag til å bli helt trygge på dette området. Usikkerheten kan løses ved klare regler, men også ved klare utsagn der dette juridisk ikke er problematisk. Alminnelig folkeopplysning knyttet til de områdene som ikke er problematiske, bør også gjennomføres så fort som mulig. Hva som er klart for noen jurister, er ikke nødvendigvis klart for folk flest, næringsliv eller forvaltning.

Heller ikke dette er særnorske problemstillinger.

I den svenske utredningen (Ds 1998:14) uttales det at det neppe er grunn til å gi noen særlig bevisregel for digitale signaturer. Under drøftingene av utkastet til UNCITRALs Uniform Rules on Electronic Signatures synes det å være delte meninger om hvorvidt man skal ha en bestemmelse om beviskraft, men den dominerende holdning er visstnok at en slik bestemmelse bør utarbeides.

I EU-kommisjonens utkast til direktiv, Article 5, heter det at elektroniske signaturer, som tilfredsstiller kravene i direktivet, a) skal anses å tilfredsstille de rettslige krav til en håndskreven signatur; og b) skal kunne føres som bevis for domstolene på samme måte. Det siste er ikke problematisk for oss. Det er derimot ikke klart hva som ligger i kravet om at en elektronisk signatur skal anses å tilfredsstille de rettslige krav til en håndskreven signatur. Formuleringen må utvilsomt innebære at lovgivningens formkrav kan oppfylles ved hjelp av elektroniske signaturer. Spørsmålet er om det også dekker bestemmelsene om presumert beviskraft som gjelder for papirdokumenter. I et tidligere utkast til direktiv var presumpsjon for beviskraften uttrykkelig behandlet. I utkastet som ble lagt frem for Rådet etter høringsmøtet i København var denne klare formulering erstattet med den henvisning til håndskreven signatur som er nevnt over.

Direktivutkastet, Article 5, tar også opp i seg den ikke-diskrimineringsregelen som er bærende i UNCITRAL's modellov, og som innebærer at en melding ikke skal nektes rettslig effekt, gyldighet og gjennomførbarhet utelukkende på det grunnlag at signaturen er i elektronisk form eller basert på et sertifikat som ikke tilfredsstiller direktivets krav eller er utstedt av en ikke godkjent sertifikatutsteder. Hvorvidt eventuelle form- eller beviskrav er oppfylt må derimot vurderes individuelt. Det er neppe grunnlag for å se på direktivets »essential requirements» som minimumskrav i forhold til ethvert formkrav i lovgivningen. Tvert om må en anta at kravene ligger et nivå over det som i mange tilfeller bør kreves. Dette er nødvendig for å kunne gi en generell regel om oppfyllelse av lovgivningens krav.

Det er ingen grunn til å vente på utviklingen av EU-forslaget til direktiv for å finne de norske løsningene mht beviskraft. Her har vi et selvstendig norsk arbeid å gjøre, og det er ingen tid å miste. Markedet trenger løsninger raskest mulig. På den annen side bør de løsningene vi kommer til også på dette området harmonere med de internasjonale. Dette vil antakelig ikke være noe problem.

8.1.4 Hvordan skal signerte elektroniske meldinger legges frem for domstolen?

Skulle en tvist oppstå mellom to parter og det kommer til sak, må de dokumenter som er relevante for saken legges frem for domstolen. Det kan imidlertid by på utfordringer å dokumentere en elektronisk melding og signatur for domstolen.

Det er grunn til å tro at det vil ta tid før man under hovedforhandlingen dokumenterer "skriftlig" materiale ved lesing fra skjerm. Det materialet det skal leses fra skal samtidig være tilgjengelig for dommere og motparter. I alle fall i en overgangsperiode vil det bli nødvendig å legge frem kopier av elektroniske meldinger i form av papirutskrifter.

Dette er imidlertid ikke uten videre enkelt, i og med at signaturen bare kan verifiseres maskinelt og ikke på papir. Signaturen kan dessuten bare verifiseres i forhold til den originale meldingen, men ikke mot det samme meldingsinnholdet i et annet filformat.

Behovet for verifisering av de elektroniske meldingene burde i prinsippet bare forekomme i de tilfellene der en av partene bestrider innholdet av eller opphavet til et dokument. Det vil imidlertid være et praktisk problem for en part dersom motparten legger frem store mengder utskrifter av utvekslede meldinger, fordi det vil være vanskelig for parten å kontrollere at ikke innholdet i noen detaljer, bevisst eller ubevisst, er endret før utskriften fant sted. En slik utskrift vil ikke ha de visuelle "kjennetegn" som f eks en kopi av et originalbrev vil ha, og som gjør det mulig forholdsvis raskt å kontrollere egen versjon mot motpartens. Særlig i de tilfellene der flere versjoner av et dokument har versert mellom partene kan dette bli problematisk.

Det er grunn til å tro at omfanget av elektronisk kommunikasjon i kommersielle sammenhenger vil øke voldsomt i løpet av de nærmeste år, og mengden elektronisk lagret informasjon som skal presenteres for domstolene vil trolig øke tilsvarende. Det er derfor behov for at det så snart som mulig startes et arbeid med å utrede hvorledes domstolene i praksis skal forholde seg til elektroniske dokumenter som legges frem i forbindelse med en tvist.

En mulig løsning kunne være å la TTP'ene skrive ut og bekrefte meldingene, som en type "bekreftet kopi". Dette ville kunne være både lettere tilgjengelig og mer "pålitelig" for

domstolen enn å få verifiseringen utført direkte i rettssalen, i alle fall inntil domstolene selv blir utstyrt med det nødvendige utstyr som de selv har tillit til.

Et alternativ er at domstolene selv, under saksforberedelsen, verifiserer og skriver ut det nødvendige antall kopier av dokumentene.

Det er under enhver omstendighet helt nødvendig at man snarest starter utredning av hvilket utstyr domstolene i nær fremtid vil trenge for å kunne verifisere den dokumentasjon som legges frem på betryggende måte.

For øvrig nevnes at det er ikke alle dokumenter som kan presenteres i form av en utskrift, men vi antar den store massen dokumenter det er aktuelt å påberope i forbindelse med en tvist, i alle fall foreløpig, vil være tekstdokumenter, eventuelt inneholdende tegninger, grafikk mv som kan presenteres på papir.

8.1.5 Tidsbegrensninger, tilbakekall og disposisjonsbegrensninger i/av nøkkelsertifikater

Bruk av tidsbegrensede sertifikater og det forhold at sertifikater fra tid til annen vil bli tilbakekalt, enten fordi det ikke lenger er aktuelt eller fordi nøkkelen er kompromittert, reiser en rekke spørsmål med hensyn til hvilken betydning sertifikatet skal tillegges etter at det er utløpt eller trukket tilbake.

Sertifikater med gyldighetstid på f eks to år, vil regelmessig bli benyttet i forbindelse med gjennomføring av transaksjoner med en alminnelig foreldelsesfrist på tre år. Hver av partene vil ha behov for å sikre tilfredsstillende dokumentasjon til foreldelsesfristen er løpt ut.

I det danske lovforslaget antar man at det ikke kan »støttes rett på» den digitale signaturen etter utløpet av sertifikatets gyldighetsperiode med mindre meldingen blir signert på nytt med et gyldig sertifikat før det opprinnelige sertifikatet løp ut. Dette synes å være en forholdsvis upraktisk løsning.

Problemet er imidlertid reelt nok. Dersom det er gått svært lang tid etter at et sertifikat løp ut eller ble kalt tilbake kan det være grunn til å trekke en eventuell presumpsjon for beviskraft. Det kan også være at kortholders plikt til å behandle kort og kode med særlig varsomhet opphører etter at sertifikatet er løpt ut. For ikke å gå glipp av den tillitskapende effekt en slik bevisregel eventuelt skulle støtte, må man finne en løsning som ikke gjør det byrdefullt for brukerne å bevare dokumentasjon i nødvendig tid for det store antall daglige transaksjoner.

Et annet spørsmål som bør vurderes nærmere er rekkevidden av disposisjonsbegrensninger som er tatt inn i sertifikatet eller den aktuelle sikkerhetspolicy. Spørsmålet gjelder både hvem begrensningene kan gjøres gjeldende overfor, hvem som kan påberope dem og i hvilke situasjoner de kommer til anvendelse. Det kan eks bli spørsmål om hvorvidt disposisjonsbegrensninger fastsatt av sertifikatutstederen for å begrense dennes samlede ansvar under sertifikatet, skal kunne påberopes av sertifikatinnehaveren overfor tredjemann i en eventuell tvist om ansvar for uaktsom omgang med kort og kode.

8.2 Betingelser for etablering og drift av TTP

8.2.1 Er det behov for autorisasjonsordninger?

Det kan være hensiktsmessig et øyeblikk å tenke på markedet for elektronisk kommunikasjon i tre til fire grupper: de tre første er næringsliv, privatpersoner/forbrukere og offentlig sektor. Den fjerde er de som har disse utgangspunktene i ulike blandinger, der kommunikasjonen går på tvers. Behovene både på kort og lang sikt kan tenkes å variere for gruppene. Det er imidlertid mye som tyder på at det sterkeste utviklingstrekket er at det er mange felles behov til stede, på tvers av slike inndelinger.

Næringslivet vil et stykke på vei, og i alle fall på kort sikt, kunne basere sin virksomhet på kontraktsregulering av informasjonsutvekslingen og sikkerhetstjenestene. På noe lengre sikt, i forbindelse med åpning av de kontraktsregulerte lukkede miljøer, vil også næringslivet kunne ha behov for den forutberegnelighet som offentlig regulering og tilsyn kan bidra med.

Forbrukerne vil i sitt møte med næringslivet formodentlig ha de samme behov for beskyttelse i forbindelse med elektronisk handel og sikkerhetstjenester som vi kjenner fra andre forbrukerforhold. Tilsvarende vil gjøre seg gjeldende for enkeltindividets kommunikasjon med myndigheter, med elektronisk selvangivelse som et eksempel. Hvor meget som er spesielt for området DS/TTP er foreløpig usikkert, men det er i alle fall behov for å ha et grunnlag for trygghet/tillit til løsningene, samt omfattende veiledning om bruk, tjenestenes faktiske begrensninger og personvernspørsmål.

Offentlig sektor kan tenkes å ha et større behov for ensrettethet enn næringslivet som er mer sektorisert. Det virker lite hensiktsmessig at forvaltningen skal operere eller benytte flere ulike løsninger for sikkerhetstjenester ved intern og ekstern kommunikasjon. Dessuten vil borgerne og næringslivet ha et behov for å kunne møte offentlig sektor med ett grensesnitt og forutsigbarhet med hensyn til virkningen av å ta systemene i bruk.

Et eksempel på »blandingstilfeller» kan være privatpraktiserende tannleger og leger. Dersom disse skal regnes under næringslivet, vil deres kommunikasjonsbehov ikke være kontraktsregulert og innenfor lukkede miljøer. Deres kommunikasjonsbehov i forbindelse med pasientbehandlinger er i stor grad mot offentlige personer/institusjoner og offentlige myndigheter. Det er her behov for pålitelige ordninger som alle kan stole på. Behov for styring og kontroll med TTP-tjenester vil derfor for helsesektoren omfatte både offentlig og privat virksomhet.

Behovet for styring kan synes sterkere for offentlig sektor enn for den private. Det virker imidlertid klart at eventuell styring må skje ut fra et helhetlig perspektiv, der de felles behovene blir retningsgivende.

Behovet for regulering kan imidlertid også begrunnes ut fra andre hensyn enn harmonisering. Forutberegnelighet med hensyn til tjenestenes rettslige status er et slikt hensyn. Det synes som om markedet har et behov for avklaring som går ut over de generelle anbefalinger man kan gi basert på dagens spinkle rettskildesituasjon. Dessuten er det langt på vei snakk om å påvirke holdninger og de nye systemene kan trenge litt «fødselshjelp». En positiv regulering av de aktuelle systemer kan bidra til å realisere dette. En slik løsning vil også kunne innebære rettstekniske fordeler ved at det etableres objektive kriterier for å vurdere pålitelighet og mulighet for forhåndsvurdering av om kravene er tilfredstilt. Dette vil bidra til forutberegnelighet for partene.

På den annen side står man overfor den utfordring at dagens systemer for digitale signaturer ikke nødvendigvis er morgendagens løsninger, og at man risikerer å regulere «gårsdagens

teknologi». Teknologinøytral lovgivning bør derfor være en målsetting. Dette kan imidlertid være vanskelig å oppnå. De allerede foreliggende utenlandske og internasjonale regulatoriske initiativ tyder på at det er vanskelig å regulere uten å knytte reguleringen forholdsvis tett opp til en teknologi eller i alle fall en nærmere bestemt organisering eller infrastruktur. Og med de vanskeligheter det synes å være med å finne en enhetlig og hensiktsmessig regulering av forholdsvis kjente løsninger, må det vises nøkternhet med hensyn til muligheten for å få til en hensiktsmessig regulering av fremtidige løsninger som vi foreløpig ikke en gang kan skissere. Det kan nok tenkes at det finnes spørsmål som kan avklares generelt, men det er neppe noen god idé å la ønsket om en helt teknologinøytral regulering komme i veien for en hensiktsmessig regulering av det som allerede finnes og som kan bidra til å løse de behov som er uttrykt tidligere i nærværende rapport. Spesialregler for den tilstedeværende teknologi og infrastruktur kan være nødvendig. Samtidig skal en være varsom med å etablere regler som medfører konservering av løsninger som ellers ville blitt forlatt. Prosedyrer for løpende evaluering og vedlikehold av regelverk blir under enhver omstendighet viktig.

Det er tidligere i rapporten påvist behov for tilgang til autentiseringstjenester for en rekke formål, herunder elektronisk handel og elektronisk kommunikasjon i forvaltningen. Samtidig eksisterer det i dag tekniske løsninger som tilfredsstiller disse behov. Det er grunn til å spørre seg hvorfor realiseringen av tjenestene i markedet ikke har kommet lenger. Et stykke på vei kan dette naturligvis skyldes forhold i markedet, organisatoriske problemer mv, men det kan ikke utelukkes at utviklingen også forsinkes av en uhensiktsmessig regulatorisk situasjon som av partene oppleves som så usikker med hensyn til deres rettslige posisjon at den utgjør en hindring for realiseringen av tjenestene. Slik usikkerhet kan strekke seg lenger enn spørsmålet om rettslig anerkjennelse av digitale signaturer, f eks til spørsmålet om omfanget av et mulig erstatningsansvar. Slik usikkerhet bør avklares og korrigerende tiltak bør iverksettes.

En slik tilnærming finner vi også i redegjørelsen til det danske Folketinget, "Sikker digital kommunikation", fra desember 1997. Det ble bl a uttalt: Man kunne i prinsippet overlate til markedet selv å få etablert nøkkelsentre, men det er tale om et nytt marked med produkter av slik teknisk kompleksitet at det er svært vanskelig for den enkelte bruker å gjennomskue om man har fått et produkt med den nødvendige sikkerhet. Dessuten bør det gjennom lovgivning avklares i hvilket omfang nøkkelsentre er ansvarlige i forbindelse med feil og misbruk av digital signatur. Den danske regjering vil derfor ta initiativ til en regulering av nøkkelsentres virke i form av en autorisasjonsordning og en rekke minimumskrav til den digitale signaturs utforming, sikkerhetsnivå mv, som kan fremme tilbud av løsninger av "fornøden" kvalitet.

Tilsvarende arbeid kunne med fordel vurderes og gjennomføres i Norge.

8.2.2 Modeller for autorisasjons- og tilsynsordninger

Vi har ovenfor nevnt muligheten for at rettslig usikkerhet kan være en hindring for realiseringen av autentiseringstjenester. Slik usikkerhet kan antakelig reduseres ved hjelp av systemer for frivillig evaluering og forhåndsgodkjenning og/eller systemer for kontroll og oppfølging av slike tjenester, f eks i form av internkontroll og melding til tilsynsorgan. Derimot vil det neppe være hensiktsmessig å innføre obligatoriske krav om forhåndsgodkjenning for i det hele tatt å kunne utstede sertifikater. Direktivutkastet utelukker dessuten en slik mulighet. Dermed er det mulig at det blir en utvikling i retning av ett marked uten noen form for regulering, og ett marked med en form for regulering som det er frivillig å ta i bruk eller ikke. Dette kan være hensiktsmessig, som en avspeiling av ulike behov i markedet for sikkerhet, fra lavt til høyt.

Frivillig forhåndsgodkjenning vil sannsynligvis virke tillitsskapende i brukermarkedet og dette vil antakelig være en drivkraft for tjenestetilbyderne for å knytte seg til godkjennings- og/eller kontrollsystem. Samtidig kan det være grunnlag for å forhåndskvalifisere rettslige virkninger ved bruk av godkjente tjenester, f eks i forhold til oppfyllelse av formkrav i lovgivningen. Det vil i enkelte sammenhenger måtte stilles obligatoriske krav om forhåndsgodkjenning.

Som nevnt tidligere har Rådet for IT-sikkerhet 46 utarbeidet og fremmet forslag til to ulike frivillige ordninger for sikkerhetssertifisering av henholdsvis IT-produkter/systemer, og organisasjoners IT-sikkerhet. Forslagene bygger på anerkjente kriterier for evaluering og sertifisering (henholdsvis ITSEC - CC for produkter/systemer, og BS 7799 for organisasjoner).

Forslagene har vært på bred høringsrunde våren 1998. På denne bakgrunn har Regjeringen høsten 1998 foreslått kr 5 millioner på 1999-budsjettet til Nærings- og handelsdepartementet, for oppretting av de to ordningene, omtrent som foreslått av RITS. Dette kan få en klart positiv betydning også for grunnlaget for ordninger med frivillig forhåndsgodkjenning av tiltrodde tjenester fra tredjeparter i forbindelse med digitale signaturer i Norge, samt grunnlaget for aksept av sertifikater/løsninger på tvers, både av landegrensene og andre grenser.

Ikke minst av hensyn til internasjonal aksept vil TTP'er kunne tenkes å etterspørre og legge til grunn sikkerhetssertifisering av hele eller deler av sin organisasjon ut fra aktuelle kriterier og eventuelt tilgjengelige tjenester for dette i Norge, samt å ville etterspørre og bruke sikkerhetssertifiserte produkter/systemer, særlig for den oppgaveløsningen som er mest sikkerhetskrevende, med behov for høyest grad av tillit. Både det teknologiske og det organisatoriske grunnlaget for å ha tillit til en TTP vil dermed kunne forenkles. I forhold til direktivutkastet fra EU om elektroniske signaturer, gir slike løsninger mulighet for TTP'er til å dokumentere at de er i stand til å etterleve enkelte av de nødvendige reglene for å bli anerkjent/forhåndsgodkjent som TTP. En frivillig akkrediteringsordning i det enkelte medlemsland er et av virkemidlene direktivforslaget åpner for.

Enhver godkjenningsordning som gjelder tjenester som skal operere over tid, må følges opp med en kontrollordning for å sikre tillit til at det tjenestenivå som det er gitt aksept for blir opprettholdt. En slik kontrollordning kan imidlertid innrettes på ulike måter, og såvel kostnader, kostnadsfordeling og tillit til ordningene vil variere. Vi anser det helt nødvendig at det etableres eller utpekes et organ som har ansvar for oppfølging og kontroll av autoriserte TTP'er og som også på oppfordring kan utføre kontroll av ikke-autoriserte TTP'er. Vi anbefaler at slike spørsmål må vurderes i sammenheng med de ordningene for sikkerhetssertifisering av IT-produkter/systemer og organisasjoner som er omtalt over.

Kontrollordningen kan organiseres enten som periodiske kontroller utført av tilsynsmyndigheten, eller baseres på et system med intern kontroll og periodisk melding til tilsynsmyndigheten, samtidig som tilsynsmyndigheten tar stikkprøvekontroller. Dokumentasjon av tilfredsstillende prosedyrer for internkontrollen bør være en del av kriteriene for forhåndsgodkjenning som sertifikatutsteder. Vi antar at den siste modellen vil være den mest hensiktsmessige.

En slik modell vil antakelig også forenkle finansieringen av kontrollordningene, i det en vesentlig del av kostnadene bæres direkte av tjenesteyteren i forbindelse med intern

kontrollen og utarbeiding av meldinger til tilsynsmyndigheten. Det antas at full ekstern revisjon er mer ressurskrevende for tilsynsmyndigheten. Det bør også vurderes om f eks revisjonsfirmaer eller klasseselskaper kan påta seg oppgaven med f eks å kvalitetsikre det til enhver tid eksisterende internkontroll system.

Oppsummeringsvis kan vi si at behovet for et tilsyns-/kontrollorgan og kontrollordninger vil være tilstede uavhengig av hvilken modell som velges i forbindelse med eventuell forhåndsgodkjenning av sertifikatutstedere. Organiseringen og den rettslige forankring for virksomheten må utredes nærmere.

8.2.3 En offentlig støttet autentiseringstjeneste for identitetssertifikater?

Vi har vist ovenfor at det må trekkes et grunnleggende skille mellom sertifikater som utelukkende eller i det vesentlige tjener til å identifisere enkeltpersoner («identitetssertifikater» i jobbsammenheng og privat) og sertifikater som gir uttrykk for en rolle (f eks innehaver av en konto), fullmakt el («rollesertifikater»).

Identitetssertifikatene vil være gjenstand for færre endringer (f eks navnebytte el) enn rollesertifikater (som f eks må endres ved bytte av arbeidsgiver el). Identitetssertifikatene kan blant annet benyttes i kommunikasjon med det offentlige, der avsenders identitet normalt er av betydning, og andre sertifikater kan etter omstendighetene bygge på eller være tilknyttet identitetssertifikatet.

Det anbefales at identitetssertifikater bør være tilgjengelig fra det offentlige eller som en offentlig støtte tjeneste som enhver vil ha praktisk og økonomisk mulighet for å få tilgang til.

Likestilt med «sertifikat» i denne forbindelse vil være andre «elektroniske legitimasjonstegn» eller autentiseringsmekanismer som eventuelle nye tjenester vil føre med seg. Inntil videre antar vi imidlertid at tredjepartstjenester også vil være nødvendig for å tilby dette for bruk i åpne nettverk.

8.2.4 Regulatoriske tiltak må ikke etablere hindringer for markedets løsninger

Elektronisk samhandel foregår i dag i stor grad i lukkede miljøer, det vil si brukergrupper som er klart definerte og som enten har forhåndsavtale med hverandre, som i en rekke EDI-samarbeid, eller er del av et felles kontrollert brukermiljø som f eks banktransaksjoner. Felles for disse er at de sammen har definert et særskilt behov for tjenester og kan etablere rammebetingelser gjennom kontrakt eller omforente retningslinjer. Dette gir mulighet for dynamikk i samarbeidet og kan fremme tilveksten av nye tjenester. Det er av betydning at eventuelle nye regulatoriske tiltak, som er ment å virke positivt på fremveksten av elektronisk samhandel, ikke utformes slik at de oppleves som hindringer for allerede fungerende forretningsmodeller.

8. 8.2.5 Harmonisering med internasjonale løsninger og tiltak

Alle de internasjonale intitiativ som er nevnt i kapittel 5 ovenfor, tar utgangspunkt i at elektronisk samhandel vil få en stadig mer dominerende rolle, og at rettslig avklaring og tilrettelegging er nødvendig for å sikre og fremme effektiv samhandel. Videre legges det stor vekt på å redusere hindringer for grenseoverskridende handel gjennom harmonisering av de rettslige rammebetingelsene.

Elektronisk handel vil også for Norges vedkommende ha en typisk grenseoverskridende dimensjon og ethvert nasjonalt tiltak må ta hensyn til internasjonale initiativ på området. Avvik fra anerkjente regionale eller globale løsninger bør unngås og må i alle fall ha en vektig begrunnelse.

Videre bør Norge involvere seg aktivt i de prosesser som pågår bl a i UNCITRAL. Dette vil bl a kunne gi verdifull erfaring og materiale til arbeidet med hjemlige tiltak i tillegg til bedre innsikt i tankegangen bak de internasjonale inititativene.

8.2.6 EU's forslag til krav til "autorisert TTP"

Utkastet til EU direktiv nedfeller et antall minimumskrav som en sertifikatutsteder må oppfylle for at digitale signaturer som støttes av sertifikatene automatisk skal oppnå rettslig anerkjennelse. Kravene, som er gjengitt nedenfor, vil være et naturlig utgangspunkt når man skal vurdere tilsvarende krav for norsk retts vedkommende. Hensynet til anerkjenning av sertifikater på tvers av landegrensene gjør dette nødvendig.

Sertifikatutstederen skal i henhold til direktivutkastets Annex II (for alle detaljer, se originalteksten):

1. dokumentere den pålitelighet som er nødvendig for å tilby sertifiseringstjenester;

2. drive en umiddelbar og sikker tilbakekallingstjeneste;

3. med hensiktsmessige virkemidler (for eksempel ved bruk av RA) verifisere identiteten og handleevnen til den person som skal ha utstedt et sertifikat;

4. ansette personell med den nødvendige kompetanse og erfaring vedrørende tjenestene og teknologien;

5. benytte systemer og produkter som det er grunn til å stole på, som ikke kan modifiseres til å bli benyttet for andre formål enn de er beregnet for;

6. innføre tiltak mot forfalskning av sertifikater og sikre konfidensialitet i forbindelse med generering av nøkler;

7. ha tilstrekkelig finansiell styrke til å operere i henhold til direktivets krav og til å møte et eventuelt erstatningsansvar, f eks gjennom hensiktsmessig forsikring.

8. oppbevare alle relevante opplysninger i tilknytning til et sertifikat i en passende tidsperiode, særlig for å kunne fremlegge dokumentasjon i en eventuell rettssak;

9. ikke oppbevare eller kopiere private krypteringsnøkler med mindre nøkkelinnehaveren selv uttrykkelig ber om det;

10. informere forbrukere skriftlig, forut for kontraktsinngåelse, i et forståelig språk og ved en »varig kommunikasjonsmetode», om vilkårene for bruk av sertifikatet, herunder eventuelle begrensninger vedrørende ansvar, eksistensen av frivillig akkreditering og prosedyrene for klager og tvisteløsning.

UNCITRAL's utkast til Uniform Rules inneholder ingen angivelse av hvilke krav en sertifikatutsteder må tilfredstille. En modell bygget over de samme prinsipper som direktivutkastet er imidlertid nevnt som alternativ dersom slike krav skal formuleres.

8.2.7 Offentliggjøring av forretningsvilkår og retningslinjer for drift av autentiseringstjenester

Både av hensyn til forbrukerne og myndighetenes mulighet for å observere utviklingen i markedet og vurdere nødvendige tiltak vil det være hensiktsmessig at forretningsvilkår og retningslinjer for driften er tilgjengelig. Det bør også vurderes å stille minimumskrav til hvilke opplysninger som skal offentliggjøres (f eks sertifiseringspolitikken - Certification Policy og sertifiseringspraksis - Certification Practice Statement).

Det forhold at tjenestene er nye, og den betydning de antas å ville ha for utviklingen av det elektroniske informasjonsmarkedet tilsier at man holder et særlig oppsyn med tjenestene. På noe sikt kan det tenkes at man vil se fellestrekk i tjenesteleverandørenes vilkår og retningslinjer som kan nedfelles i lovgivningen og på den måten forenkle og øke oversiktligheten i markedet. Krav om offentliggjøring vil også ha betydning for brukernes mulighet til enkelt å orientere seg og gjøre seg opp en mening om tjenestenes innhold og troverdighet. Tilgang vil også ha betydning for sertifikatutstederens mulige erstatningsansvar overfor en tredjemann som disponerer i tillit til innholdet i et sertifikat men som ikke selv har avtale med sertifikatutstederen.

8.2.8 Nye modeller for handel - virkninger på formueretten og andre rettsområder

Fremveksten av elektronisk handel fører med seg mer enn endring av kommunikasjonskanaler. Det medfører også endringer i rollefordeling og etablerte relasjoner. Dels i form av fremvekst av nye tjenester, dels ved øket spesialisering og informasjonsdeling og -spredning, men også i forhold til den grunnleggende forutsetning at fysiske personer, med evne til å vurdere den enkelte situasjon, er involvert i transaksjonene. Fremveksten av automatiserte transaksjonssystemer er en del av dette. Man skal ikke utelukke at fremveksten av disse systemene rokker ved forutsetninger for eksisterende regulering som kan gjøre det nødvendig med oppdateringer.

Vi skiller som tidligere nevnt mellom de såkalte identitetssertifikater og rollesertifikater. Fordeling av oppgaver og ansvar i forbindelse med rollesertifikater bør utredes. Det samme gjelder de øvrige rettslige virkninger av å løsrive rollene fra den underliggende identitet, f eks i forhold til fullmektigens ansvar ved overskridelse av fullmakter og rollesertifikatets posisjon i forhold til eksisterende fullmaktstyper som frasagnsfullmakten.

I tillegg bør man vurdere nærmere håndteringen av sertifikater som ikke er knyttet til noen enkeltperson men som direkte identifiserer en virksomhet eller et informasjonssystem. I tillegg reiser tidsbegrensning og tilbakekalling av sertifikater særlige spørsmål.

Det bør også settes i verk tiltak for å vurdere hvorvidt eksisterende straffebestemmelser på tilfredsstillende måte dekker de handlingsalternativer som oppstår i forbindelse med elektronisk handel. Hensiktsmessige straffesanksjoner mot misbruk av nøkler og infrastruktur kan være en medvirkende faktor når tillit til systemene skal etableres.

8.2.9 Sårbarhetsanalyser knyttet til etablering av autentiseringstjenester og økende elektronisk samhandel.

Etterhvert som en stadig større andel av kommunikasjonen foregår elektronisk øker også avhengigheten av disse systemene, blant annet som følge av at manuelle rutiner og alternativer nedbygges og kravene til hastighet øker. En utvikling i retning av kommunikasjon i åpne nett vil samtidig øke avhengigheten av tilgang til autentiseringstjenester.

Dersom en enkelt bruker av tjenestene opplever en system- eller sikkerhetssvikt vil dette vanligvis være et lokalt problem for den virksomhet eller etat det gjelder. Hvis derimot en bransje eller sektor av norsk næringsliv baserer sine autentiseringstjenester på sertifikater utstedt av en bestemt tjenesteleverandør, og det inntrer forhold som gjør at tilliten til nevnte tjenesteleverandør faktisk svekkes, vil dette kunne få store ringvirkninger dersom virksomhetenes sertifikater for en periode ikke anerkjennes av handelspartnerne. En slik situasjon kan etter omstendighetene få samfunnsøkonomisk betydning, og det bør iverksettes arbeid for å vurdere mulige konsekvenser og mottiltak. Utredningsarbeidet bør løpe parallelt med iverksetting av tjenestene.

8.3 Personvernspørsmål

Øket elektronisk samhandel utløser også en rekke spørsmål av personvernmessige utfordringer i forbindelse med sertifisering. Dette gjelder bl a spørsmålet om de såkalte »elektroniske spor» og muligheten for å opptre anonymt. Men ut fra et personvernmessig synspunkt kan man også oppstille et krav om at man må ha mulighet for entydig å kunne identifisere seg selv og derved unngå å bli forvekslet med en annen. Disse problemene er ikke nye, men de vil forsterkes i takt med at vi i stadig større grad benytter datamaskinbaserte nettverk som basis for vår informasjonsbehandling.

Personopplysningslovutvalgets innstilling (NOU 1997:19 »Et bedre personvern») behandlet blant annet spørsmålet om elektronisk samhandel. Innstillingen er nå til behandling i Justisdepartementet og en lovproposisjon er ventet i løpet av høsten 1998. Arbeidsgruppen ser det derfor ikke som sin oppgave å drøfte personvernspørsmålene i særlig grad. Noen selvstendig drøfting av slike spørsmål er ikke gjennomført i arbeidsgruppen.

I det følgende vil vi bare kort gjengi noen overordnede synspunkter på hvilken særlig betydning bruk av digitale signaturer og nøkkelsertifikater kan ha for personvernet.

Personopplysninger samles inn, behandles, lagres og gjøres tilgjengelig for andre i forbindelse med søknad om nøkkelsertifikat, utferdigelse og publisering av disse og i forbindelse med tilbakekallingslister.

Systematisk utlevering av nøkkelsertifikater vil innebære økt spredning av de personopplysninger sertifikatet inneholder. På den annen side vil sertifikatet normalt bli benyttet i tilknytning til verifisering eller kryptering av en melding som enten inneholder eller forutsetter de samme opplysningene som finnes i sertifikatet. For eksempel vil sertifikatinnehaverens navn normalt være en del av den melding sertifikatet er relatert til. Et rollesertifikat som f eks bekrefter en persons fullmakt til å opptre på vegne av en virksomhet, vil vanligvis bare bekrefte riktigheten av et forhold som uansett forutsettes å være til stede når en ansatt bestiller en vare på vegne av en bedrift. I normalsituasjonen vil sertifikatet altså ikke tilføre noen opplysninger av betydning.

Det vil også være mulig å operere med anonymiserte rollesertifikater. I en rekke tilfeller vil det være uten interesse for mottakeren av en melding hvem avsenderen faktisk er. Det kan være tilstrekkelig å vite at vedkommende er autorisert til å opptre på vegne av en virksomhet eller til å få tilgang til en tjeneste.

Utover sertifikatene selv vil også sertifikatkatalogene og de såkalte »tilbakekallingslistene» inneholde personopplysninger. Sertifikatkatalogene vil inneholde opplysninger som skal gjøre det mulig å knytte et sertifikat til en fysisk person. Dette kan nok etter omstendighetene være opplysninger som går utover det som finnes i den underliggende melding, f eks opplysninger om bosted, men det vil i de fleste tilfelle være tale om opplysninger av triviell karakter og opplysningene vil ofte være tilgjengelig også fra andre kilder. Kataloginformasjon vil ikke bli spredt aktivt på samme måte som sertifikater, men vil være tilgjengelig på forespørsel. Tilbakekallingslistene vil inneholde opplysninger om sertifikater som ikke lenger er gyldige. Det vil være et valg om årsaken til tilbakekallingen skal fremgå eller ikke.

Det er tenkelig at tilgang til krypteringsteknologi og nøkkelinfrastrukturtjenester, også kan være nyttige verktøy for å ivareta personvernhensyn.

For det første er krypteringsteknologien og nøkkelinfrastrukturen et velegnet virkemiddel for å beskytte informasjon mot uautorisert innsyn under overføring og lagring.

For det andre gjør teknologien det mulig å oppnå sikker identifisering, og derigjennom unngå å bli forvekslet med en annen.

Det reduserer også muligheten for at uvedkommende kan komme til å opptre i en annens navn og på den måten skaffe seg uautorisert adgang til informasjon eller knytte en ufordelaktig handling eller opplysning til den vedkommende utgir seg for å være. Det kan ikke utelukkes at tilgangen til elektronisk kommunikasjon etablerer en avstand og »ufarliggjøring» som senker terskelen for uønskede handlinger som de fleste ellers ville avstått fra. Mulighet for sikker identifisering kan bidra til å forebygge dette.

Bruk av fødselsnummer i sertifikat eller katalog kan være en hensiktsmessig måte å oppnå entydig identifisering på, eventuelt med bruk av ulike former for kryptering eller »pseudonym». Det må også tas henstn til hva som er personvernmessig forsvarlig eller akseptabelt i et helhetlig perspektiv.

8.4 Ansvar og erstatning

Spørsmålet om ansvar og erstatning kan for det første oppstå i forholdet mellom en sertifikatinnehaver og en tredjepart, f eks i forbindelse med misbruk av en privat nøkkel.

For det andre kan ansvar oppstå i forholdet mellom TTP'en og en sertifikatbruker. Sertifikatbrukeren kan være TTP'ens egen abonnent eller en tredjepart som stoler på innholdet i et sertifikat eller katalog.

Tap kan også oppstå hos en tredjepart som uriktig er blitt innført i en katalog uten egentlig å være kunde hos TTP'en. Det siste er et spørsmål av typisk personvernmessig art og bør muligens drøftes i det perspektivet. De to andre situasjonene er mer tradisjonelt erstatningsrettslig preget.

Usikkerhet om mulig ansvar for misbruk av digitale signaturer, sertifikater med uriktig innhold og svikt i tilgjengeligheten til hele eller deler av tjenestene, antas å utgjøre en vesentlig hindring for utbredelsen av digital signatur systemer og TTP-tjenester, og det er viktig å få spørsmålene utredet nærmere. Dette er dels et spørsmål om å klarlegge gjeldende rett, dels et spørsmål om det er behov for å gripe inn med lovgivning eller på annen måte skape avklaring eller endring av den ellers bestående rettstilstand.

8.4.1 Sertifikatinnehavers ansvar

Vi vil først se på sertifikatinnehavers omgang med sin private nøkkel og de problemer det kan forårsake.

Situasjonen kan f eks være at den registrerte taper kontroll med kort og kode ved at noen overværer bruken og tilsniker seg kortet mens vedkommende en kort stund forlater sin arbeidsplass el. Tilgang til kortet og koden setter besitteren i stand til å opptre som rette innehavers elektroniske dobbeltgjenger. Dette vil raskt lede til at noen lider tap, ved at misbrukeren i løpet av kort tid kan generere et stort antall transaksjoner. Det vil alltid gå en viss tid før rette innehaver får meldt fra om at nøkkelen er kompromittert, sertifikatet blir trukket tilbake og databasen blir oppdatert med de nye opplysninger.

Beskrivelsen ovenfor er et typisk tilfelle av falsk, dvs noen opptrer og utsteder meldinger under en annens identitet. Tradisjonelt vil en person ikke bli bundet eller pålagt ansvar dersom noen urettmessig utgir seg for vedkommende. Den bærende tanke er at vedkommende ikke har noen mulighet til å verge seg mot misbruk av egen identitet. Den eneste som kan oppdage og forebygge falsken er eventuelt mottaker.

Dette kan imidlertid stille seg annerledes dersom den det gjelder har vært uforsiktig med remedier som setter andre i stand til å utgi se for vedkommende. Slik har det f eks vært antydet for signaturstempler ol. Parallellen til den private nøkkelen er nærliggende. Situasjonen vil jo her dessuten være at mottaker nettopp ikke har noen mulighet for å verge seg. Kontroll av signaturer, sertifikater og tilbakekallingslister, som er de kontroller det er mulig å foreta innenfor rammen av tilgjengelige tjenester og teknologi, vil ikke gi noen indikasjoner på at noe er galt i scenariet ovenfor.

Dette er likevel ikke uten videre nok til å binde den uskyldige pseudoavgiveren. Spørsmålet er om ikke man må kunne identifisere noe subjektivt klanderverdig hos vedkommende for at ansvarsallokering skal kunne skje. Typisk at vedkommende uaktsomt har latt uvedkommende få innsyn i de koder eller passord som styrer tilgangen til den private nøkkelen eller somlet med å melde fra om at kortet som inneholder nøkkelen er kommet på avveie.

Om man skulle komme til at pseudoavgiveren kan bebreides blir det spørsmål om han skal anses bundet til den transaksjon som er foretatt eller om forholdet kun skal utløse et erstatningsansvar. Spørsmålet er drøftet i UNCITRAL uten at det er oppnådd enighet om løsningen.

TTP'ens egne kunder kan lide tap f eks ved at deres sertifikat ikke er tilgjenge

8.4.2 Sertifikatutsteders ansvar overfor egne abonnenter

lig, feilaktig er ført på en tilbakekallingsliste eller inneholder uriktige opplysninger som gjør at vedkommendes kommunikasjonsmotpart avviser en transaksjon som følge av at sertifikatet ikke kan verifiseres. TTP'ens ansvar i denne situasjonen vil i første rekke bero på en tolking av avtalen mellom partene om hvilken ytelse TTP'en har påtatt seg å levere.

TTP'ens kontraktsplikter kan være formulert som omsorgsforpliktelser eller resultatforpliktelser.

Omsorgsforpliktelsen vil gjerne være begrenset til å utføre tjenesten med den aktsomhet man i alminnelighet må kunne forvente for tilsvarende ytelser, f eks at det blir gjennomført forsvarlige kontroller av en brukers identitet eller at forsvarlige prosedyrer følges ved vedlikehold av sertifikatkataloger og tilbakekallingslister. Resultatforpliktelsen er derimot kjennetegnet ved at TTP'en forplikter seg til å levere et bestemt resultat, f eks at sertifikatene skal være objektivt sett korrekte i sitt innhold. Antakelig vil TTP'ens tjeneste inneholde elementer av begge deler. Også når det gjelder ansvar for sertifikatenes innhold vil man kunne finne begge typer, f eks dersom TTP'en operer med flere sertifikattyper med ulikt sikkerhetsnivå.

Det alminnelige utgangspunkt er at TTP'en er objektivt ansvarlig for mislighold av en resultatforpliktelse mens han for en omsorgsforpliktelse kun hefter dersom det er utvist uaktsomhet. Forskjellen behøver imidlertid ikke være så stor som den kan synes, i det aktsomhetsnormen i visse tilfeller settes så høyt at det nærmer seg et objektivisert ansvar, særlig dersom det gjelder svikt ved tjenestens kjerneegenskaper. Det er grunn til å tro at TTP'en, som selger sine tjenester på tillit, er særlig utsatt for en skjerping av aktsomhetskravet.

I det foreliggende utkast til direktiv er det foreslått en mellomløsning. TTP'en er ansvarlig for riktigheten av innholdet i et sertifikat med mindre feilen skyldes opplysninger han har mottatt fra den sertifikatet er utstedt til og TTP'en kan dokumentere at han har tatt de forholdsregler som er praktisk mulige for å verifisere de aktuelle opplysningene. Denne situasjonen retter seg imidlertid mot den som stoler på innholdet i et sertifikat. Ansvaret overfor egne kunder, eller for svikt i tjenestens tilgjengelighet, er ikke behandlet.

8.4.3 Sertifikatutsteders ansvar overfor tredjemann (villedningsansvaret)

Bruk av digitale signatursystemer i åpne nettverk vil bl a være kjennetegnet ved at de aktuelle sertifikater også vil bli utvekslet med aktører som ikke selv er kunde hos sertifikatutstederen. Dersom sertifikatet f eks inneholder uriktige opplysninger, eller feilaktig ikke er ført på en tilbakekallingsliste, kan økonomisk tap oppstå hos den som disponerer i tillit til at sertifikatet er gyldig og inneholder korrekte opplysninger. Spørsmålet er om den tapslidende kan kreve hele eller deler av dette tapet dekket av TTP'en. Dette reiser vanskelige erstatningsrettslige spørsmål som det foreløpig ikke finnes noe klart svar på.

For det første er det spørsmål om hvilket grunnlag TTP'en eventuelt skal hefte på. For det andre et spørsmål om hvilke deler av tjenesten og hvilke medhjelpere det heftes for. For det tredje blir det et spørsmål om hvilke tap som omfattes av et eventuelt ansvar.

To motstridende hensyn vil her være behovet for et erstatningsansvar for å sikre tillit til at tjenestene holder tilfredsstillende kvalitet på den ene siden, og behovet for å sikre TTP'en mot et så tyngende eller usikkert ansvar at det hemmer fremveksten av denne type tjenester i

markedet på den annen. I og med at primærområdet for tjenestene er transaksjoner med et stort tapspotensiale vil også de mulige erstatningskrav kunne anta betydelig størrelse. Det ligger en betydelig utfordring i å finne en rimelig balanse mellom disse to hensynene.

I tillegg kommer det særlige poeng at tjenestene skal benyttes i et globalt elektronisk marked. Situasjonen i dag er at grunnlaget for erstatning for denne type tap i stor grad varierer mellom de ulike land. Harmonisering med rettsstillingen hos våre handelspartnere vil derfor være et viktig poeng for å unngå unødig friksjon i forbindelse med grenseoverskridende transaksjoner. Direktivutkastets forslag til løsning er slik sett utvilsomt et viktig moment, men etterlater flere vanskelige spørsmål uløst.

TTP'ens mulige ansvar overfor tredjepart (andre enn egne kunder) for feil begått av underleverandører behøver også avklaring.

8.4.4 Ansvar for manglende kontroll eller svikt ved lisensiering av TTP

Dersom det iverksettes autorisasjonsordninger eller andre kontrollordninger for sertifikatutstedere, kan det bli spørsmål om kontrollorganets ansvar for manglende oppfølging eller kontroll av en virksomhet dersom noen lider tap fordi sertifikattjenesten ikke holdt et forsvarlig nivå. Grunnlaget for og konsekvensene av et slikt mulig ansvar bør utredes.

8.4.5 Ansvarets omfang og ansvarbegrensninger

I de tilfellene der ansvarsgrunnlag konstateres blir det spørsmål om hvorledes ansvarets omfang skal avgrenses.

Det blir også spørsmål om hvilke ansvarsbegrensninger som kan aksepteres og hvorledes disse skal bli virksomme mellom partene. Dette gjelder særlig behovet for kontroll med ansvaret overfor tredjemann som tjenestetilbyderen forutsetningsvis ikke har noen kontrakt med.

Løsninger basert på å bygge inn ansvarsbegrensninger i retningslinjene for driften av sertifikattjenesten eller direkte i sertifikatet har vært foreslått. Konsekvensene av de ulike løsningsforslag bør vurderes nærmere.

8.5 Kommentar og konklusjon

På bakgrunn av det rettslige landskapet internasjonalt, i EU og i Norge, ser vi at det er en rekke rettslige tiltak som må gjennomføres for å oppnå målsettingen om at elektroniske dokumenter og signaturer skal bli like akseptert rettslig og sosialt som de papirbaserte, og for at handel over elektroniske nett skal bli like vanlig som tradisjonell handel.

På spørsmålet om digitale signaturer kan tas i bruk nå, er svaret ja. På store bruksområder er det uten problemer, mens på andre kan det være juridisk problematisk eller umulig. Hvordan skal man vite når det er trygt? Prinsippene om avtalefrihet og fri bevisførsel og -vurdering gir grunnlag for at det »fritt frem» for bruk av digitale signaturer mv. Innenfor avtalefrihetens områder, enten det er mellom privatpersoner, i handel, eller annet, er det ingen rettslige hindre for bruk av digital signatur. Likevel er mange usikre på jussen, også på dette området. Det er ikke unaturlig å tenke at dette henger sammen med at teknologien er ny, kompleks og lite forståelig for de fleste, og vel foreløpig uprøvet for domstolene. Kan man stole på den da?

Teorien sier ja, både juridisk og teknisk (på visse forutsetninger / visse forbehold på det tekniske), men »folk flest» tviler. Næringslivet tviler. Forvaltningen tviler. Med slik tvil til stede i så stort omfang, vil man naturlig nok ikke investere i løsningene. Elektronisk kommunikasjon og handel kommer dermed ikke ordentlig i gang. Man føler at det mangler sikre rettslige rammebetingelser.

I tillegg er det tenkelig at mange rettsregler kan være til hinder for bruk av digitale signaturer utenfor avtalefrihetens område. På slike områder er det grunn til tvil og tilbakeholdenhet, til reglene er funnet, vurdert og eventuelt korrigert til å tillate elektroniske løsninger, eventuelt på gitte premisser. Noe annet kan føre til at man bryter regler og hensyn bak reglene, med negative konsekvenser. En slik tilstand er uholdbar, og det haster nå med å gjøre de nødvendige grep.

Hva med å stille krav til markedet for TTP-tjenester? Bør det reguleres? For å være på linje med internasjonal utvikling, herunder EU-forslaget til direktiv, må myndighetene ikke innføre obligatoriske krav til markedet, men heller legge til rette for frivillige ordninger. Disse vil være rettslig regulert og gir en høyere teknisk og rettslig trygghet, for det markedet som trenger det. Dette kan være ett av flere grunnlag for aksept av sertifikater over landegrensene. Dermed kan ett regulert og ett uregulert marked eksistere side om side, og dekke ulike behov for sikkerhetsnivå, ut fra ulike krav til grunnlaget for tillit. De deler av markedet som ikke føler behov for slik tilrettelegging forblir uhindret, og de deler av markedet som ønsker det, får tilgang til et høyere sikkerhetsnivå og en tryggere tjeneste.

En klar konklusjon fra arbeidsgruppen er at det er på det rettslige området myndighetene må gjøre en hovedinnsats, både for aksept av digitale signaturer og for å legge til rette for å kunne stole på en komplisert teknologisk og organisatorisk infrastruktur ved hjelp av gode rettslige rammebetingelser i harmoni med internasjonale løsninger. Det er sannsynlig at allmen aksept påvirkes betydelig av eventuell full rettslig aksept og gode rammebetingelser på de ulike områdene. I tillegg må det mye kunnskapsformidling til.

Del IV: Anbefalinger om tiltak

I denne delen av rapporten fremmes de tiltakene som arbeidsgruppen har samlet seg om på bakgrunn av gjennomgangen foran. I kapittel 9 legges det vekt på de rammebetingelsene som må på plass, dels av hensyn til rettslig likestilling av elektroniske dokumenter og kommunikasjon rent generelt, herunder aksept av digitale signaturer (kapittel 9.2), dels det som skal til for å tilrettelegge for etablering og drift av TTP-tjenester (kapittel 9.3), og for å få digitale signaturer »ut til folket». I kapittel 9.4 følges dette opp av forslag til tiltak som understreker at vi trenger mer praksis og konkret erfaring, utveksle erfaringer og å spre kunnskap på sentrale områder for å fremme forståelse og bruk av digitale signaturer mv. Som et viktig premiss i det videre arbeidet foreslås det mer aktiv deltakelse internasjonalt og på standardiseringsområdet.

---

44 Norsk EDIPRO, Meldingssikkerhet - Tiltrodde tredjeparter og digitale signaturer, 1994.

45 Riksarkivet har NOARK 4 på høring høsten 1998, se: http://www.riksarkivet.no/nyheter.html

46 Rådet for IT-sikkerhet, Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner, Sluttrapport 13 november 1997. Vær oppmerksom på at begrepet »sertifisering» der brukes i en annen

betydning enn i denne rapporten. Man sikter der til muligheten for å slå fast hvorvidt f eks et produkt er utviklet og fungerer i samsvar med gitte kriterier, eller en organisasjon er organisert og fungerer etter (andre) gitte kriterier. Når slikt samsvar er evaluert og konstatert etter nærmere regler, gir dette grunnlag for en såkalt sertifisering, som bekrefter samsvaret.

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Rådet for IT-sikkerhet

Digitale signaturer gir tillit til elektronisk kommunikasjon

Forslag til tiltak for aksept og utbredelse

DEL IV: ANBEFALINGER OM TILTAK

I denne delen av rapporten fremmes de tiltakene som arbeidsgruppen har samlet seg om på bakgrunn av gjennomgangen foran. I kapittel 9 legges det vekt på de rammebetingelsene som må på plass, dels av hensyn til rettslig likestilling av elektroniske dokumenter og kommunikasjon rent generelt, herunder aksept av digitale signaturer (kapittel 9.2), dels det som skal til for å tilrettelegge for etablering og drift av TTP-tjenester (kapittel 9.3), og for å få digitale signaturer "ut til folket". I kapittel 9.4 følges dette opp av forslag til tiltak som understreker at vi trenger mer praksis og konkret erfaring, utveksle erfaringer og å spre kunnskap på sentrale områder for å fremme forståelse og bruk av digitale signaturer mv. Som et viktig premiss i det videre arbeidet foreslås det mer aktiv deltakelse internasjonalt og på standardiseringsområdet.

9. Tiltak for aksept, tilretteleggelse, erfaringer og kunnskap

9.1 Innledning

I tråd med mandatet til arbeidsgruppen presenteres her forslag til tiltak for å sikre at rettsreglene legger til rette for bruk av digitale signaturer. Tiltakene i kapittel 9.2 og 9.3 er i stor grad anbefalinger om hvilke utredningsoppgaver det er behov for.

Målsettingen for de rettslige anbefalinger er at de skal lede frem til etableringen av et rettslig rammeverk som gir forutberegnelighet og trygghet og derved legger til rette for effektiv utnyttelse av elektronisk kommunikasjon i privat og offentlig sektor. Innføring og bruk av moderne informasjons- og kommunikasjonsteknologi er et sentralt spørsmål i de fleste private og offentlige virksomheter. Elektronisk utveksling av dokumenter og elektronisk saksbehandling og handel utgjør i denne sammenheng et viktig effektiviseringspotensiale. Kravene til informasjonssikkerhet i form av autentisering, tilgjengelighet, integritet og konfidensialitet vil øke, og de utviklede teknikker er nyttige verktøy for å dekke kravene.

Næringslivet har tatt konsekvensen av disse utfordringene og er i dag både tilbyder og bruker av ulike løsninger for utveksling av elektroniske dokumenter og elektronisk saksbehandling. Forvaltningen har tilsvarende stort behov og stor bruk. Utviklingen er klart markedsdrevet.

Som grunnleggende premisser ligger bl a at løsningene skal dekke konkrete behov og være tilgjengelige for relevante brukerne, ikke virke kostnadsdrivende ut over det som lar seg legitimere via en inntektsside/budsjettet, baseres på åpne og helst internasjonale standarder, fokusere på teknologi som kan bidra til å realisere nye måter å drive forvaltning og forretning på, mv. Løsningene må tilfredsstille eventuelle krav nedfelt i lov eller forskrift og må kunne virke på tvers av bransjer, forvaltninger og over landegrensene.

Alt arbeid på dette området bør skje med tilbørlig hensyn til de initiativ som kommer fra henholdsvis EU Kommisjonen, UNCITRAL og nasjonale initiativ i de andre nordiske land for å sikre regionalt og internasjonalt tilpassede løsninger og forebygge handelshindringer som følge av varierende nasjonale krav.

For øvrig er tiltakene formulert for å oppfylle målsettingene som er satt av de to siste norske regjeringene, gjengitt i kapittel 4.2 foran. Eksempel på en sentral målsetting er formuleringen om at elektronisk kommunikasjon og bruk av nett som infrastruktur for samhandling skal bli like akseptert, tillitvekkende og ha samme juridiske holdbarhet som tradisjonell papirbasert og skriftlig kommunikasjon og dokumentasjon. Et annet eksempel er formuleringen om at handel over elektroniske nett skal bli en like vanlig handelsform som tradisjonell handel. Både IT-politisk redegjørelse 1998, næringsrettet IT-plan 1998 - 2001 (Norge - en utkant i forkant), og statssekretærrapporten Den norske IT-veien, Bit for Bit, fra 1996 gir sterke mål og føringer for arbeidet på dette området.

Det kan velges mellom ulike ambisjonsnivåer. Et hovedspørsmål på det rettslige området er om man skal nøye seg med å fjerne eventuelle ubegrunnede hindringer for bruk av elektronisk kommunikasjon (slik at regler som krever papirkommunikasjon bare skal eksistere dersom papir ivaretar funksjoner som elektronisk kommunikasjon ikke kan erstatte), eller om myndighetene også skal delta mer aktivt for å legge til rette for at de rettslige rammevilkårene for elektronisk kommunikasjon blir best mulige. Et eksempel på dette kan være å la det offentlige etablere rammebetingelser for tiltrodde tredjepartstjenester.

Materialet som foreligger i dag gir generelt ikke grunnlag for helt bestemte anbefalinger om hvilke rettslige løsninger som bør velges. På ett punkt har arbeidsgruppen ut fra diskusjoner kommet til at den vil komme med en klar anbefaling om løsning, nemlig i forhold til en digital signaturs beviskraft, se kapittel 9.2 nedenfor.

9.2 Rettslig likestilling av elektroniske dokumenter og -signaturer med de papirbaserte

Tiltak 1:*Arbeidsgruppen foreslår at det blir utviklet regler som sikrer elektroniske dokumenter og signaturer anerkjennelse som bevis på linje med papirdokumenter og underskrifter (positiv beviskraft), og at vilkårene for en slik anerkjennelse klargjøres.*

Det foreslås tre tiltak på dette området, som har sammenheng med hverandre. Dette er de tiltakene arbeidsgruppen foreslår høyest prioritert (sammen med tiltaksforslag 10 om pilotforsøk), med hovedprioritet til dette forslaget om å sikre elektroniske dokumenter og digitale signaturer full likestilling/positiv beviskraft. For å klare dette, må man gjennom tiltak

2 og 3 først. Tiltak 1 fremstår derfor som en målsetting for de to andre, men ikke den eneste målsettingen.

Tiltak 2 og 3 er mer generelt og nøytralt utformet. Disse sier at man må kartlegge hindringer og nøye vurdere endringsmuligheter, i god tradisjon, før man eventuelt kommer frem til noe. Dessuten at man ikke kan foregripe resultatene av vurderingene. Dette må nødvendigvis ta noe tid, men det viktig at det ikke tar for lang tid. En tidsramme på maksimalt to år foreslås for å gjennomføre disse tre tiltakene, slik at man kommer i mål med tiltak 1 innen utløpet av år 2000. Når arbeidsgruppen på denne måten løfter frem dette ene tiltaket, og understreker at dette haster, er det for å sette kartlegging og vurderinger inn i en realistisk ramme, som har stor økonomisk og praktisk betydning, og for å uttrykke et sterkt ønske om et bestemt sluttresultat. De politiske målsettingene gjengitt i kapittel 4.2 kan etter arbeidsgruppens mening ikke nås, hvis man ikke gjennomfører dette.

Ansvarlig: Justisdepartementet.

Mulige deltakere: Nærings- og handelsdepartementet. Arbeids- og administrasjonsdepartementet. Institutt for rettsinformatikk. Statsministerens kontor. Regelverksforvaltende myndigheter generelt.

Tiltak 2:*Det bør gjennomføres et kartleggingsarbeid for å bringe på det rene når norsk lovgivning krever bruk av papir/underskrift.*

Vi viser til gjennomgangen av temaet i kapittel 8.1 foran.

Utgangspunktet er at elektroniske dokumenter og digitale signaturer nyter godt av prinsippet om formfrihet, fri bevisføring og fri bevisvurdering. De er slik sett like »gyldige» som papirversjonene.

Samtidig finnes det enkeltbestemmelser i lovgivningen (lov og forskrift) som stiller krav om at spesielle formkrav er fulgt, ved at særskilte dokumenter benyttes eller ved krav om underskrift. Det er ikke meningsfylt å drøfte generelt om en digital signatur er «gyldig». Spørsmålet er snarere om det, på det aktuelle området, foreligger noen formkrav, og i så fall hvorledes disse i det aktuelle tilfellet skal forstås, eventuelt hva som er virkningen av ikke å etterkomme dem.

For å kunne ta stilling til når elektronisk kommunikasjon kan eller bør kunne benyttes som alternativ til papirkommunikasjon, må man altså gjennomgå hvert enkelt av formkravene i norsk rett. Dette innebærer å kartlegge hvilke norske rettsregler som i dag krever underskrift/bruk av papir. Det bør med andre ord foretas en systematisk gjennomgåelse av underskriftskrav i norsk lovgivning. Noe arbeid er allerede gjort i tilknytning til tidligere EDIPRO-rapporter.

Konkret foreslår vi at kartleggingsarbeidet gjennomføres ved at regjeringen (dvs JD i samarbeid med bl a AAD og NHD) utarbeider ett eller flere høringsnotater som sendes til offentlige organer som forvalter ulike lover og forskrifter. Høringsnotatet bør oppfordre til utredning av hvilke formkrav som finnes, hvilken funksjon de har, om funksjonen er nødvendig, og i så fall om den kan erstattes ved elektroniske hjelpemidler. Vi anbefaler også at Institutt for rettsinformatikk, UiO blir invitert til å delta. Det bør vurderes om en »støttegruppe» eller »task force» bør etableres i tillegg til det arbeidet den enkelte

regelforvalter må gjøre, både til hjelp for disse og for å ta tak i helheten i problemstillingene. I denne gruppen må det finnes godt med kompetanse ikke bare på juss, men også på elektronisk kommunikasjon mv, herunder på denne rapportens område. Jf vurderingene som skal gjennomføres iht tiltak 3 nedenfor.

Dernest bør «funnene» analyseres for å klarlegge hvilke rettslige funksjoner kravet til papir/underskrift har. Det er grunn til å tro at en undersøkelse vil konkludere med at kravet til papir/underskrift i en del tilfeller ikke har noen funksjon utover en rent praktisk måte å formidle informasjon på. Papirformen har rett og slett vært eneste mulighet. I de tilfellene der papir/underskriftskravet har funksjoner utover dette, vil undersøkelsen trolig avdekke et mangfold av funksjoner - alt fra et ønske om å sikre klarhet og notoritet, som f eks avtaler om salgspant, til skriftlige dokumenter som rettighetsrepresentativ, f eks i form av et negotiabelt dokument der rettsvirkninger er knyttet til form.

Ansvarlig: Justisdepartementet.

Mulige deltakere: Nærings- og handelsdepartementet. Arbeids- og administrasjonsdepartementet. Institutt for rettsinformatikk. Statsministerens kontor. Regelverksforvaltende myndigheter generelt. En spesielt opprettet støttegruppe/ekspertgruppe.

Tiltak 3: D*et må vurderes hvilke endringer som er nødvendige eller hensiktsmessige for å få de generelle rettslige rammevilkårene på plass, og endringene må deretter gjennomføres.*

Analysen av hvilke funksjoner kravet til papir har, kan brukes til å finne kriterier for når de ulike funksjonene er blitt benyttet. Dette vil gi grunnlag for å vurdere hvilke av funksjonene som teknologien må ivareta for at elektroniske underskrifter skal bli minst likeverdig med tradisjonell papirkommunikasjon. En oversikt over typetilfeller vil gi et kvalifisert grunnlag for å mene noe om hvilke lovendringer som er nødvendige og hensiktsmessige. Det kan bli aktuelt både å fjerne eller endre eksisterende regler og å legge nye til. Viktige områder der det forvaltningsmessige ansvaret er uklart eller ikke tilstede, må klargjøres og ansvar plasseres. Ansvaret for langtidslagrete elektroniske dokumenter er ett eksempel på et slikt behov.

Regler som det kan være aktuelt å legge til lovverket, er bl a regler om hvilken bevismessig betydning elektroniske dokumenter vil ha. Hvis det ikke gis særregler, gjelder det alminnelige prinsippet om at domstolene legger til grunn det som fremstår som mest sannsynlig. Hvis retten mener at en elektronisk signatur med stor grad av sikkerhet fastslår at det er A som har utferdiget dokumentet, vil retten legge til grunn dette.

Et alternativ til det alminnelige prinsippet om fri bevisvurdering er å gi regler som tillegger elektroniske dokumenter og -signatur positiv beviskraft på linje med papirdokumenter, og klargjør vilkårene for dette (f eks at den aktuelle TTP-tjenesten tilfredsstiller visse tekniske og organisatoriske minstevilkår). På den måten kan en rydde av veien usikkerhet om hvor stor vekt domstolene vil tillegge et elektronisk dokument. Hvilken løsning som bør velges, må vurderes nærmere. Poenget her er bare å gi et eksempel på problemstillinger som krever nærmere utredning før lovvedtak kan treffes.

Vurderingene som gjøres må også ta i betraktning at løsningene på dette området vil bety mye for om man i fremtiden får et tilstrekkelig grunnlag for at effektiviseringspotensialet som ligger i elektronisk utveksling av dokumenter skal kunne realiseres.

En nødvendig forutsetning for at en slik utvikling skal finne sted, er at det etableres tilstrekkelig tillit til elektroniske dokumenter og at denne tilliten baseres på et sikkert fundament. På den tekniske siden er man kommet et stykke gjennom dokumenterte og utprøvde standarder og teknikker basert på begrepene digitale signaturer og tiltrodde tredjeparter. Området er imidlertid fremdeles ungt, umodent og i startfasen, og det tilbys på markedet løsninger til forskjellige behov og med varierende sikkerhetsnivå og kvalitet. Beviskraften i et elektronisk dokument er imidlertid ikke i seg selv avklart selv om dokumentet er signert med en digital signatur utstedt ved hjelp av tekniske og organisatoriske fullverdige løsninger.

Denne situasjonen begrenser næringslivets og forvaltningens utnyttelse av teknikkene ved at en ikke kan være sikker på hvilken verdi en investering i løsninger vil ha. Verdien av generelle løsninger for elektronisk dokumentutveksling kan dermed ikke fastslås og virksomheter kan ikke basere seg på denne kommunikasjonsform med mindre det er etablert manuelle og papirdrevne rutiner ved siden av. Disse rutinene er fordyrende og begrenser nytteffekten av overgang til elektronisk dokumentutveksling gjennom å fjerne deler av rasjonaliseringsgevinsten.

Situasjonen kan også bidra til at det i næringslivet blir en bransjevis utvikling der det utvikles en rekke løsninger for enkeltbransjer, men som ikke kan brukes generelt. Helt parallell risiko løper en i offentlig forvaltning.

For å endre denne situasjonen foreslår arbeidsgruppen som nevnt i tiltak 1 at det blir utviklet regler som sikrer elektroniske dokumenter anerkjennelse som bevis på linje med papirdokumenter/underskrifter (positiv beviskraft), og at vilkårene for en slik anerkjennelse klargjøres.

Vilkårene (tekniske og organisatoriske) for å gi digitale dokumenter beviskraft bør utformes slik at den enkelte virksomhet ut fra forretningsmessige vurderinger kan foreta den nødvendige tilpasningen, herunder de markedsmessige. Avklaringen bør gjøre det mulig for tilbyder av sertifikat-tjenester å tilby sertifikater som er generelle i forhold til bransjer og virksomheter, mens valget av bruk bør overlates til den enkelte bedrift/virksomhet ut fra egne behov.

Siden elektronisk handel og kommunikasjon generelt vil øke sterkt i årene som kommer, vil mengden av elektronisk lagret informasjon som skal legges frem for domstolene ventelig øke tilsvarende. Det er derfor behov for raskest mulig å utrede hvordan domstolene i praksis skal forholde seg til slik elektronisk informasjon som legges frem i forbindelse med tvister.

Når rettsreglene skal legge til rette for bruk av elektroniske signaturer mer generelt, blir et første lovteknisk spørsmål om det bør gis en egen lov, eller om endringene best kan skje i de respektive regelverk. Det finnes gode grunner for begge løsninger. Noen endelig konklusjon utover forslaget i tiltak 1 skal vi ikke driste oss til å foreslå, ettersom det neppe er grunnlag for å trekke (andre) slike konklusjoner før det innholdsmessige arbeidet er gjennomført. Eksempler på argumenter for en egen lov kan imidlertid anføres: behovet for å skape klarhet og trygghet på et nytt og teknisk komplisert område av tverrgående samfunnsmessig betydning (herunder elektronisk handel), at det er snakk om å legge til rette for en trygg og effektiv overgang fra papirbasert til elektronisk kommunikasjon (som samfunnsfunksjoner i stor grad er avhengige av), at lovgivning både gjennom politisk og pedagogisk signaleffekt

kan fremme overgangen på en gunstig måte, og til slutt at egen lov kan egne seg best i forhold til vår tilpasning til eventuelle EU-direktiv.

Ansvarlig: Justisdepartementet

Mulige deltakere: Nærings- og handelsdepartementet. Institutt for rettsinformatikk. Statsministerens kontor. Regelverksforvaltende myndigheter generelt. En spesielt opprettet støttegruppe/ekspertgruppe.

9.3 Tilrettelegging for etablering og drift av TTP-tjenester

9.3.1 Frivillig godkjennings- og kontrollordning for TTP'er

Tiltak 4:*Det etableres frivillig ordning som tilbyr TTP'er å operere iht til autorisasjon/godkjenning ut fra anerkjente kriterier.*

Enhver samhandling mellom parter er basert på tillit mellom partene og til den måten samhandlingen skjer på. Som oftest reguleres dette av avtaler partene imellom og krav til de løsninger som benyttes. Dette er et naturlig utgangspunkt også ved bruk av digitale signaturer og tiltrodde tredjeparter.

Det finnes ulike metoder for etablering av tillit. En måte er å la den annen part og løsningen undergå en vurdering. Skal slike vurderinger ha noen verdi må de skje etter opptrukne retningslinjer med klare kriterier og det må finnes klare krav til hvem som kan foreta slike vurderinger.

Et klart trekk i utviklingen internasjonalt er at man legger vekt på å utnytte markedskreftene best mulig, og ikke å skape unødige hindringer. Tilsvarende holdninger viser den norske regjering, jf kapittel 4.2 foran. Myndighetenes rolle skal etter dette ivaretas ved å legge til rette de rammer er nødvendige, f eks mht regelverk og eventuelle ordninger for godkjenning (akkreditering o l), samt som praktisk aktør/bruker som næringsliv og privatpersoner må forholde seg til. Internasjonalt legges det generelt opp til frivillighet mht ordninger for å godkjenne virksomheter som vil drive som TTP'er. De ordninger arbeidsgruppen anbefaler, følger det vi oppfatter som den internasjonale trenden for rollefordelingen mellom marked og myndighetsutøvelse, og som vi oppfatter er de politiske signalene fra våre øverste myndigheter.

En interessant tilnærming finner vi i redegjørelsen til det danske Folketinget, "Sikker digital kommunikation", fra desember 1997. Det ble bl a uttalt: »Man kunne i prinsippet overlate til markedet selv å få etablert nøkkelsentre, men det er tale om et nytt marked med produkter av slik teknisk kompleksitet at det er svært vanskelig for den enkelte bruker å gjennomskue om man har fått et produkt med den nødvendige sikkerhet. Dessuten bør det gjennom lovgivning avklares i hvilket omfang nøkkelsentre er ansvarlige i forbindelse med feil og misbruk av digital signatur. Den danske regjering vil derfor ta initiativ til en regulering av nøkkelsentres virke i form av en autorisasjonsordning og en rekke minimumskrav til den digitale signaturs utforming, sikkerhetsnivå mv, som kan fremme tilbud av løsninger av "fornøden" kvalitet.»

Tilsvarende arbeid kan etter arbeidsgruppens mening med fordel vurderes og gjennomføres i Norge.

Det forslåtte tiltaket innebærer at det settes i gang et slikt arbeid for utforming av en frivillig autorisasjonsordning for tilbydere av TTP-tjenester i Norge. Målet må være å ivareta fellesbehov i samfunnet på tvers av ulike grupper, herunder nasjonal og internasjonal sikker elektronisk kommunikasjon og handel, og for å ivareta behovet for rettslig forutberegnelighet. Det bør tas utgangspunkt i direktivforslaget fra EU, men også andre lands lovgivning/utkast til lovgivning, herunder det danske. Erstatningsansvar ved feil, tilgjengelighetssvikt osv må klarlegges spesielt, dels ut fra gjeldende rett, dels ut fra en vurdering av nye regulatoriske behov på dette området, som eventuelt må ivaretas i form av ny lovgivning.

For å kvalitetsikre digitale signaturer og tiltrodde tredjeparter foreslås etablert enhetlige regler for vurdering av tillit som sikrer allmen aksept nasjonalt og internasjonalt.

Reglene bør utformes med bakgrunn i internasjonale standarder og innenfor rammen av etablerte ordninger for samsvarsvurdering. Ordninger som etableres bør ikke virke diskriminerende i forhold til EUs fire friheter.

Rettslig usikkerhet kan være en hindring for realiseringen av autentiseringstjenester. Slik usikkerhet kan antakelig reduseres ved hjelp av systemer for frivillig evaluering og forhåndsgodkjenning og/eller systemer for kontroll og oppfølging av slike tjenester, f eks i form av internkontroll og melding til tilsynsorgan. Muligheten for forhåndsgodkjenning vil sannsynligvis virke tillitsskapende i brukermarkedet og dette vil antakelige være en drivkraft for tjenestetilbyderne til å knytte seg til godkjennings- og/eller kontrollsystem. Samtidig kan det være grunnlag for å forhåndskvalifisere rettslige virkninger ved bruk av godkjente tjenester, f eks i forhold til oppfyllelse av formkrav i lovgivningen.

Et eget område for videre utredning og vurdering er kryssertifisering. (avtalegrunnlag, samsvar med anerkjente normer for ulike forhold, f eks sikkert utstyr (ITSEC/CC), sikker generell organisasjon (BS7799), sertifiserings-regler (certification policy), sertifiseringspraksis (certification practice statement), mv. Avtalegrunnlaget kan involvere både bilaterale og multilaterale avtaler. Også på dette området inneholder EU's direktivforslag innspill.

Næringslivet tilbyr og bruker i dag digitale signaturer og TTP'er uten regulering fra det offentlige. Skal regulering innføres må det offentlige også ta ansvar, herunder sørge for internasjonal aksept gjennom harmoniseringsarbeid og bilaterale avtaler.

Myndighetene må også ta ansvar for å koordinere egen elektronisk saksbehandling vis a vis næringslivet.

Som del av en godkjenningsordning for TTP-tjenesteytere bør det vurderes slike forhold som er nevnt i kapittel 8.2 foran.

Ikke forhåndsgodkjente tjenester må vurderes individuelt, ut fra de vanlige forholdene på et marked. Eksistensen av frivillige godkjenningsordninger bør ikke ha noen dempende eller uheldig virkning for den del av markedet som velger å operere utenfor ordningen, heller ikke for lukkede grupper mv.

Ansvarlig: Nærings- og handelsdepartementet

Mulige deltakere: Justervesenet/Norsk Akkreditering, Arbeids- og administrasjonsdepartementet, Justisdepartementet, Datatilsynet, Forsvarets overkommando/sikkerhetsstaben.

Tiltak 5:*Det etableres eller utpekes et offentlig eller privat organ som har ansvar for oppfølging og kontroll av TTP'er som på frivillig grunnlag er blitt godkjent.*

Det er naturlig at en frivillig godkjenningsordning må følges opp med en kontrollordning for å sikre tillit til at det tjenestenivå som er godkjent, opprettholder denne kvaliteten over tid. Det finnes ulike modeller for dette. Metodikken for internkontroll kan være hensiktsmessig også i denne sammenhengen. Modellen for kontroll må velges slik at tilliten til den frivillige godkjenningsordningen opprettholdes. Også for dette temaet vil det være nødvendig å vurdere de premissene og tilsvarende opplegg som måtte legges til grunn i EU og ellers, bl a av hensyn til aksept av sertifikater utstedt under denne ordningen.

Ansvarlig: Nærings- og handelsdepartementet

Mulige deltakere: Justervesenet/Norsk Akkreditering, Arbeids- og administrasjonsdepartementet, Justisdepartementet, Datatilsynet, Forsvarets overkommando/sikkerhetsstaben.

9.3.2 Forretningsvilkår

Tiltak 6:*Det bør vurderes å stille krav om offentliggjøring av forretningsvilkår og retningslinjer for drift av autentiseringstjenester.*

Både av hensyn til forbrukerne og myndighetenes mulighet for å observere utviklingen i markedet og vurdere nødvendige tiltak vil det være hensiktsmessig at forretningsvilkår og retningslinjer for driften er tilgjengelig. Det bør vurderes å stille minimumskrav til hvilke opplysninger som skal offentliggjøres. Det forhold at tjenestene er nye, og den betydning de antas å ville ha for utviklingen av det elektroniske informasjonsmarkedet tilsier at man holder et særlig oppsyn med tjenestene. På noe sikt kan det tenkes at man vil se fellestrekk i tjenesteleverandørenes vilkår og retningslinjer som kan nedfelles i lovgivningen og på den måten forenkle og øke oversiktligheten i markedet. Krav om offentliggjøring vil også ha betydning for brukernes mulighet til enkelt å orientere seg og gjøre seg opp en mening om tjenestenes innhold og troverdighet. Det må sikres at eventuelle nye regulatoriske tiltak ikke etablerer hindringer for videreføring av eksisterende løsninger og etablering av nye løsninger i lukkede brukergrupper.

Ansvarlig: Nærings- og handelsdepartementet

Mulige deltakere: Justervesenet/Norsk Akkreditering, Arbeids- og administrasjonsdepartementet, Justisdepartementet, Datatilsynet, Forsvarets overkommando/sikkerhetsstaben.

9.3.3 Ansvar og erstatning

***Tiltak 7:** Ansvars- og erstatningsforhold for ulike typer roller må utredes nærmere.*

Usikkerhet om mulig ansvar for misbruk av digitale signaturer, sertifikater med uriktig innhold og svikt i tilgjengeligheten til hele eller deler av tjenestene, antas å utgjøre en vesentlig hindring for utbredelsen av digital signatur systemer og TTP-tjenester, og det er viktig å få spørsmålene utredet nærmere. Dette er dels et spørsmål om å klarlegge gjeldende rett, dels et spørsmål om det er behov for å gripe inn med lovgivning eller på annen måte skape avklaring eller endring av den ellers bestående rettstilstand.

Man må se på henholdsvis: Sertifikatutsteders ansvar, ansvar overfor egne abonnenter, ansvar overfor tredjemann, ansvar ved manglende kontroll eller svikt ved godkjenning/lisensiering av TTP. Dessuten se på ansvarets omfang og mulige begrensninger.

Ansvarlig: Justisdepartementet

Mulige deltakere: Nærings- og handelsdepartementet, Arbeids- og administrasjonsdepartementet, Institutt for rettsinformatikk.

9.3.4 Behovet for robuste tjenester

Tiltak 8:*Iverksette sårbarhetsanalyser knyttet til etablering av autentiseringstjenester og økende elektronisk samhandel.*

Etterhvert som en stadig større andel av kommunikasjonen foregår elektronisk øker også avhengigheten av disse systemene, blant annet som følge av at manuelle rutiner og alternativer nedbygges og kravene til hastighet øker. En utvikling i retning av kommunikasjon i åpne nett vil samtidig øke avhengigheten av tilgang til autentiseringstjenester. Dersom en enkelt bruker av tjenestene opplever en system- eller sikkerhetssvikt vil dette vanligvis være et lokalt problem for den virksomhet eller etat det gjelder. Hvis derimot en bransje eller sektor av norsk næringsliv baserer sine autentiseringstjenester på sertifikater utstedt av en bestemt tjenesteleverandør, og det inntrer forhold som gjør at tilliten til nevnte tjenesteleverandør faktisk svekkes, vil dette kunne få store ringvirkninger dersom virksomhetenes sertifikater for en periode ikke anerkjennes av handelspartnerne. En slik situasjon kan etter omstendighetene få samfunnsøkonomisk betydning. Fokus bør omfatte helt eller delvis bortfall eller alvorlig forstyrrelse av tjenestene over en tidsperiode, med vurdering av mulige konsekvenser og mottiltak. Problemstillinger rundt langtidslagring av signerte dokumenter, samt tilgang til nødvendig nøkkelmateriale kan med fordel inkluderes i vurderingene. Utredningsarbeidet bør løpe parallelt med iverksetting av tjenestene.

Ansvarlig: Nærings- og handelsdepartementet

Mulige deltakere: Justisdepartementet, Direktoratet for sivilt beredskap, aktuelle tjenesteytere.

9.3.5 Identitetssertifikater »til folket»

Tiltak 9:*Det etableres en offentlig eller offentlig støttet autentiseringstjeneste for identitetssertifikater.*

Det må trekkes et grunnleggende skille mellom sertifikater som utelukkende eller i det vesentlige tjener til å identifisere enkeltpersoner («identitetssertifikater») og sertifikater som gir uttrykk for en rolle (f eks innehaver av en konto), fullmakt el («rollesertifikater»). Det anbefales at identitetssertifikater gjøres tilgjengelig fra det offentlige eller som en offentlig

støtte tjeneste som enhver vil ha praktisk og økonomisk mulighet for å få tilgang til. Slike identitetssertifikater antas å være gjenstand for færre endringer (f eks navnebytte el) enn rollesertifikater (som må endres ved bytte av arbeidsgiver ol). Sertifikatene kan blant annet benyttes i kommunikasjon med det offentlige (der avsenders identitet normalt er av betydning) og andre sertifikater kan etter omstendighetene bygge på eller være tilknyttet identitetssertifikatet. Likestilt med «sertifikat» i denne forbindelse vil være andre «elektroniske legitimasjonstegn» eller autentiseringsmekanismer som eventuelle nye tjenester vil føre med seg. Inntil videre antar vi imidlertid at tredjepartstjenester også vil være nødvendige for å tilby dette for bruk i åpne nettverk. Det er naturlig å se tiltaksforslaget i forhold til det som planlegges av Arbeids- og administrasjonsdepartementet om elektroniske id-kort, både i en nasjonal sammenheng, og for offentlig ansatte.

Ansvarlig: Arbeids- og administrasjonsdepartementet

Mulige deltakere: Kommunenes sentralforbund, Justisdepartementet.

9.4 Tiltak for å vinne konkret erfaring og kunnskap

9.4.1 Pilotforsøk på tvers av grenser

Tiltak 10:*Det gjennomføres minst ett pilotforsøk med en offentlig nøkkelinfrastruktur (PKI) for digitale signaturer som omfatter forvaltning, næringsliv og privatpersoner. Det læres av eksisterende prosjekter, og informasjon deles.*

Som vi har sett, kan sertifikat-basert infrastruktur for offentlig nøkkelhåndtering (også kalt PKI) sørge for de mekanismene som er nødvendige for å etablere tillitsforhold og tilgang til sikkerhetstjenester. Tillitsforholdene kan gå ut over eller på tvers av både organisatoriske og internasjonale grenser, til og med når partene er ukjente for hverandre. Mens de tekniske sidene ved en PKI begynner å bli noe mer modne og klare (men det står igjen en del), er det nok generelt slik at de korresponderende operasjonelle temaene ikke er like godt forstått eller utprøvd. Det er grenser for hvor langt en kan komme i teoretiske tilnærminger til de organisatoriske spørsmålene. Det må nå legges betydelig vekt på å vinne praktiske erfaringer i større grad enn hittil både teknisk og operasjonelt, og på å spre de erfaringer som gjøres slik at de kan deles. Det må legges vekt på å få ut maksimal læring og utprøving på generelt nivå i forbindelse med det som kan anses som nødvendig infrastruktur på tvers av de nevnte kjerneområdene.

Ut fra de relativt få erfaringene vi hittil har, er det grunn til å rope varsko i forhold til for små ressurser både menneskelig og budsjettmessig ved slike prosjekter. Vi minner om at Danmark nå er i gang med et antall pilotprosjekter for digitale signaturer, der det er satt av kr 15 millioner danske kroner til formålet. Arbeidsgruppen mener dette er et av de viktigste tiltakene å gjennomføre, sammen med tiltak nr 1. i stor grad kan og bør gjennomføres parallelt, og det anbefales å prioritere gjennomføring av dem ved å komme i gang så raskt som mulig, og å ha gjennomført hovedtiltakene

Ansvarlig: Nasjonalt informasjonsnettverk (NIN), Infrastruktur for nasjonalt informasjonsnettverk (ININ) (programmer under Norges forskningsråd)

Deltakere: Arbeids- og administrasjonsdepartementet, Kommunenes sentralforbund, Nærings- og handelsdepartmentet.

9.4.2 Informasjon, erfaringer og kunnskapsformidling

Tiltak 11: *Det bør på en aktiv måte utveksles erfaringer i forhold til offentlig nøkkel infrastrukturer gjennom eksisterende fora på relevante områder, også på tvers mellom forvaltning og næringsliv. Det bør vurderes å starte en norsk parallell til den svenske organisasjonen SEIS.*

Det er flere eksisterende fora som kan være aktuelle møteplasser. Vi peker på Norges forskningsråd - ININ-prosjektet, Fellesforum for elektronisk handel (NHD, Edipro, eforum.no, NHO, HSH), Rådet for IT-sikkerhet, KOSTRA mv. I tillegg vet vi at AADs prosjekt for rammeavtaler for digitale signaturer og TTP-tjenester vil etablere et leverandørforum.

Et forum som samlet offentlige og næringslivsinteresser i en uavhengig medlemsorganisasjon på linje med det svenske SEIS (Sikker Elektronisk Informasjon i Samfunnet) bør vurderes. Med medlemsavgift.

Ansvarlig: Arbeids- og administrasjonsdepartementet og Nærings- og handelsdepartementet

Deltakere: Næringslivet, Rådet for IT-sikkerhet, Fellesforum for e-handel, Statskonsult mv

Tiltak 12:*Det må gjennomføres tiltak for å fremme de generelle kunnskapene på området for digitale signaturer og tjenester fra tiltrodde tredjeparter.*

Dette er et område med stor betydning, og som antakelig relativt få forstår. Det er et betydelig misforhold mellom betydningen og kunnskapene. Selv om den enkelte bruker ikke behøver å forstå »innmaten» i teknikken, er det viktig å få spredd kunnskaper om hva teknikken kan gjøre for oss, og at den er/kan være til å stole på. Den usikkerheten som finnes i dag, skyldes blant annet manglende kunnskaper, som skyldes manglende informasjon på det riktige nivået. Arbeidsgruppen tror det er et klart behov for formidling av allmenkunnskap på området, av hensyn til alminnelig, sivil bruk i samfunnet av digitale signaturer og TTP'er. En ide kunne være å lage en »Aksjon digitale signaturer» for en periode, stille ressurser til rådighet, og drive god folkeopplysning.

Ansvarlig: Nærings- og handelsdepartementet

Deltakere: Rådet for IT-sikkerhet, Statskonsult, Statens informasjonstjeneste, Administrasjonsdepartementet, næringslivet,.

9.4.3 Internasjonal deltakelse. Lage norsk standard.

Tiltak 13:*Norge må prioritere deltakelse i internasjonale fora, herunder standardisering.*

Aktivitetsnivået internasjonalt er høyt. Det er mange problemstillinger som må finne sine løsninger internasjonalt. Et viktig område er å finne frem til et system for gjensidig godkjenning og tillit over landegrensene, både i forhold til sertifikater og TTP'er. De modeller og initiativer som det arbeides med i sentrale land og organisasjoner har stor verdi/betydning, også for Norge. Temaet er av internasjonal karakter, og løsninger må finnes på felles, internasjonal basis. Det er derfor om å gjøre å komme i posisjon til å vurdere nytten av og utnytte best mulig det arbeidet som skjer ute. Som et minimum bør vi løpende sørge for å

følge så godt med i det som skjer at vi er ajour til enhver tid (ikke bare skippertak hver gang det nedsettes en arbeidsgruppe).

Der sentrale internasjonale organisasjoner er aktive, må Norge sørge for å ha aktiv deltakelse. Dette er den beste måten å tilføre landet nødvendige kunnskaper og kompetanse på, samt en nødvendig måte hvis en vil påvirke løsninger, som i sin tur vil ha betydning nasjonalt. Så vidt arbeidsgruppen vet, deltar Norge i EU/EØS- og i OECD-sammenhenger på en aktiv måte, også i forhold til digital signatur og TTP-spørsmål. Deltakelse i UNCITRALs arbeider har vi derimot ikke. Dette må etter vår mening vurderes som en meget viktig arena å delta på. Norge må også sørge for å være ajour til enhver tid med kunnskaper om andre lands utvikling og erfaringer.

Aktiv erfaringsinnhenting, deltakelse i utlandet når det er viktig/relevant, besøk hos land som har gode eksempler/har kommet langt, og som det er mye å lære av, analysere og spre informasjon om eksisterende erfaringer. Betydningen av dette bør ikke undervurderes.

Det bør gis støtte til aktiv norsk deltakelse i de standardiseringssammenhengene som er viktigst. Med den betydning standarder har på sikkerhetsområdet som byggesteiner for »alt annet», er det svært viktig at vi fra norsk side holder oss så godt orientert om denne utviklingen som mulig, og deltar aktivt. Dette gjelder både »gamle» og nye standardiseringsgrupper, som f eks de knyttet til Internett. Det pågår løpende standardiseringsarbeid i ISO og i Internet Engineering Task Force (IETF) som har direkte relevans til dette arbeidet og som bør følges opp fra norsk side. Norsk Teknologistandardisering har etablert en nasjonal referansekomite K171 Informasjonssikkerhet for standardiseringsarbeid i ISO/IEC JTC/SC27. Komiteen bør utvides til også å dekke det pågående standardiseringarbeidet i IETF. Norsk Teknologistandardisering disponerer en bevilgning til å støtte reiser hvor det gis 50 % reisestøtte. Det bør øremerkes midler til egen prosjektstøttebevilgning som i tillegg til normative anbefalinger også vil omfatte utarbeidelse av norske høringssvar og mulighet til å påta seg editor-oppgaver i standardiseringsarbeidet.

Ansvarlig: Nærings- og handelsdepartementet

Deltakere: Justisdepartementet, Norsk teknologistandardisering, Samferdselsdepartementet, Post- og teletilsynet, Statskonsult, næringsliv, universitet.

Tiltak 14:*Det bør iverksettes et arbeid for å oversette og tilpasse til norske forhold den britiske standarden for sikkerhetssertifisering av organisasjoner (BS 7799) og settes i gang en prosess for å gjøre den til norsk standard.*

0 Generelt bør standarder velges, tilpasses og profileres ut fra norske behov og forhold, uten å gå på tvers av innholdet i standarden eller det internasjonale aspektet. Arbeidsgruppen foreslår konkret at dette bør gjøres med den britiske standarden BS 7799, A Code of Practice for Information Security Management. Dette er en standard som stiller krav og gir veiledning i forhold til sikker informasjonsbehandling i en organisasjon. Den er utarbeidet av britisk industri, i samarbeid med det britiske industridepartementet og gjort til britisk standard. Den er lagt til grunn for sertifiseringordninger rettet mot organisasjoner, i UK, Holland og Sverige (sertifisering da brukt i en annen betydning, som tidligere omtalt). Den er foreslått lagt til grunn i Norge, på området for sikkerhetssertifisering av organisasjoner. Arbeidsgruppen tror at den vil være aktuell også for vurderingen av den generelle organisasjonsmessige

sikkerheten hos TTP'er, dvs de deler av vurderingene som ikke er spesielt rettet inn mot det å utstede sertifikater som bekrefter tilhørighet mellom en identitet og et offentlig sertifikat.

Ansvarlig: Norsk Teknologistandardisering

Deltakere: Nærings- og handelsdepartementet, Justervesenet/Norsk Akkreditering, Datatilsynet, Forsvarets overkommando/sikkerhetsstaben.

9.5 Kommentar og konklusjon

De tiltakene som foreslås er av grunnleggende karakter. Vi trenger å gjennomføre slike tiltak i Norge, akkurat som man trenger å gjøre tilsvarende arbeider i andre land, både i Europa og i OECDs medlemsland verden rundt. Forslagene har slik sett en »gjenklang» internasjonalt; vi er ikke alene om å se behov for slike tiltak. I en viss grad forutsettes det både i arbeider i regi av EU, OECD og UNCITRAL at mye av det som foreslås må gjøres av den enkelte nasjon, dels av hensyn til hver nasjon, men ikke minst de internasjonale sidene ved utviklingen, og hensynet til å ha kvalifiserte grunnlag for tillit og gjensidig aksept over landegrensene som baserer seg i størst mulig grad på fellestenkning. Så vidt vi kan forstå fanger våre forslag til tiltak opp de mest aktuelle aksjonene som er nødvendige å ta av hensyn til for at Norge skal følge med i den internasjonale utviklingen på dette området. Det er ikke slik at tiltaksforslagene er særnorske, - tvert om bygger de på tilsvarende tankegang som vi finner internasjonalt. Forslagene legger ikke til grunn at vi skal finne på særløsninger i Norge, men legge internasjonale normer, kriterier og standarder til grunn, og helst delta aktivt i utviklingen av disse.

Tiltakene legger helt klart til grunn at det er næringslivet og markedet som er hovedaktører og må styre den teknologiske og markedsmessige utviklingen, mens myndighetene kan gi bidrag ved å være en god bruker, og ved på enkelte utvalgte områder å legge til rette for særlig de deler av markedet som har behov for noe høyere sikkerhetsnivå enn det ordinære og generelt lave. Et viktig premiss er at markedet ikke skal hemmes av myndighetenes tiltak, - *frivillighetsprinsippet* er sterkt understreket, for eksempel i forhold til godkjenningsordning for TTP'er. Dessuten at regulerte og uregulerte løsninger må kunne leve side om side uten å forstyrre hverandre. Det er grunn til å tro at det fortsatt vil være en sterk og dynamisk utvikling videre på den delen av markedet som ikke har behov for slik sikkerhet som denne rapporten handler om. Dette markedet er i øyeblikket meget stort, og ganske sikkert voksende. Tiltakene fra arbeidsgruppen tar ikke sikte på å påvirke eller forstyrre denne utviklingen. Men arbeidsgruppen legger til grunn at det er sterke og klart uttrykte behov både nasjonalt og internasjonalt for at myndigheter legger til rette på noen relativt få, men viktige områder, for den delen av markedet som trenger litt »ekstra» tillit og sikkerhet. Dette handler om premisser for en trygg og effektiv overgang fra papirbasert til elektronisk kommunikasjon, for den mer seriøse delen av kommunikasjonsbehovet.

Det anbefales sterkt at tiltakene som er foreslått i størst mulig grad gjennomføres parallelt der de ikke er avhengige av å komme i rekkefølge. Tiltakene for rettslig aksept av elektroniske dokumenter og signaturer vil for eksempel ikke hindre arbeid med å vinne konkret erfaring med teknologien gjennom tverrgående pilotprosjekter. På hvert del-område er det nødvendigvis ikke uoversiktlig om lover og regler er til hinder eller ikke. Det er på ingen måte nødvendig å vente med å ta teknologien i bruk for å vinne erfaringer. På store virkeområder er det heller ingen rettslige problemer. Vi har avtalefrihet, fri bevisførsel og fri bevisvurdering for domstolene, hvis det skulle være aktuelt. Dette gjelder også for digitale signaturer! Likevel

mener vi det er nødvendig med de avklaringer og rammebetingelser som foreslås, for at overgangen fra papirbasert til elektronisk kommunikasjon skal bli effektiv og trygg, for både forvaltning, næringsliv og folk flest i egenskap av borgere og forbrukere. Vi kan også påberope oss at dette er det i all hovedsak enighet om internasjonalt, - nå er det om å gjøre å gjennomføre de nødvendige tiltakene.

Konklusjonen*er at tiltakene som er foreslått bør settes i gang og gjennomføres innenfor en tidsramme på to år, altså innen utløpet av år 2000.*

Tiltakene kan og bør i stor grad gjennomføres parallelt. Dette gjelder arbeidet med regelverket og rettslig aksept/likestilling (tiltakene 1, 2 og 3), det gjelder tiltakene for å legge til rette og å gi rammebetingelser for bl a frivillig godkjenningsordning for TTP'er (tiltakene 4 - 9), og det gjelder ikke minst arbeidet med å vinne erfaring gjennom pilotforsøk som involverer borgere, næringsliv og forvaltning på tvers, aktiv deling av den informasjonen og de erfaringene som finnes til gjensidig nytte, høyningen av aktivitetsnivået internasjonalt og i forhold til standardisering, samt valg og tilpasning av standarder for norske forhold (tiltakene 10 - 14). Noen av oppgavene er av løpende karakter og bør følgelig ikke begrenses av en slik tidsramme. Alle de tre hovedområdene for innsats anses viktige å prioritere. Arbeidsgruppen har imidlertid vurdert rettslig aksept og konkrete pilotforsøk som de viktigste.

Vedlegg 1: Ordliste, forkortelser og referanser

Ordliste

Autentisering Prosessen med å bekrefte en oppgitt identitet. (DSD)

Autentiseringstjeneste sikrer at en enhet (person/prosess) virkelig er den som en gir seg ut for å være

Adgangskontroll Kontroller for å motvirke uautorisert adgang til systemer eller informasjon.

Autorisering Tilordning av rettigheter til aktører en person har i tilknytning til et i IT-system

Certification Authority (CA) Se sertifiseringsautoritet.

Dataintegritet Det at informasjon ikke blir endret eller ødelagt på en uautorisert måte. (DSD)

Digital signatur En kryptografisk sjekksum generert ved hjelp av en privat krypteringsnøkkel (offentlig nøkkel kryptografi).

Dokument En informasjonsenhet som kan utveksles mellom aktører.

Endesystem Den enhet som foretar signering og verifisering av signatur.

Identitetssertifikat Sertifikat som kopler en identitet til en offentlig nøkkel på en autorisert måte gjennom en signatur fra en sertifiseringsautoritet (elektronisk legitimasjon).

Ikke-benekting Den egenskap at mottakeren av et dokument har sikkerhet for (kan sannsynliggjøre) at den angitte avsender ikke senere kan nekte å ha sendt dokumentet, samt at mottakeren ikke senere kan nekte for å ha mottatt.

Integritet Det forhold at informasjon ikke er endret under lagring eller transport.

Konfidensialitet Den sikkerhetstjenesten som skal sikre at informasjon ikke blir gjort tilgjengelig for uvedkommende.

Kryptering Konfidensialitetsbeskyttelse ved kryptografiske metoder. Brukes primært for å skjule informasjonsinnhold ved overføring over nettverk.

Non-repudiation Se ikke-benekting.

Nøkkeldata Nøkkeldata betyr i denne sammenhengen selve nøklene, samt tilhørende parametre som er nødvendige for å opprette sikker kommunikasjon mellom to eller flere parter.

Konfidensialitet Konfidensialitet innebærer at informasjon ikke er tilgjengelig for uautoriserte personer eller ikke-godkjente systemer. (DSD)

Kryssertifisering Kryssertifisering er en mekanisme som innebærer at to CA'er tilhørende forskjellige PKI-domener gir hverandre sertifikater for å stadfeste et tillitsforhold. Denne fremgangsmåten skiller seg fra den strengt hierarkiske modellen der tillit flyter nedover langs fast definerte "stier" i et hierarki. Det er ikke snakk om kryssertifisering innenfor et PKI-domene.

Melding En datamengde som kommuniseres mellom aktører, f. eks. innhold i en epost. Kan bestå av flere dokumenter.

Navn En unik identifikator som identifiserer en aktør.

PIN-kode Passord som brukes for autentisering mot et smartkort. Begrepet PIN-kode brukes for å unngå forveksling med passord for innlogging på datasystemer.

Public Key Infrastructure (PKI) En PKI er en samling av infrastruktur (datasystemer, distribusjonssystemer og rutiner) som eksisterer med det formål å generere, revokere (tilbakekalle), sende ut, og på andre måter håndtere offentlige nøkkelsertifikater.

Revokeringsliste På engelsk: Certificate Revocation List - CRL. Se tilbakekallingsliste.

Rollesertifikat Sertifikat som kopler en rettighet / rolle til en offentlig nøkkel på en autorisert måte gjennom en signatur fra en sertifiseringsautoritet. Rolle angis som navneattributter eller på annen måte.

Sekvensintegritet å sikre at en meldingsutveksling har foregått i riktig rekkefølge

Sertifikat En kopling mellom en offentlig nøkkel og en identitet (eller en rettighet / rolle), signert av en sertifiseringsautoritet.

Sertifikatrevokering/tilbakekalling Ugyldiggjøring av et utstedt sertifikat før utløpet av sertifikatets gyldighetsperiode.

Sertifisering Ved en sertifisering vil brukerens identitet og andre data knyttes til brukerens offentlige nøkkel, ved hjelp av CA'ens digitale signatur. Den offentlige nøkkelen, brukeridentiteten og signaturen er inneholdt i brukerens konfidensialitets-sertifikat.

Sertifiseringsautoritet (SA) En sertifiseringsautoritet er en betrodd instans som går god for identiteten til registrerte brukere. Dette stadfestes ved at CA'en utsteder et sertifikat til brukeren.

Smartkort Plastkort (typisk bankkortstørrelse) som inneholder en eller flere mikroprosessorer, og som kan kommunisere med datamskiner o.l. gjennom en smartkortleser. Et smartkort kan lagre informasjon på en sikker måte, og kan inneholde funksjoner for kryptografi.

Smartkortleser Utstyr koplet til en datamaskin for kommunikasjon mellom maskinen og smartkort.

Sporbarhet Sikrer at viktige hendelser i systemet kan spores til ansvarlige personer eller prosesser

Tilbakekalling Prosedyrer for å erklære et sertifikat ugyldig før utløpet av gyldighetsperioden.

Tilbakekallingsliste Liste som inneholder oppdaterte oversikter over sertifikater som av en eller annen grunn er kalt tilbake slik at de ikke lenger er gyldige. Disse oversiktene må være tilgjengelige for brukerne til enhver tid. Et sertifikat kan være erklært ugyldig f. eks. fordi tilsvarende private nøkkel er kompromittert. Tilbakekallingslister er signert av samme sertifiseringsautoritet som utstedte sertifikatene som er tilbakekalt. Se revokeringsliste.

Tilgjengelighet Sikre at informasjon og resursser er tilgjengelig for brukere som har rettmessige adgang til informasjon

Tiltrodd Tredjepart (TTP) En organisatorisk/teknisk enhet som av andre parter er betrodd å ivareta sikkerhetsrelaterte funksjoner og oppgaver på deres vegne.

X.509 Del av X.500 serien. Definerer bl.a. autentiseringsmetoder basert på offentlig nøkkel kryptografi, format på sertifikat for å knytte offentlig nøkkel til en identitet, og format på tilbakekallingslister (CRL). Aktuelle versjoner er sertifikat versjon 3 (X.509v3 sertifikat) og CRL versjon 2 (CRLv2).

Forkortelser

BS7799 En britisk standard: A Code of Practice for Information Security Management

CA Certification Authority

CC Common Criteria (CC) erstatter regionale kriterier med felles globale kriterier, som er på vei til å bli en ISO standard og åpner for å definere spesifikke sikkerhetsprofiler for ulike produkter og systemer.

CPS Certificate Practice Statement

CP Certification Policy

DSD Datasikkerhetsdirektivet

DSS Digital Signature Standard benytter andre matematiske prinsipper enn RSA og er inkludert i standarder fra ISO/IEC, ANSI og IEEE.

FO/S Forsvarets overkommando/Sikkerhetsstaben

EDI Electronic Data Interchange - elektronisk utveksling av strukturerte data mellom heterogene datasystemer

EDIFACT EDI for administration, commerce and transport; internasjonal standard for EDI som innbefatter syntaks, dataelementer og meldinger

EDNA Elektronisk dokumentutvekslingssystem i norsk administrasjon for å ivareta krav til signatur, konfidensialitet, utveksling og arkivering.

ELEKTRA Skattedirektoratets prosjekt som skal styrke skatteetatens service overfor næringslivet

GRLD Skattedirektoratets system for grunnlagsdata og oppgaver fra tredjemann

ININ en prosjektgruppering for å ta seg av felles infrastrukturspørsmål og kvartalsvise fagsamlinger i Nasjonalt Informasjons Nettverk (NIN) i regi av Norges forskningsråd

IPSEC et sikkerhetstillegg til TCP/IP-standarden spesifisert av Internet Engineering Task Force (IETF)

ITSEC Et sett av europeiske kriterier for evaluering og sertifisering av sikkerhet i IT-produkter og systemer, som bl a kan benyttes for produkter for digitale signaturer.

LDAP Lightweight Directory Access Protocol

NOARK-4 Riksarkivets nye standard for arkivering, på høring høsten 1998.

NPSS Nordic Post Security Services

K171 nasjonal referansegruppe for informasjonssikkerhet i Norsk Teknologistandardisering

KOSTRA Kommunal- og regionaldepartementets prosjekt for kommune-stat rapportering av regnskapsopplysninger

MVA3 Skattedirektoratets forvaltningssystem for merverdiavgiften

NIN Nasjonalt informasjonsnettverk i regi av Norges forskningsråd, innrettet for igangsetting av et antall pilotprosjekter og demonstratorer for å oppnå økt elektronisk samhandling.

PSA Skattedirektoratets system for forhåndsutfylt selvangivelse

SHA Secure Hash Algorithm en komponent for å komprimere en melding før selve signeringen

SLN Skattedirektoratets system for likning av næringsdrivende

PGP Pretty Good Privacy, programvarepakke for kryptering og signering av elektronisk post og datafiler.

PKI Public Key Infrastructure

RIPEMD-160 en komponent for å komprimere en melding før selve signeringen

RSA offentlig nøkkelkryptografi for signering, basert på en hemmelig signeringsnøkkel og en offentlig verifiseringsnøkkel og oppkalt etter opphavsmennene (Rivest, Shamir, Adleman), metoden (fra 1978) har vært en de facto standard på området.

SA Sertifiserings Autoritet

SEIS Secured Electronic Information in Society er en svensk ideell organisasjon som arbeider for sikker digital kommunikasjon i åpne nett ved hjelp av åpne nøkkelsystem, sertifikat og aktive kort

SET Secure Electronic Transaction

SSL Secure Sockets Layer

TTP Tiltrodd Tredje Part/Trusted Third Party

UNCITRAL United Nations Commision on International Trade Law

UPU Universal Post Union

VPN Virtual Private Networks

Referanser

Referansene gitt nedenfor er ikke systematisk ordnet. Selv om listen følgelig ikke ser særlig elegant ut, håper vi den likevel kan være til nytte. Noen er uten og andre er med web-adresser. Webadressene er sjekket og funnet i orden i skrivende stund (nov 98).

- Meldingssikkerhet - Tiltrodde tredjeparter og digitale signaturer, Norsk EDIPRO, 07.12.1994.

- Digitale signaturer og Tiltrodde tredjeparter, Norsk EDIPRO, Desember 1996.

- X.509:1997 INFORMATION TECHNOLOGY -OPEN SYSTEMS INTERCONNECTION - THE DIRECTORY: AUTHENTICATION FRAMEWORK Recommendation X.509 version 3, International Telecommunication Union (ITU)

- Instruks for behandling av dokumenter som av sikkerhetsmessige grunner må beskyttes (Sikkerhetsinstruksen), fellesblankett X-0076

- Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i Sikkerhetsinstruksen (Beskyttelsesinstruksen), fellesblankett X-0076

- Direktiv for sikring av ADB-system og datanett gradert etter sikkerhetsinstruksen eller beskyttelsesinstruksen, Forsvarets overkommando 1997

- Sluttrapport fra utvalg for vurdering av behov for kryptopolitikk, Fo/S 1997-11-10 for Rådet for IT-sikkerhet i Nærings- og handelsdepartementet

- Norsk Arkivstandard versjon 4, sendt på høring 1998-09-15, endelig versjon ventes i januar 1999, Riksarkivet http://www.riksarkivet.no/nyheter.html

- Statens Generelle Kravspesifikasjon for edb-støttet saksbehandling og ledelse, SGK 1 til 7, kravspesifikasjoner utgitt av Statskonsult 1991-1996

- Samordnet løsning for elektronisk overlevering av opplysninger fra næringslivet til Skattedirektoratet, Brønnøysundregistrene og Statistisk Sentralbyrå, versjon 2.0, 28.mai 1997

- Den norske IT-veien Bit for Bit, Rapport fra Statsekretærutvalget for IT, Samferdselsdepartementet, januar 1996

- Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering, Statskonsult rapport 1998:13, basert på en kartleggingsstudie ved innføring av elektronisk saksbehandling i forvaltningen, Statskonsult notat 1997:3

- Elektronisk post i statsforvaltningen, utredning fra arbeidsgruppe avgitt 9.juni 1995, Administrasjonsdepartementet

- Arbeids- og administrasjonsdepartementet og Kommunenes Sentralforbund samarbeider om rammeavtaler med standardiserende effekt i offentlig forvaltning, herunder rammeavtaler for digitale signaturer mv. Se kravspesifikasjon for digitale signaturer og annet relevant materiale på websiden: http://forvaltningsnett.dep.no/.

- Proposal for a European Parliament and council directive on a common framework for Electronic Signature, 13.05.98

- Recommendation of the Council concerning Guidelines for Cryptographic Policy, 27 March 1997

- Outline and preliminary draft: Inventory of Approaches to Authentication and Certification in a Global Networked Society, 24 June 1998

- EDITT - EDI Trusted Third Parties Workshop. Rainer A. Rueppel, Revocation and Revocation Certificates, Barcelona, TEDIS, Feb. 1995

- FAST, «First Attempt to Secure Trade», TEDIS Phase II, T1.1 «Credentials, Attributes and Certificates», TEDIS April 1994.

- Recommendation X.208, Specification of abstract syntax notation one (ASN.1), CCITT (ITU-T)Genova 1989.

- CA-Policies i praktiken, TeleTrusT Sverige, 1996

- Norsk EDIPRO standard utvekslingsavtale versjon 2, august 1995 (engelsk 1996)

- Rammebetingelser for elektronisk handel. Problemområder og problemstillinger knyttet til lov og regelverk for elektronisk handel. Nærings- og handelsdepartementet, november 1998. Se dokumentet og delta i høringen frem til 15. januar 99 på følgende webside: http://www.dep.no/nhd/publ/1998/ehandel/html

- UNCITRAL (United Nations Commission on International Trade Law)

http://www.un.or.at/uncitral/en-index.htm

Inneholder bl a Model Law on Electronic Commerce, Draft Uniform Rules on Electronic Signatures, og rapporter fra sesjonene som holdes regelmessig av The Working Group on Electronic Commerce, der bl a ulike versjoner av Draft Uniform Rules løpende diskuteres.

- EU

http://www.ispo.cec.be/

EC Information Society Project Office, - omfattende lenker til relevante dokumenter/arbeider/prosjekter.

http://www.ispo.cec.be/eif/policy/97503toc.html

Communication from the Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions Ensuring Security and Trust in Electronic Communication, DG XIII, COM (97) 503. Det er her det varsles at et direktiv er foreslått i 1998.

http://www.ispo.cec.be/ecommerce/

EU kommisjonen. Omfattende oversikt over temaet elektronisk handel i et europeisk perspektiv. Pekere til mye, bl.a. http://www.ispo.cec.be/ecommerce/issues.htm (generell oversikt over ulike temaer), og http://www.ispo.cec.be/ecommerce/securit1.htm (oversikt innenfor temaet "security aspects") og http://www.ispo.cec.be/ecommerce/legal.htm ("legal aspects")

http://www2.echo.lu/legal/en/labhome.html

http://www2.echo.lu/legal/en/ecommerc/digsig.html

Begge de sistnevnte adressene er: European Commission Legal Advisory Board (LAB), Homepage, for henholdsvis E-commerce/Digital signatures and encryption

- EUs INFOSEC-program

http://www.cordis.lu/infosec/home.html

Inneholder oversikt over aktivitetene i dette programmet de siste 5 årene.

http://www.cordis.lu/infosec/src/study2.htm

Inneholder bl a Legal and Regulatory Issues concerning the TTPs and Digital Signatures - Final Report (European Trusted Services Infrastructure - ETS), June 1997. Dette står ikke for DG XIIIs syn, men er et forberedende arbeid for et EU-direktiv på området.

- Annen standardisering

Ulike standardiseringsinitiativ innen ISO, ETSI, EDIFACT, etc: http://www.r3.ch/news

Internet Engineering Task Force (IETF) arbeider http://ietf.org/ids.by.wg/pkix.html (oversikt), samt draft standarder på ftp://ftp.ietf.org/internet-drafts/draft-ietf-pkix-ipki3cmp-07.txt (to siste ledd varierer)

Cordis: A study for the European Commision on standardisation issues for the European Trusted Services, Andrew Colleran, juni 1997 establishing a framework for trust http://www.cordis.lu/infosec/src/study4.htm

European Committee for Banking Standards: TR 402 V.1 Certification Authorities, des.97 med behandling av ulike sertifikat-format (x.509, iso11166, EDIFACT,....) http://www.ecbs.org/download.html (look for the headline SECURITY and there for TR 402)

NIST Special Publication 800-15, Minimum Interoperability Specification for PKI Components (MISPC), version 1 sept 1997, US Dep. Of Commerce, Technology Administration, National Institute of Standards and Technology 1997-09, URL is http://csrc.nist.gov/pki/mispc/welcome.html

Links to European legislation (UK policy paper on trusted third parties and the German Digital Signature Law) and a decent list of links to digital signature legislation in the United States of America at http://www.qmw.ac.uk/~tl6345/

- Danmark

http://www.fsk.dk/fsk/div/udk-digi-sign/

Det danske lovforslaget om digitale signaturer som ble sendt på høring våren 1998.

- Sverige

http://www.seis.se/

Den svenske organisasjonen Sikkerhet i informasjonssamfunnet (SEIS) har utarbeidet en rekke spesifikasjoner for å implementere digital signatur i forbindelse med smartkort, bl.a. elektronisk ID applikasjon (SEIS S1 og svensk standard SS614330), elektronisk ID sertifikat (SEIS S3 og svensk standard SS 614331), elektronisk ID kort - svensk profil (SEIS S4 og svensk standard SS 614332).

- Finland

http://www.vaestorekisterikeskus.fi/

Den finske organisasjonen for elektronisk ID med tilsvarende spesifikasjoner (jfr. SEIS over); FINEID S1, FINEID S3, FINEID S4. I tillegg er det utarbeidet en katalogspesifikasjon FINEID-S5 og et FINEID pilotkort med tilhørende sertifikat-spesifikasjon..

- Generelle henvisningssider

http://www.iki.fi/avs/eu-crypto.html

Inneholder omfattende oversikt over europeiske forhold.

http://www.magnet.state.ma.us/itd/legal/pki.htm

Denne kaller seg The PKI Page, og fungerer som en informasjonsbank for folk som vil bruke "public key infrastructure as tool for securing net-based communications and transactions". Folk oppfordres også til å sende inn egen informasjon. De ser ut til å ha mye amerikansk og kanadisk stoff, men lite fra resten av verden.

- Storbritannia

DTI

http://www.dti.gov.uk/pubs/index.html

Departement of Trade and Industry (DTI) presenterer her et "Public Consultation Paper on Detailed Proposals for Legislation", March 1997 på temaet: Licensing of Trusted Third Parties for the Provision of Encryption Services, samt senere oppfølgingsdokumenter.

UK-ITSEC scheme:

http://www.itsec.gov.uk

omfatter også en oppdatert, online versjon av listen med sertifiserte produkter, og dokumenter om evalueringer som er gjennomført + noen pekere, tror jeg. Litt annet tema enn elektroniske/digitale signaturer. Denne ordningen (og liknende i andre land) kan evt brukes til å sertifisere relevante produkter på signatur-området.

- USA

http://www.abanet.org/scitech/ec/isc/dsg.html

(American Bar Assosiation)

Her ligger bl a en "Digital Signature Guidelines" med undertittel: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce (aug.96)

http://www.itl.nist.gov/div893/

NISTs Computer Security Division, med oversikt over programmer for "protection of uclassified automated information systems", som omfatter krypto, avansert autentiseringsteknologi, offentlig nøkkel infrastruktur, krypto nøkkel "recovery" osv

http://www.ss.ca.gov/digsig/finalregs.htm

Final Draft of Proposed Digital Signature Regulations in California. Publisert i november 1997. Har en annen tilnærming enn f eks Utahs lovgivning om digital signatur.

http://www.jya.com/crypto.htm

Daglig oppdatering av materiale om kryptografi, digitale signaturer, krypto politikk og mer. Det er på Cryptome du først kan lese om den nye amerikanske krypto politikken.

- Canada

http://www.cse-cst.gc.ca/cse/english/gov.html

Communications Security Establishment, som bl a har The Government of Canada Public Key Infrastructure (PKI).

- OECD

http://www.oecd.org/dsti/sti/it/index.htm

Nyheter og oversikt. Inneholder mye, deriblant materiale fra Ottawa-konferansen i oktober 1998 om elektronisk handel.

Vedlegg 2: Behov uttrykt gjennom forsøk og initiativer i norge

Nedenfor følger en noe fyldigere gjennomgang av det som ble omtalt i kapittel 5.3. Gjennomgangen bærer preg av at den er satt sammen fra mange bidragsytere, og den er ikke tekstlig bearbeidet for å få frem kun en måte å skrive/beskrive på. De enkelte områdene er nok også fremstilt på varierende detaljnivåer. Vi synes likevel at teksten gir en oversikt som er verdifull. Den viser at det er mange aktører i Norge som på ulike måter føler et sterkt behov for sikker elektronisk kommunikasjon.

Handel

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 oss 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 policy-uttalelsen fra Kommisjonen der bruken av kryptering og digitale signaturer i

forbindelse med elektronisk handel er et sentralt tema. Se til orientering websiden til EU, med oversikt over området 47. Dette er en innfallsport til en nærmest overveldende mengde informasjon om ulike initiativer både i EU og i resten av verden, som fortløpende ajourføres.

I Norge har Statssekretærutvalget for IT satt problemstillingen på dagsorden høsten 1998. Et fellesforum 48 for elektronisk handel er etablert av Nærings- og handelsdepartementet i samarbeid med eforum.no, Norsk EDIPRO, Næringslivets Hovedorganisasjon og Handelens og Servicenæringenes Hovedorganisasjon. Etableringen kommer som en oppfølging av Regjeringens Næringsrettede IT-plan. Forumet er en arena for dialog og diskusjon i forhold til myndighetenes arbeid med rammebetingelsene for elektronisk handel

Nærings- og handelsdepartementet har det overordnede ansvar for å stimulere til og tilrettelegge for elektronisk handel i Norge, men privat må sektor lede utviklingen. I Næringsrettet IT-plan 1998-2001 er elektronisk handel et sentralt område. Et viktig tiltak som skal gjennomføres, er å vurdere nødvendige tilpasninger i lov- og regelverk, inkludert løsninger for digitale signaturer og tiltrodde tredjeparter. Et grunnlagsdokument 49 er utarbeidet som ledd i oppfølgingen av dette tiltaket. Statssekretærutvalget for IT har ved en rekke anledninger drøftet ulike sider ved e-handel, og Regjeringen har slått fast prinsippene, hovedinnretningen og prioriteringene for arbeidet med rammebetingelser for elektronisk handel.

I denne rapportens sammenheng er det tatt kontakt med ulike bransjer innen handelen og det er tatt utgangspunkt i utveksling av prisinformasjon, ordre og faktura. Forskjellene vedrørende behov er ikke store. Store pågående prosjekt er gjerne innen spesielle bransjer og dreier seg ikke om åpen handel, der alle skal kunne handle med alle. To eksempler er:

- handel med legemidler - en lukket og oversiktlig brukergruppe bestående av medisingrossister og apotek som ennå ikke har tenkt gjennom krav i et åpent nettverk
- bygg og anlegg - der det er vanlig med bruk av avtaler som regulerer forhold mellom partene om priser, rabatter, leveringstidspunkt med mer, man vet med andre ord hvem man handler med.

I en åpen handel hvor alle skal kunne handle med alle, vil man hverken ha lukkede bruker-grupper eller forhåndsinngåtte avtaler mellom partene.

Det er enighet om at når det gjelder rene handelsmeldinger er det normalt ikke krav til konfidensialitet, men kravet kan være tilstede hvis overføringen dreier seg om pristilbud. Innen bygg og anlegg eksisterer spesielle handelsavtaler for elektronisk handel, som regulerer priser, rabatter, leveringstidspunkt mm. Den informasjon som handelspartene utveksler er ikke uten videre åpent for andre. Det betyr at handelsmeldinger utvekslet mellom faste handelspartnere i mange tilfeller anses som konfidensielle, spesielt der det ligger avtaler bak som er forhandlet frem mellom dem. Hvis forhandling om avtaler foregår elektronisk vil dette selvfølgelig være konfidensielt.

Det stilles ikke krav om signatur på handelsmeldinger. Det er ikke stilt klare krav om ikke-benekting, men det er normalt at det kreves logging av utvekslinger. For at elektronisk overførte handelsdokumenter skal kunne brukes i stedet for papirdokumenter, har regnskaps-lovgivningen spesielle krav til lagring - samtidig som det kreves juridisk logg.

- Behov: Sekvensintegritet, integritet, ikke-benektet mottak, autentisert avsender, rett mottaker og i visse tilfeller konfidensialitet

Betaling

Banktjenester er i stor grad et spørsmål om tillit. For betalingsformidling og andre banktjenester vil behovene for sikkerhetstjenester i et produkt være avhengig av forhold til de verdier som skal beskyttes, og de risiki man ser for forskjellige typer angrep.

For betalinger er det naturlig å skille mellom to grupper av sikkerhetsbehov:
a) Behov for sikkerhetstjenester og mekanismer for å få tilgang til konto eller betalingsinstrument.
b) Behov for sikring av betalingstransaksjonene.

I mange betalingssystemer er det bygget inn sikkerhetsmekanismer som gjør at innehaver av kort eller konto må identifisere seg slik at uautorisert aksess ikke forekommer. Data som autentiserer en kontoinnehaver må enten beskyttes mot innsyn eller være av en slik art at de ikke er forutsigbare for en eventuell angriper.

Betalingstransaksjonene må også beskyttes. Her er det viktig å sikre seg mot manipulering av f. eks. transaksjonsbeløp og kort / kontonummer. Det er også viktig å legge inn sikkerhetstjenester som gjør at fjerning av transaksjoner eller innsetting av falske transaksjoner vil bli oppdaget. Det kan også være behov for å verifisere at en transaksjon eller en forespørsel kommer fra en kjent og godkjent kommunikasjonspartner (autentisering av opphav). Ved sending av forespørsler før en transaksjon kan gjennomføres, er det viktig at svaret fra den enhet som kontrollerer forespørselen, ikke kan endres fra nei til ja (eller omvendt).

Det vil også være behov for konfidensialitet og da gjerne av deler av en transaksjon. Dette kan være tilfelle ved autentiseringsdata hvis disse skal sendes som nevnt over. For elektronisk handel vil behov for konfidensialitet også kunne gjelde deler av transaksjonsdata. I transaksjoner som involverer flere parter kan det være ønskelig å skjule data som ikke er relevant for den enkelte involverte (f. eks. kan data om hvilke varer som kjøpes skjules for banken).

Det er også viktig at meldinger kommer fram i tide, at betaling skjer innen en tidsfrist - og at både avsender og mottaker får melding om at betaling har skjedd. Disse meldingene må kunne lagres slik at de kan brukes med beviskraft ved eventuelle disputter.

Innenfor feltet elektronisk betalingsformidling er man opptatt av å få avklart digitale signaturers rettslige beviskraft. Dette leder i sin tur til at det er ønskelig å ha retningslinjer for utstedelse av nøkler og sertifikat og krav til tiltrodde tredjeparter.

- Behov: Autentisering av personer, autentisering av utstyr som er opphav for meldinger, autentisering av mottak av meldinger, integritet, sekvensintegritet, ikke-benekting av mottak, ikke-benekting av sending og at meldinger kommer fram i tide.

Petroleumsbransjens elektroniske markedsplass: Secure Oil Information Link (SOIL)

Oljeindustrien samarbeider tett gjennom alle prosesser i både oljeselskaper og leverandørindustri gjennom oljefeltenes levetid. SOIL har som målsetning å effektivisere elektronisk samarbeid i oljeindustrien for lettere å utvikle tette, integrerte, prosesskoblede virtuelle organisasjoner.

Som teknisk motivasjon for å gjøre dette kan nevnes forhold som:

- Kompleks administrasjon
- Arbeidskrevende vedlikehold av adresser og kataloger
- Nye partnere medfører mye arbeid
- Stort antall linjer
- Alle vedlikeholder egne sikkerhetsløsninger
- Sikkerhet håndteres ved å utelukke hverandre på nettverksnivå
- Krav til kapasitet og sikkerhet gjør det vanskelig å benytte Internet

Markedsmessig motivasjon:

- Telemarkedet liberaliseres
- Konkurrende virksomheter etableres

- Ny modell må hindre at noen aktører får monopol

En samarbeidsgruppe bestående av Statoil, Saga, Norsk Hydro, BP Norge, Shell, Amoco, Philips, og Oljedirektoratet ble etablert høsten-97. I tillegg er OLF blitt løpende informert om utviklingen av konseptet. Det ble utført en markedsundersøkelse i nov. - jan. `98. Deretter ble det kjørt formell forespørsel i feb. - jun. '98. Fellesdata er valgt som leverandør. Løsningen har fått navnet SOIL - Secure Oil Information Link.

Test av tjenester og utprøving av pilot løsninger har foregått siden aug. '98 og en forventer at SOIL vil være i drift før årsskifte.

SOIL er ment som en markedsplass og teknisk infrastruktur for oljebransjen og baseres på bruk av internasjonale standarder (ref. IETF). Et høykapasitets bredbåndsnett danner basis i løsningen. Se følgende stikkord for funksjonalitet som vil tilbys over dette nettet:

- Sikkerhet er hovedkriteriet for måten dette er utformet på (design-kriterium). Mange teknikker og metoder er brukt for å forhindre uautorisert tilgang.
- Garantert tjenestekvalitet gjennom etablerte SLA krav. SLA rapporter gjøres tilgjengelige til hver kunde via web-løsning.
- E-mail, katalogtjeneste, og tiltrodd tredjepart (TTP) tjeneste er implementert i lokale ved Fellesdata i Skøyen i Oslo, som er sikret mot elektromagnetiske pulser (EMP).
- Extranet etableres som en markedsplass for autoriserte SOIL brukere.
- Kan etablere kundetilpassede lukkede brukergrupper.
- Skalerbarhet (aksesskapasitet og tjenester).
- Støtter de fleste aksessteknologier inn mot SOIL 50
- Kan benytte flere Internet tjenesteytere
- Aksess til SOIL er uavhengig av tele-leverandør så lenge standarder er brukt (eks. Telenor, Telia, ElTele).
- SOIL har lokale aksesspunkt i Stavanger, Bergen, og Oslo.

- SOIL «backbone» er basert på ATM. Båndbredde er en dynamisk ressurs, og utvidelser vil bli implementert ved behov.

Tjenestene er delt i to grupperinger, for henholdsvis tilgang (access) og tjenester (services) 51.

Tjenesten for sikker e-mail benytter sertifikat 52 utstedt av Fellesdata som tiltrodd tredjepart. En vil benytte følgende sikkerhetsgrad på sertifikatene: Sterk autentisering 53, konfidensialitet 54, integritet og ikke-fornektelse 55 .

I tillegg til å bruke dagens systemer i SOIL (typisk MS Windows og unix-klienter) vil man utvikle dette til også å kunne benytte nye løsninger basert på web-teknologi. En forventer også utvikling mot bruk av katalogtjenester og sertifikat for tilgangskontroll 56.

- Behov: Autentisering, konfidensialitet, integritet og ikke-fornektelse.

Norsk EDIPRO

En rapport fra Norsk EDIPRO i 1996, Digitale signaturer og tiltrodde tredjeparter, inneholder konkret utformete forslag på tre av de antatt viktigste områdene, - overordnede retningslinjer for en sikkerhetspolicy for TTP-tjenester, et forslag til det som kalles en »standard» i Norge for sertifikatformat, samt et forslag til en sikker navnestruktur. Rapporten fremhevet at formålet med å etablere det den kalte en sikker meldingsinfrastruktur basert på TTP-tjenester er å dekke viktige behov i forhold til autentisering, konfidensialitet, integritet og ikke-benekting. Det ble understreket at TTP-er må være tiltrodd evnen til upartisk å levere tjenester med en høy grad av funksjonell og teknisk tillit (sikkerhet) i forhold til elektronisk meldingsutveksling.

Offentlig innkjøp

Når det offentlige står for innkjøp av varer og tjenester er det i motsetning til næringslivet en del overordnede prinsipp som må ivaretas:

- åpenhet - kunngjøring og elektronisk informasjon må være tilgjengelig for hele verden
- likeadgang - 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 dokument 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 ikke i det offentliges øyne ett system eller en fastlagt serie med aktiviteter, men dels alternative virkemidler for å håndtere store volumer basert på EDI/EDIFACT og dels komplekse anskaffelser med kravspesifikasjoner publisert på web. Arbeids- og administrasjons-departementet (AAD) planlegger et eget program for elektronisk handel ved offentlige innkjøp som vil forfølge slike sentrale problemstillinger.

Når det gjelder dokument som er pålagt å benytte er det kunngjøringen krever til innlevering av tilbud innen et bestemt (absolutt) tidspunkt, dvs. krav om å sende tilbudet i tide eller minimum kunne bevise at tilbudet er sendt innen et bestemt tidspunkt (i dag godtas poststempling innen et bestemt tidspunkt).

Et tilbud er konfidensielt for alle, inklusive innkjøper, fram til et bestemt åpningstidspunkt som er senere enn innleveringstidspunktet for tilbudet.

For de som leverer inn tilbud er det viktig å være sikker på at bare de tilbud som var levert på rett måte, er med i konkurransen og dette må det være mulig å kontrollere (i dag er det gjerne offentlig anbudsåpning av papirkonvoluttene).

- Behov: Konfidensialitet (frem 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

Statskonsult

Statskonsult har gjennom flere år jobbet med området elektronisk saksbehandling, elektronisk innrapportering og IT- standardisering. Det er bl a laget følgende rapporter og notater som direkte eller indirekte har tatt for seg temaer rundt digitale signaturer og TTPer.

- Elektronisk saksbehandling (Statens generelle kravspesifikasjon), Statskonsult 1998.
- Innføring av elektronisk saksbehandling (veileder), Statskonsult 1998.
- En kartlegging av juridiske problemstillinger som reises ved innføring av elektronisk saksbehandling, Statskonsult notat 1997:3.
- Juridiske problemstillinger ved elektronisk saksbehandling og dokumenthåndtering, Statskonsult rapport 1998:13.
- NOSIP 2.0, Norsk OSI Profil (Krav til standarder som skal benyttes ved elektronisk kommunikasjon i staten), Statskonsult 1996
- Elektronisk datautveksling og innrapportering, Statskonsult rapport 1998:15.

Statskonsult har også etablert et brukerforum for elektronisk saksbehandling hvor offentlige etater kan ha en møteplass for utveksling av erfaringer med elektronisk saksbehandling og man kan få Statskonsult til å ta opp konkretet problemstillinger som brukerne måtte ha. Dette forumet er en del av et større program om elektronisk saksbehandling som Statskonsult er ansvarlig for. Programmet er flerårig og delfinansiert av AAD.

I notatet Elektronisk samhandling med og i offentlig sektor - Forslag til strategi for elektronisk datautveksling for offentlig sektor 1997 - 2001 57 skisseres en mulig strategi og handlingsplan for elektronisk datautveksling. Det foreslås blant annet prioritering av arbeidet for etablering av en tilstrekkelig nasjonal infrastruktur for informasjonssikkerhet. Det anbefales at dette må prioriteres, og at slikt arbeid inkluderer forsøksvirksomhet og etter hvert etablering av ordninger for digital signatur. Det anbefales dessuten at det igangsettes, prioriteres og gjennomføres et arbeid for at norske lover blir tilpasset elektronisk samhandling.

Arbeids- og administrasjonsdepartementet og rammeavtaler i offentlig sektor

Forvaltningsnettprosjektet ble startet i 1996 etter initiativ fra Arbeids- og administrasjonsdepartementet (AAD) i samarbeid med Kommunenes sentralforbund (KS). Det skal 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. I tillegg skal prosjektet etablere en rekke andre typer fellestjenester som er nødvendige for en helhetlig og velfungerende elektronisk infrastruktur. Digital signatur med tilhørende sertifiseringstjeneste er et prioritert område for offentlig sektor med et dokumentert behov hos ulike offentlige virksomheter for denne type tjenester.

Teknologien anses nå allment tilgjengelig og det finnes flere leverandører som vil tilby sertifiseringstjenester. Enkelte etater er allerede gått ut med forespørsler om leveranse av løsninger for digital signatur og sertifiseringstjenester med tanke på prøveprosjekter for elektronisk dokumentutveksling. Det er imidlertid et problem at teknologien (og sertifiseringstjenestene) ikke er godt nok standardisert og det kan oppstå situasjoner der to aktører ikke vil være i stand til å kommunisere med hverandre på grunn av at de har valgt forskjellige teknologiske løsninger og ulike sertifiseringstjenester.

Virksomheter (eller privatpersoner) som skal samhandle elektronisk med flere offentlige etater kan derfor komme i en situasjon der det kan være ulike krav til løsninger for digital signatur og sertifisering fra de ulike offentlige etater.

AAD har derfor, innenfor rammen av Forvaltningsnettprosjektet, tatt initiativ til samordning av krav til digital signatur-løsninger og sertifiseringstjenester innenfor offentlig sektor.

Det ble satt i gang arbeid med en felles kravspesifikasjon for sertifiseringstjenester (og andre tiltrodd tredjepartstjenester) samt systemer for digital signatur og meldingskryptering.

Kravspesifikasjonen ble utviklet i tett samarbeid med de etater som har størst behov for slike tjenester og/eller har kommet lengst i å ta dem i bruk og legger opp til at de nødvendige nøkler skal kunne legges inn på et smartkort (et kort som tilsvarer et vanlig bankkort, men med større «intelligens») som kan benyttes ved signering/kryptering av meldinger. Et slikt kort kan kombineres med et vanlig identifikasjons/adgangskort.

Det planlegges å legge denne kravspesifikasjonen til grunn for en utlysning av forespørsel om tilbud på sertifiseringstjenester og produkter for realisering av digital signatur i praksis. Tilbudene skal vurderes med tanke på inngåelse av rammeavtaler med aktuelle leverandører. Avtalene vil være tilgjengelig for hele offentlig sektor.

Det er frivillig for offentlige virksomheter å benytte seg av rammeavtalene og de må finansiere kjøpet av produkter/tjenester selv. Fordelen med rammeavtalene er at etatene ikke behøver å bruke ressurser på kravspesifisering, utlysning og behandling av tilbud. Det er en enkel prosedyre å kjøpe på en rammeavtale. Avtalen ivaretar også det nødvendige juridiske rammeverket for hvert enkeltkjøp.

AAD ønsker fortrinnsvis å inngå avtaler med flere leverandører av sertifiseringstjenester. Det vil i den forbindelse bli stilt krav om såkalt kryssertifisering, dvs. at de valgte leverandørene skal godkjenne hverandres tekniske løsninger, rutiner for og organisering av sertifikat- og nøkkelutstedelse. Det kan også bli aktuelt å stille særskilte krav til de valgte leverandørene om at de skal inngå forpliktende samarbeidsavtaler seg i mellom. Dette for å unngå situasjonen beskrevet ovenfor, med ikke-samspillende løsninger for digital signatur.

Arbeids- og administrasjonsdepartementet vil i tillegg til arbeidet under Forvaltningsnett-prosjektet iverksette et eget utredningsarbeid med spørsmål knyttet til utstedelse av et nasjonalt elektronisk ID-kort («borgerkort») og et enhetlig elektronisk ID-kort for de offentlig ansatte (med ID-kort menes her smartkort som både fungerer som fysisk identifikasjon og som en bærer av eierens elektroniske signatur- og krypteringsnøkler).

Tilbudene over Forvaltningsnettprosjektets rammeavtaler vil representere selve det tekniske grunnlaget for realisering av slike kort. I tillegg er det nødvendig å utrede forankringen og organiseringen av utstedelse og vedlikehold av slike kort. Arbeidet vil ha generell gyldighet og bør derfor ses i sammenheng med sektorinitiativer på området som f eks elektronisk helsepersonellkort og pasientkort.

Kommunal- og regionaldepartementet - pilotprosjektet EDNA

Kommunal- og regionaldepartementet og Husbanken gjennomfører pilotprosjektet EDNA - Elektronisk Dokumentutveksling i Norsk Administrasjon. Prosjektet skiller seg ut ved at det har utprøvd i praksis det som ellers »bare» blir beskrevet som teoretiske muligheter (f eks i denne rapporten). Derfor gis det noe bredere omtale nedenfor.

Et pilotprosjekt ble igangsatt med utgangspunkt i eksisterende edb-systemer, og med krav om å overholde gjeldende rammer og regler for saksbehandlingen i forvaltningen, se figur 2 nedenfor. Det var praktisk bruk av digitale signaturer, kryptering og TTP-tjeneste som var de sentrale mål. 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.

Ved prosjektstart i 1995/96 ble det klart at det ennå ikke forelå tilbud om tilfredsstillende teknologiske løsninger på markedet. En utviklingsavtale måtte inngås, ut fra kravspesifikasjon og scenarier knyttet til offentlig saksbehandling, med de tilhørende spesifikke sikkerhetstiltak 58. Som industripartner ble Posten SDS kontraktmotpart for en utviklingsavtale støttet av Statens Nærings- og distriktutbyggingsfond (SND). En norsk sikkerhetsapplikasjon SecApp (SecurityApplication) er utviklet. Den er basert på åpne løsninger iht internasjonale standarder, implementert og utprøvd, og har vært i daglig bruk i en periode. Måten implementeringen av sikkerhetskravene er gjennomført på, er evaluert og kvalitetssikret.

EDNA kan sies å være et pionerprosjekt på forvaltningsområdet ikke bare i nasjonal, men også i internasjonal sammenheng. Det er etablert helt konkrete operative løsninger for å ivareta krav til signatur, konfidensialitet og arkivering ut fra de formulerte forvaltnings- og sikkerhetsbehov, samt krav til leverandøruavhengighet. Løsningene og erfaringene fra dette prosjektet har klar eksempel- og overføringsverdi for offentlig sektor. Det minnes om at dette er løsninger for å ivareta sentrale sikkerhetsfunksjoner, ikke et elektronisk saksbehandlings-system som sådan. I et fremtidig elektronisk saksbehandlingssystem skal slike sikkerhetsfunksjoner som nå utprøves i praksis være integrert.

Prosjektledelsen i EDNA ser det som både ønskelig og nødvendig at det videre arbeidet på området skjer i samarbeid med næringslivet og sivile organisasjoner. Dette anses påkrevet fordi det i nær fremtid vil bli behov for elektronisk kommunikasjon med disse. Allerede i dag skjer det (som nevnt nedenfor) en del innrapportering fra privat til offentlig sektor. Privatpersoner og næringsliv vil i stadig større grad komme i direkte elektronisk kontakt med

førstelinjetjenester fra for eksempel Husbanken og Skattedirektoratet. Da er det viktig at løsningene som legges til grunn er omforente.

Figur 2: Dette er en skisse over dagens generelle saksgang i departementet/departementene, som følges i EDNA-prosjektet. I dagens EDNA-løsning kan dette synes tungvint, men ved en fremtidig løsning vil disse funksjonene bli integrert i/med et elektronisk saksbehandlingssystem, som vil forenkle og effektivisere prosessene for de som deltar i dem. Figuren er lånt fra EDNA-prosjektet.

- Behov: Meldingsintegritet, autentisering av opphav, konfidensialitet

Innrapportering til og i det offentlige, mv.

Statskonsult har i sin rapport om 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 digital signatur. 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 digital signatur 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 for bruk av kryptografiske løsninger.

- Behov: Autentisering og meldingsintegritet 59, sporbarhet og ikke-benekting - tidsstempling og logging, konfidensialitet.

Når det gjelder innrapportering til Statistisk sentralbyrå (SSB) og KOSTRA (kommune-stat innrapportering) er det lagt spesielt vekt på kryptering av sensitive data. Det er bare noen svært få innberetninger som krever signatur, KOSTRA vil imidlertid kreve dette etter hvert. Det legges heller ikke vekt på ikke-benekting.

- Behov: Konfidensialitet (kryptering av sensitive data)

Når det gjelder innrapportering til Brønnøysundregistrene, gjelder det offentlig tilgjengelig informasjon (regnskap) og er således ikke konfidensielle. Her er det derimot krav om signatur og ofte flere enn en signatur.

- Behov: Autentisering

Fiskeridirektoratet har et prosjekt på gang med innrapportering av bl.a. fangstmeldinger og passivmeldinger fra skip via satellitt. Krav til sikkerhet er under vurdering, men det er i alle fall krav til riktig avsender og meldingsintegritet.

- Behov: Autentisering og integritet

Statens vegvesen, Vegdirektoratet har utarbeidet en håndbok for elektronisk billettering med krav til samordning som myndighetene stiller overfor kollektivselskapene ved investering i elektroniske billetteringssystemer. Anonyme betalingsmåter som verdikort reduserer behovet for kontantbeholdning hos fører, men øker krav til sikkerhet og kryptering av informasjon på et chipkort. Det legges opp til at selskapene har ansvar for generering av sikkerhetsmoduler og utstedelse av egne kort til brukere.

- Behov: Autentisering opphav, integritet, sekvensintegritet, konfidensialitet og ikke-benekting

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).

Datatilsynet vil iht forslaget 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.

Riksarkivet utarbeider ny arkivstandard 60 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 dokument, samt ved arkivering.

Helsesektoren

I helsesektoren formidles store mengder informasjon innen administrativ saksbehandling og pasientbehandlingen. Årlig foretas ca. 12-16 millioner konsultasjoner i primærhelsetjenesten, 3 mill. polikliniske konsultasjoner i sykehus og 650 000 innleggelser i 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.

Regler for journalføring er i dag hjemlet i flere helsepersonellover. Reglene omfatter bl.a. krav til føring, innsynsrett, innhold, utlevering og lagring. En elektronisk pasientjournal i sykehus (helseinstitusjoner) er i dag ikke likestilt med papirjournal og det kreves at pasientinforma-sjonen skal oppbevares og lagres som papir eller mikrofilmet. Regler for oppbevaring og lagring gis av Datatilsynet og Riksarkivaren. Oppbevaringsplikt er i dag uendelig for somatiske og psykiatriske institusjoner (med unntak av røntgenbilder som er 10 år), mens for allmennlege- og tannlegevirksomhet er oppbevaringsplikten satt til 10 år etter siste nedtegning.

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 (institusjonregistre) og til sentrale større registre. Som ved annen dokumentforsendelse er det behov for identifisering av avsender og beskyttelse mot ikke autorisert innsyn.

Sosial- og helsedepartementet utarbeider ny lov om helsepersonell og ny lov om helseregistre og elektronisk behandling av helseopplysninger, der det legges opp til å likestille elektronisk og papirbasert pasientjournal, at nedtegninger i pasientjournalen skal signeres og at man i forskrifter vil gi nærmere regler for føring, langtidslagring, kodeverk, signering og kommunikasjon. Det legges videre opp til at departementet kan gi bestemmelse om form og frist for innsamling av helsopplysninger til sentrale helseregistre, herunder pålegg om sikkerhet, bruk av standarder, kode og klassifikasjonssystemer m.m.

- Behov: Konfidensialtet (identifiserbare personopplysninger), integritet, autentisering opphav, sikre at melding kommer frem (laboratoriemeldinger, henvisning/epikrise), autentisere mottaker, sekvens-integritet (bl.a. ved at resepter ikke kan skrives ut flere ganger), signatur (bl.a. journal, resept, legeregning og overføring av helseopplysninger).

Forsvaret

Forsvarets overkommando/ Sikkerhetsstaben har gjennomført et arbeid med det mål å belyse problemstillinger omkring sikkerhet i endesystemer. Aktuelle områder som er vurdert er bl. a. bruk av digitale signaturer, TTP-tjenester, samt opprettelse av et domene for offentlig nøkkelkryptografi i Forsvaret. Det er fokusert på Forsvarets behov, men gruppen har også vurdert arbeidets konsekvenser og relevans for statsforvaltningen forøvrig. Arbeidsgruppen har utarbeidet en rapport som i tillegg til å komme med vurderinger, også anbefaler konkrete løsninger, samt skisserer behovet for videre arbeid. Gruppens anbefalinger og arbeid vil følges opp, og det vil sannsynligvis etableres et PKI-pilotprosjekt i løpet av 1998.

NATO har i lengre tid arbeidet med planer om å etablere en NATO PKI. Det er opprettet en gruppe (PKI Ad Hoc Working Group) som skal utrede aktuelle tekniske og operative løsninger. Målet med arbeidet er å få etablert et felles NATO PKI domene, med full interoperabilitet i hele domenet. De enkelte medlemsland bidrar med innspill til dette arbeidet. Flere av innspillene er basert på konkrete erfaringer ved bruk av allerede implementerte nasjonale løsninger. Dette dreier seg om PKI strukturer, varierende TTP-tjenester, og bruk av digitale signaturer.

Gruppen har utarbeidet et draft for hvilke mål og resultater som skal oppnås, samt frister for dette arbeidet. Det dreier seg om 5 hovedpunkter med tilhørende underpunkter. Disse er å: A: Etablere en arkitektur for et NATO PKI, B: Komme til enighet om en management struktur og tilhørende prosedyrer, C: Implementere et pilot PKI for å teste infrastrukturen og management prosedyrene, D: Dokumentere et felles rammeverk, og etablere en felles forståelse for ulike PKI-spesifikke begreper, samt (E):Potensielle oppgaver.

Norges forskningsråd

Programmet Nasjonalt informasjonsnettverk (NIN) er innrettet for igangsetting av et antall pilotprosjekter og demonstratorer for å oppnå økt elektronisk samhandling. ININ er etablert som en prosjektgruppering for å ta seg av felles infrastrukturspørsmål og kvartalsvise fagsamlinger skal samle ulike faglige støttemiljø for å ta del i erfaringsutvekslingen.

ININ har igangsatt en rekke fellesprosjekter for å etablere en infrastruktur mellom prosjektene, bl.a.

- ININ-K Implementering og initiell drift av en katalogtjeneste for NIN. Katalogtjenesten er i prøvedrift og kan nås via web på http://maxware.no/nin

Prosjektet har klarlagt hvilke type katalogopplysninger som er interessante internt i informasjonsnettverk og hva slags prosesser som er brukbare for å sikre oppdateringer og ønsket beskyttelse og eksponering med sporbarhet og autentitet. Det er åpent for demonstratorene i NIN å lage egne understrukturer i katalogen.

- ININ-K Katalogforum. Sammen med Arbeids- og administrasjonsdepartementet er det tatt initiativ til å etablere et samarbeidsorgan som kan sørge for koordinering om kataloginformasjon og katalogtjenester, som epost- og edi-adresser, digitale sertifikater og annen kontaktinformasjon.
- ININ-S Sikring og integritet i informasjonsnettverk. Prosjektet har levert en sikkerhetshåndbok og arbeider med planer om et sikkerhetsforum.
- ININ-T Kvalitetundersøkelser av IKT tjenestetilbud. Prosjektresultatene er lagt ut på web-siden til Veritas.
- ININ-B BitBank. Forprosjekt for problem knyttet til langtidslagring av elektroniske dokument og signaturer. Prosjektet har som målsetting å forta en første kartlegging av behov, beskrive tiltak som er igang hos ulike instanser og gi en teknologisk status.
- ININ-N Normer og standarder. En tjeneste i å etablere normer og standarder av prosjektresultatene i NIN-demonstratorene, samt gi råd om eksisterende standarder og prosesser for å endre disse.

Det er videre etablert samarbeid med Forvaltningsnettprosjektet i AAD og Kommunenes Sentralforbund om å prøve ut kravspesifikasjonene i praktiske NIN-demonstratorer.

Vedlegg 3: Kort oversikt over standarder

Det er ikke plass til å gi en fullstendig oversikt over alt standardiseringsarbeid som er av relevans for etablering av systemer for digitale signaturer.

En oversikt er for øvrig på europeisk initiativ utført av Andrew Colleran: Standardisation Issues for the European Trusted Services - ETS. 61

I norsk offentlig sektor lages det ulike rammeavtaler i regi av Forvaltningsnettprosjektet (i et samarbeid mellom Arbeids- og administrasjonsdepartementet og Kommunenes Sentralforbund). En kravspesifikasjon for digitale signaturer mv er utarbeidet, som grunnlag for kommende rammeavtaler på dette området. Formålet er blant annet å oppnå en standardiseringseffekt på området for digitale signaturer i offentlig forvaltning. Løsningene her kan også få betydning for privatpersoner og næringsliv som kommuniserer med forvaltningen. Se nærmere omtale i pkt 5.3.5 foran, samt websiden som inneholder kravspesifikasjonen, diskusjoner og artikler med nærmere omtale: http://forvaltningsnett.dep.no/.

I staten er det slik at Statskonsult er tillagt ansvaret for vedlikehold og videreutvikling av NOSIP og etableringen av et standardiseringssekretariat for statlig sektor. NOSIP kan omfatte krav til standarder for digitale signaturer og sertifikatformater, og omfatter i dag krav til kataloger. Statskonsult reviderer i disse dager (høsten 1998) NOSIP og vurderer å ta med krav til standarder for digitale signaturer, sertifikater og kataloger.

En liten advarsel til leserne: teksten nedenfor inneholder et stort antall forkortelser mv fra en teknisk orientert verden. For lesere som er interesserte og har kunnskaper på dette området vil forhåpentlig teksten være både lesbar og interessant. For lesere på et mer overordnet nivå kan dette bli litt mye av det gode, og det kan være nok å konstatere at det finnes mange standarder på området som vil støtte bruken av digitale signaturer, og mange flere er under utvikling. Men »detaljene» kan man overlate til spesialistene.

Sluttbrukerapplikasjoner og sluttbrukerutstyr - standardisering og stabilitet

Generelt bør brukervennlighet prioriteres ved implementering i sluttbrukerapplikasjoner og -utstyr. For digitale signaturer og kryptering vil i tillegg gjelde at disse i størst mulig grad blir usynlige for bruker, både

- i grensesnitt mot underliggende datakommunikasjonstjenester
- mot en katalogtjeneste
- ved dekryptering i en brukers postmottakstjeneste

Enkelte av sikkerhetstjenestene bør være synlige nettopp av den grunn at brukerne skal være bevisste hva de gjør. I visse tilfelle kan det ikke være ønskelig med synlighet, f.eks. ved signering på (EDIFACT-)konvertert melding.

De komponentene som kan inngå ved normal bruk av et system for digital signatur og meldingskryptering er:

- Lokalt system (typisk PC-klient) hos avsender av meldingen,
- Katalogsystem for henting av sertifikater og tilbakekallingslister,

- Meldingsformidling, f. eks. over nettverk, eller ved lagring av filer med felles aksess - dette inngår ikke i kravspesifikasjonen,
- En tjeneste for tiltrodd tidsstempling av meldinger skal tilbys, men vil typisk brukes bare i spesielle tilfeller,
- Tiltrodd (ekstern) verifikasjonstjeneste for de offentlige etater som ønsker å benytte en slik tjeneste,
- Lokalt system hos mottaker - dette kan være en PC-klient for en bruker, eller en postmottakstjeneste hos den mottakende etat.

Med tanke på en funksjonsspesifikasjon kan følgende tjene til hjelp:

- Systemet må ha god brukervennlighet
- Effektiviteten i løsningen, inkludert aksess til katalog, må være tilfredsstillende
- Søking i katalog bør så langt som mulig være transparent for brukeren, eventuelt med et godt, enkelt bruker-grensesnitt.

I Sverige er det utarbeidet en funksjonsspesifikasjon for Allterminalen, en sikkerhetsløsning for PC'er i nettverk med støtte for aktive kort, se www.seis.se/kort/normer/seisfunkspec.html

Algoritmer for digitale signaturer / kryptografiske hash 62funksjoner

Den mest brukte algoritmen for digitale signaturer kalles RSA etter opphavsmennene (Rivest, Shamir , Adleman). Metoden ble presentert i 1978 og har siden det vært en de facto standard på området. RSA algoritmen er inkludert i standarder fra ISO/IEC, CEN, IEEE, Internet S/MIME, SSL, SET.

Et viktig alternativ til RSA er den amerikanske standarden beskrevet i FIPS PUB 186 - Digital Signature Standard (DSS). DSS benytter andre matematiske prinsipper enn RSA og er inkludert i standarder fra ISO/IEC, ANSI og IEEE.

I tillegg til selve signaturalgoritmen er det også behov for å standardisere kryptografiske hashfunksjoner. Disse benyttes til å komprimere meldingen før selve signeringen og er en sikkerhetkritisk komponent i systemet. I dag er Secure Hash Algorithm, versjon 1 (SHA-1) og RIPEMD-160 ansett som de beste kandidatene til denne oppgaven. SHA er definert i FIPS-PUB 180-1 og skal benyttes sammen med DSS. Begge hashfunksjonene er definert i en standard fra ISO/IEC. En annen hashfunksjon som også inngår i mange spesifikasjoner er MD5, men denne vurderes i dag som mindre sikker enn SHA-1 og RIPEMD-160 .

Sertifikatformater

ITU-T X.Recommendation X.509 (ISO/IEC 9594-8) "Information Technolgy - Open SystemsInterconnection - The Directory: Authentication framework".

Denne rekommendasjonen spesifiserer autentiseringstjenester for X.500 kataloger. Standarden spesifiserer også syntaks for såkalte X.509 sertifikater. Versjon 3 er den nyeste og mest brukte. Denne definerer en sertifikat struktur som gir anledning til utvidelser for å støtte mange forskjellige anvendelser. Dette gir anledning til interoperabilitet mellom ulike komponenter og spesielle tilpasninger som kan dekke de fleste behov. X.509 v3 sertifikater benyttes i dag av Internett PKI-standard.

Et X.509 v3 sertifikat består av følgende felt:

- versjon
- serienummer
- signatur algoritme
- utsteder
- gyldighetsperiode
- bruker navn
- informasjon om offentlig nøkkel
- identifikasjon av utsteder
- identifikasjon av bruker
- utvidelser
- CAs signatur over de andre feltene

Rapporten «Digitale signaturer og tiltrodde tredjeparter « fra Norsk EDIPRO inneholder et forslag til sertifikatformat basert på X.509v.3, som et utgangspunkt for diskusjon om hva man bør samle seg om i Norge.

Signaturformater

Et forslag til formater for digitale signaturer er spesifisert i PKCS #7 og PKCS #9. World Wide Web Consortium studerer feltet i detalj med tanke på utarbeide nødvendige spesifikasjoner for å støtte utveksling mellom ulike løsninger. IEEE P1363 gjør også et omfattende arbeid på dette området. Prosjektet antas ferdig inneværende år.

Offentlig nøkkel infrastruktur (PKI) og krav til interoperabilitet

Den amerikanske standardiseringsorganisasjonen NIST har utviklet «Minimum Interoperability Specifications of PKI Components». Målet med dette dokumentet er å spesifisere egenskaper, meldinger, formater og sertifikatfunksjoner som kan sikre samtrafikk mellom PKI-komponenter levert av forskjellige leverandører.

Internet Public Key Infrastructure er en firedelt standard fra IETF for utvikling av et PKI for Internett. Standarden består av fire deler:

- Part 1: X.509 Certificate and Certificate Revocation List Profile
- Part 2: Operational Protocols
- Part 3: Certificate Management Protocols
- Part 4: Certificate Policy and Certificates Practices Framework.

Tiltrodde Tredjepart tjenester (TTP)

ISO/IEC JTC1/SC27 arbeider med å spesifisere bruk og administrasjon av TTP-tjenester. Det foreligger en teknisk rapport 63. En ny standard for TTP-tjenester til støtte for digitale signaturer 64 er nå under utarbeidelse. Også innenfor ETSI skjer det arbeid på dette området.

Programmeringsgrensesnitt (APIs)

Programmeringsgrensesnitt må være tilgjengelig både inn mot ulike PKI-tjenester og mot lavere sikkerhetsmoduler, f.eks basert på smartkort eller annen maskinvare. PKCS#11

definerer grensesnitt mellom sertifikat og applikasjon. Smarkortleverandører har også definert sin API, f eks MEL API under et operativsystem for smartkort som kalles Multos. For øvrig finnes GSS-API som et generiske grensesnitt mot sertifiseringstjenester mens CAPI fra Microsoft og Generic Cryptographic Services API fra Open Group er eksempel på grensesnitt mot spesifikke kryptotjenester.

Sikkerhetsprotokoller

Arbeid innenfor dette området vil dels søke å ta fram spesifikasjoner for spesifikke sikkerhetsprotokoller, dels legge inn nødvendig sikkerhetsfunksjoner i eksisterende protokoller. Av nye og viktige protokoller kan nevnes fra Internet Lightweight Direct Access Protocol (LDAP), Internet Security Association and Key Management Protocol (ISAKMP)/OAKLEY, Secure Sockets Layer (SSL), Secure Electronic Transaction (SET). Secure/Multipurpose Internet Mail Extensions (S/MIME) og nye sikkerhetsfunksjoner i Ipv6 er eksempel på hvordan sikkerhet bygges inn i etablerte protokoller.

Smartkortteknologi

Utviklingen tyder på at bruk av smartkort blir en viktig komponent i et framtidig system for digitale signaturer. Smartkortet vil både beskytte de hemmelige nøklene og utføre sikkerhetskritiske kryptofunksjoner. ISO 7816 spesifiserer de fysiske egenskaper til kortet og kommunikasjon med kortterminal. Det eksisterer ulike typer smartkort, fra minnekort for enkel lagring av informasjon (telefonkort) til prosesserbare kort med en eller flere applikasjoner på kortet.

[Arbeid innenfor CEN TC224 og ISO TC68 er viktig for å etablere de nødvendige standardene på dette området. En ny versjon av SET (C-SET) vil basere seg på bruk av smartkort. Microsoft, Netscape m.fl har blitt enig om et felles grensesnitt for å kommunisere med slike aktive kort og vi kan forvente at smartkortleser blir en integrert del av en standard PC innen kort tid.]

For å etablere en løsning for bruk av digitale signaturer som lett kan oppdateres i tråd med den teknologiske utviklingen og endrede krav, kan det utvikles et sett med kryptografiske moduler. Man kan tenke seg at det benyttes en kortteknologi som kan inneholde slike moduler, samt funksjoner for håndtering av nøkkelmatriell og algoritmer for de enkelte brukerne. Kort og applikasjoner for elektronisk pengepung er basert på standarder nevnt ovenfor. Europay, Masercard og VISA har i EMV'96 spesifisert transaksjonsflyt og sikkerhet mellom smartkort og kortterminal. EMV Errata '98 spesifiserer ny funksjonalitet for smartkort som kan inneholde flere applikasjoner. De ovennevnte modulene må ha ett felles grensesnitt, og dette grensesnittet må defineres og bør være lik en av CAPI standardene.

Katalogtjenester

For å finne fram til sertifikatet for en gitt bruker, vil det være nødvendig med en effektiv katalogtjeneste. Rekommendasjon X.500 fra ITU-T er standardreferansen for slike tjenester.

Tidsstempling

I mange sammenhenger er tidspunktet for når et dokument ble signert eller kommunisert essensielt for sikkerheten eller fullbyrdelsen av en transaksjon. Tidsstempling kan utføres av en TTP som begge parter har tiltro til.

Public Key Infrastructures/Certification Authority tjenester krever også bruk av time-stamp service for å sikre seg mot at utgåtte sertifikat benyttes til å signere objekter for en dato når sertifikatet var gyldig.

En arbeidsgruppe innenfor PKIX i IETF har uttalt at de vil utvikle en egen protokoll for en slik tjeneste. Arbeidet er interessant.

Evaluering og administrasjon

Bruk av digitale signaturer krever tillit til mange kritiske komponenter. Det kan oppnås ved at utvikling og implementering av produkter evalueres og sertifiseres. ITSEC 65 er eksempel på et sett av europeiske kriterier for slik evaluering. USA og Canada har hver sine kriteriesett. Det har vært arbeidet lenge for at alle slike regionale kriterier på sikt blir erstattet av felles kriterier globalt, Common Criteria (CC). CC er høsten 98 på vei til å bli en ISO standard og åpner for å definere spesifikke profiler for ulike systemer. Den tyske digital signatur-ordningen legger til grunn at ITSEC brukes som målestokk for å evaluere sikkerheten i produkter for digitale signaturer (men også der vil CC bli brukt når den foreligger som en internasjonal ISO-standard).

BS 7799:1998 er et annet sett av tiltak som kan benyttes til å sertifisere at en organisasjon har et IT-system med nødvendige sikkerhetstiltak. Den består av prosessbeskrivelser for revisjon, risikohåndtering, sertifisering, samt bakenforliggende krav til å sette i gang med arbeidet. BSI DISC har laget et støttesystem som hjelper organisasjoner til å utvikle sine informasjons-systemer - helt til endelig c:cure sertifisering, som er det godkjente sertifiseringssystemet for BS 7799.

Guidelines for the Mangement of IT Security (ISO/IEC 13335) er et rammeverk i flere deler som gir nødvendig bakgrunn for administrasjon av sikkerhetsløsninger.

Nasjonalt vil bl a regelverk fra Kredittilsynet og Datatilsynet, samt den nye loven om forebyggende sikkerhetstjeneste, og det nettopp reviderte statlige Datasikkerhetsdirektivet, gi pålegg om å gjennomføre en rekke sikkerhetstiltak. Bruk av evaluerte og sertifiserte produkter, herunder for digitale signaturer og innholdskryptering, vil kunne gjøre det lettere å etterleve ulike sikkerhetskrav, deriblant i regelverk som nevnt.

I Norge har forslag til to ulike ordninger for sikkerhetssertifisering av henholdsvis produkter/systemer, og organisasjoner, vært fremmet av Rådet for IT-sikkerhet 66. Forslagene har lagt til grunn de nevnte kriteriene for evaluering og sertifisering (henholdsvis ITSEC - CC for produkter/systemer, og BS 7799 for organisasjoner), se kapitel 8.2.2. Regjeringen har foreslått kr 5 millioner på 1999-budsjettet for å etablere disse to ordningene.

vedlegg 4: kort oversikt over aktuelle produkter og ttp-tjenester

Det eksisterer en rekke produkter, både norske og internasjonale, som gjør det mulig å foreta digital signering og håndtere sertifikater. Heller ikke her tar vi sikte på å gi noen uttømmende oversikt. Språkbruken i dette vedlegget er blitt relativt full av forkortelser og fagbegreper.

Elektronisk post

Sikkerhetsprodukter for meldingsformidling og elektronisk post kan påføre meldingen en digital signatur og eventuelt kryptere innholdet i den i tillegg. Sammen med den signerte meldingen kan det sendes et nøkkelsertifikat med en entydig identifikasjon av avsender. Mottakeren kan verifisere mot en sperre/tilbakekallingsliste om sertifikatet er gyldig, samt verifisere sertifikatutstederens digitale signatur. Spesifikasjonen S/MIME er blitt IETF-standard for sikker e-post og bygger på åpen nøkkel-teknologi og RSA-signering. Følgende krav kan stilles for en e-post-klient ved bruk av S/MIME:

- det skal være mulig på en brukervennlig måte å lage og verifisere S/MIME-baserte meldinger
- støtte for å importere og/eller eksportere den privat nøkkelen og sertifikatet til bruk i andre e-postklienter
- brukeren skal angi passord for å få adgang til nøkler, enten en gang eller hver gang nøklene benyttes
- støtte for automatisk lagring av nye sertifikat i klienten, dvs når man har verifisert et sertifikat så kan det lagres lokalt i klienten for framtidig bruk
- støtte for å hente sertifikat i kataloger via LDAP
- støtte for lagring av nødvendige CA sertifikat, i klienten, for verifisering av brukersertifikat
- støtte for å hente tilbakekallingslister via LDAP
- støtte for å verifisere tilbakekallingslister
- støtte for å verifisere sertifikat mot tilbakekallingslister
- støtte for sterk kryptering, dvs krypteringsnøkler som er lengre enn 40 bits

De krav som er markert med kursiv tekst er relevante for en sikker e-postløsning. I de e-postløsninger som finnes tilgjengelige i dag savnes bare denne funksjonaliteten. I IETFs S/MIME working group pågår det arbeid med å spesifisere hvordan sikre e-postløsninger skal håndtere og bruke tilbakekallingslister. Dagens produkter savner helt denne funksjonalitet. En annen mangel med produkter som er utviklet i USA er for svak kryptering, dette på grunn av de amerikanske eksportrestriksjonene. Det kan derfor, i mange tilfelle, være vanskelig å stille krav til sterk kryptering, siden de fleste produktene kommer fra USA. Nedenstående produkter er blitt gjennomgått og godkjent av RSAs S/MIME Interoperability Center. I hovedsak er produktene av to typer, dels POP3 (iblant IMAP) klienter og dels plug-ins til Microsofts e-post klienter.

- Microsoft Outlook Express (inngår i Explorer 4.0)
- Netscape Messenger (inngår i Communicator 4.0)
- Worldtalk Worldsecure Client
- Baltimore Technologies Mail Secure
- Entrust/Express
- SSE TrustedMIME

Produktene fra Baltimore Technologies og SSE utvikles i Irland og kan derfor beholdes med sterk kryptering.

Ingen av de produkter som er beskrevet over har innebygget støtte for elektroniske id-kort, men følgende muligheter finnes:

- Netscape Messenger benytter grensesnittet PKCS#11 og via dette kan det etableres støtte for elektroniske id-kort.
- SSE TrustedMIME har idag støtte for et eget smart kort og kan kanskje komme til å støtte elektroniske id-kort.

Arbeidsgruppen kjenner til to norske produkter for digitale signaturer. Produktet Conax-Postsec fra Telenor Conax finnes i en grunnleggende versjon som ikke benytter sertifikater, men er planlagt integrert med sertifikater i kommende versjoner. For å signere brukes smartkort og PIN-kode basert på algoritmene MD5 og RSA. Produktet beskrives på http://www.conax.com

Produktet SecApp fra Posten SDS finnes i flere konfigurasjoner. I vanlig bruk benyttes sertifikater som enten bæres av smartkort, eller legges som krypterte filer på diskett eller harddisk. Produktet gjør oppslag i offentlig katalog for å hente sertifikater eller tilbakekallingslister og er planlagt integrert med browserteknologi, se http://www.sds.no/produkt/

En markedsundersøkelse gjennomført for Samarbeidsgruppen 67 i november 1997 viser at Bull, IBM, Network Security (ActivCard), PDI Consult (Algorithmic Research) og Telenor Bedrift leverer sikkerhetsløsninger av forskjellige typer, bl.a. smartkort-løsninger for autentisering av brukere, konfidensialitet og digitale signaturer.

WorldWideWeb-baserte tjenester og applikasjoner

Det største gjennomslag har PKI-teknikken fått for www-baserte tjenester. PKI-teknikk er nå blitt standard teknikk for sikkerhet på Internet. Støtte for teknikken finnes f.eks. i standard-browsere både fra Netscape og Microsoft med funksjoner som SSL-protokoll for autentisering/kryptering og LDAP for tilgang til katalogtjenester. På samme måte inneholder webserver-produktene støtte for disse protokollene.

Et problem i denne sammenheng er at de produkter som får eksportlisens fra USA har et sikkerhetsnivå som er å betrakte som lite tilfredsstillende på områder med et noe høyere krav til sikkerhet: autentisering kan skje bare med inntil 512-bits nøkkellengde, noe som i dag ikke anses som tilstrekkelig. Likeledes skjer innholdskryptering bare med 40-56 bits nøkkellengde, noe som heller ikke gir tilstrekkelig beskyttelse mot de som vil skape tilgang til informasjonen. Med den dominerende plass amerikansk programvareindustri har på verdensbasis, og verdens tilsvarende avhengighet, er dette et problem som rammer globalt.

Svenske virksomheter, blant andre AU-system og Nexus har utviklet produkter som kan benyttes for å høyne sikkerheten og også komplettere svakhetene i de nåværende produkt fra Microsoft og Netscape, f.eks. håndtering av tilbakekallingslister for sertifikat.

En tydelig tendens innen IT-området er at flere applikasjoner gjøres web-baserte i form av intranet. Man kan t.o.m. påstå at stort sett alle nye applikasjonsutviklingsprosjekt er basert på web/internet-teknikk.

Samme sikkerhetsarkitektur kan dermed anvendes for alle slike typer av applikasjoner, enten det er saksbehandlingssystem i sosialtjensten eller journalsystem i helsesektoren.

Elektronisk handel

Det finnes en rekke norske leverandører av løsninger for elektronisk handel. De fleste er basert på meldingsstandarden UN/EDIFACT. Flere leverandører er i ferd med å gå over til versjon 4 av EDIFACT, som bl a gir støtte for digital signering av meldinger og utveksling av sertifikater. Et norsk forum for elektronisk handel, eforum.no, er etablert som en ideell organisasjon med medlemsbedrifter som bruker elektronisk handel i egen virksomhet eller er tilbyder av produkt og tjenester. Eforum.no har inngått samarbeidsavtale med CommerceNet International om erfaringsspredning til sine medlemmer.

I det svenske Topplederforums prosjekt for elektronisk handel har man forutsatt at edi-sertifikat lagres i katalog. Kort med id-sertifikat gir mulighet for å beholde edi-sertifikat. Det er et sterkt ønske at samme løsning med kort benyttes også i andre sammenhenger. Elektronisk handel i henhold til Topplederforums avtale baseres på handel mellom parter bundet i avtaler og sertifikat kan utveksles ved avtaleinngåelse.

Generelle klient-server-applikasjoner

Mange eksisterende system og produkt for klient/server-miljø som benyttes i offentlig forvaltning er ikke, eller planlegges ikke å bli web-basert. Disse system og produkt må derfor »PKI-tilpasses». Å gjøre en slik tilpasning kan innebære et relativt stort arbeid, selv om arbeidet kan forenkles med »verktøykasser» fra noen av leverandørene i markedet. Her må kundene i offentlig sektor stille felles krav til sine leverandører og få dem til å implementere støtte for PKI og elektroniske id-kort.

Fjernarbeid

I takt med stadig mer fleksibelt arbeidsliv og med moderne kommunikasjonsteknikk finnes det i dag store muligheter til å arbeide på avstand mot virksomhetens interne datamiljø. Et alvorlig problem i denne sammenheng er sikkerheten: Hvordan autentisere brukere som ringer inn eller kopler seg opp på Internet, og hvordan skal informasjonen beskyttes på veien?

Den teknikken som akkurat nå er mest lovende for slik bruk kan sammenfattes under betegnelsen »Virtual Private Networks», VPN. Med denne teknikk bygges det opp et virtuelt privat nett utenpå en offentlig nettjeneste som kan være det offentlige internettet.

All den »interne» trafikken sendes gjennom en sikker »tunnel» i det offentlige nettet. Sikkerheten omfatter autentisering i en sikkerhetsserver før klientene slippes inn i det interne nettet og kryptering av all tunneltrafikk.

For VPN har det tidligere vært tilgjengelig en mengde leverandørspesifikke sikkerhetsløsninger, men selv her skjer en standardisering som bygger på PKI-teknikk, og i IETF har man spesifisert IPSEC, et sikkerhetstillegg til TCP/IP-standarden.

Det finns flere VPN-produkter på markedet, f eks Digital Altavista Tunnel, Microsoft PPTP, Semaphore NSS (Network Security System) og Teamware Internet Security Server. De første produktene kommer fra USA og har derfor begrenset sikkerhet. Det siste produktet kommer fra Finland og leveres med sterkere kryptering og vil i løpet av 1998 ha støtte for elektronisk id-kort. I Norden benytter Telenor Marlink produktet NSS i sitt »Electronic Commerce»-produkt rettet mot internasjonal shippingindustri. Nøkkeladministrasjon og sertifikatutstedelse er helautomatiske prosesser mellom parvise krypteringsenheter og er således sin egen Certification Authority.

Selv om det altså ikke finnes ferdige produkter som kan benytte det elektroniske id-kortet på dette området, så er dette kanskje en av de viktigste tilpasningene for elektroniske id-kort i framtida, slik at man får en sikker binding til en spesifikk bruker, og ikke til hans PC.

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) er en programvarepakke for kryptering og signering av elektronisk post og datafiler. Programmet baserer seg på asymmetriske teknikker for signering og nøkkeldistribusjon, mens en symmetrisk algoritme benyttes for volumkryptering av filer. Ulike algoritmer er tilgjengelige i forskjellige versjoner av programmet. PGP er fritt tilgjengelig for privat bruk, men finnes også i kommersiell versjon fra Network Associates. Programmet er mye utbredt på Internett.

PGPs tilnærming til utveksling av sertifikater basere seg på en form som man kan kalle "kjede av tillit". PGPs offentlige nøkler er validert/sertifisert/signert ikke av en CA men av den enkelte bruker på basis av den enkelte brukers tillit til andre. Alle PGP-brukere kan sertifisere enhver nøkkel han eller hun ønsker å sertifisere. Dette betyr at brukeren tror at den aktuelle nøkkelen tilhører personen som er navngitt i sertifikatet. PGP tillater også brukerne å si at de stoler på sertifikater som en annen bruker har gått god for og slik skapes en kjede av tillit.

Offentlige PGP-nøkler legges ofte på den enkelte brukers hjemmeside, eller man utveksler nøkler ved å treffe hverandre personlig. Dette er en enkel måte å utveksle offentlige krypteringsnøkler på, men virker best for små brukergrupper. For større brukergrupper rekker ikke tilliten langt nok og man får raskt offentlige nøkler som verken du eller noen du stoler på har gått god for. Dermed kan ikke nøkkelen brukes til å verifisere avsenderen.

Et problem med PGP nøkler er at de aldri slutter å være gyldige og at det ikke finnes noen metoder for å kalle tilbake sertifikater.

Utprøving

Utover det som har vært nevnt i kapitel 4.3 (og vedlegg 2), pågår det også andre prosjekter for å vinne erfaring med digital signatur, ikke minst i utlandet.

EU's langvarige satsing er nevnt tidligere 68. De fleste EU-prosjekter relatert til digitale signaturer og TTP-problemstillinger er tilgjengelige fra den websiden som er oppgitt i fotnoten. Dette er til sammen et meget omfattende materiale, fra 1992 frem til i dag, og bør studeres for å nyte godt av de erfaringene som er gjort. Oversikt over relevante Rådsbeslutninger finnes på en egen side. DG XIII begynte allerede i 1992 å se på spørsmål knyttet til det som ble kalt Trusted Services, herunder initiativer på områdene elektroniske signaturer (Electronic Signatures) og tjenester fra tiltrodde tredjeparter (Trusted Third Party Services, TTPS). Initiativene ble tatt i samråd med SOGIS, en rådgivende gruppe sammensatt av »senior officials» fra medlemslandene (der Norge har deltatt, først med en representant, så med to, som observatører). I en rekke prosjekter er bl a konkrete produkter prøvd ut.

Den finske regjering har i en beslutning av februar 1998 slått fast at det skal utstedes et elektronisk ID-kort til alle finske borgere, som grunnlag for «elektroniske transaksjoner med det offentlige». Det finske folkeregister ble utpekt som utsteder av slike kort. Det skal også utstedes egne ID-kort for offentlig ansatte.

Den svenske forvaltningen har nylig utlyst en forespørsel om tilbud på sertifiseringstjenester ifm et elektronisk ID-kort for ansatte i forvaltningen.

I Sverige har et stort antall pilotprosjekt med elektronisk id-kort blitt utført med spesifikasjoner fra foreningen SEIS, med eksempel fra IDOL-prosjektet der studenter ved den Kongelige Tekniske Høyskolen i Stockholm utstyres med elektroniske ID-kort, og har muliggjort kommunikasjon med LADOK (studieresultat, adressendringer) og Teknologibutikken (bokbestillinger). Disse pilotprosjekt har alle vist at elektroniske ID-kort er meget anvendelige. At det finnes standarder har gjort at det allerede i dag finnes et antall produkt og tjenester tilgjengelig på markedet. Eksempel på svenske virksomheter som i dag tilbyr produkt med elektroniske ID-kort er Telia (kortutstedelse, tjenester), Posten AB (kortutstedelse, tjenester), WM-data (kortutstedelse, produkter), Dynasoft AB (produkter), AU-system Ego (produkter), Siemens Nixdorf (produkter), Entegrity AB (Produkter) och Nexus AB (produkter). Foruten disse allerede ferdige produkter finns det et stort antall europeiske produkter som med liten innsats kan tilpasses til det norsk elektronisk ID-kort.

I Danmark har Dansk forskningsministerium valgt ut 9 offentlige etater og har bevilget DKR 15 mill. for å sette i gang utprøvinger, jfr. http://www.fsk.dk/fsk/presse/980630-1.html .

Aktuelle TTP-tjenester

Det finnes i dag norske virksomheter som tilbyr TTP-tjenester, men det ikke er gjort noen vurdering av disse fra arbeidsgruppens side. TTP-tjeneste brukes i ulike betydninger og med et potensielt stort marked.

Hver leverandør markedsfører sin tjeneste som er den bruker gjør avtale direkte med. For å realisere en PKI-løsning behøves viktige komponenter i infrastrukturen som

- en SertifiseringsAutoritet (SA) for utstedelse av sertifikat med åpne, offentlige nøkler
- en katalogtjeneste for lagring og distribusjon av sertifikat og tilbakekallingslister

For begge disse systemkomponenter finnes det ferdige løsninger i markedet.

I Norge

Det er flere aktører i det norske markedet som tilbyr sertifiseringstjenester i dag, mange av disse er bransjerelaterte eller de rene sikkerhetsløsningene for autentisering som leveres i Norge av Merkantildata/ProtectData. Vanligste hjelpemiddel i slike løsninger er engangs-passord/digipass/tokens. Diskusjonen begrenses i det neste til å gjelde de som tilbyr digitale signaturer og/eller kryptering.

Telenor har hatt i drift en TTP-tjeneste siden 1996, med blant annet Certification Authority (CA), Registration Authority (RA) og kortproduksjon. Tjenesten er etablert i Telenors kryptosenter (som er godkjent for krypto i forvaltningen av Forsvarets overkommando/Sikkerhetsstaben for det som angår rikets sikkerhet mv). Telenor Bedrift er engasjert i enkelte pilotprosjekter på ulike områder.

Innen helsesektoren er det i samarbeid med Kompetansenter for IT i helsesektoren (KITH) og applikasjonsleverandører for lege og apotek, utviklet løsninger for overføring av resepter

mellom lege og apotek. Systemet er satt i drift mellom Grünerløkka legesenter og Grünerløkka apotek.

Et annet prosjekt omfatter elektronisk utveksling av pasientinformasjon i forbindelse med overføring av utskrivningsklare pasienter. Aker sykehus og Bjerke bydel deltar som brukere av løsningen. Det er utviklet løsning for elektronisk saksbehandling basert på applikasjonene On-mail/On-file hvor TTP-tjenesten inngår som en sømløs sikkerhetsløsning i totalkonseptet. Prosjektet er planlagt videreført til også å omfatte andre behov for utveksling av pasientinformasjon mellom Aker sykehus og eksterne partnere.

Telenor gjennomfører høsten 1998 en omfattende oppdatering av den teknologiske plattformen, og planlegger å være på markedet med denne tidlig i 1999.

Ved Posten SDS er det i drift sertifikatsentral (Certfication Authority, CA). Sertifikatene følger X.509 standarden og publiseres i en offentlig katalog. Tjenesten inneholder også en sikker PC-modul (Local Registration Authority) som koples on-line mot sertifikatsentralen og utplasseres hos større organisasjoner for identifisering etter organisasjonenes egne sikkerhets-instrukser og utdeling av sertifikatbærere og PIN-koder. Sertifikater for privatpersoner vil bli tilgjengelige ved bestilling på postkontor av Postens ID-kort.

Fellesdata er tilbyder av sertifiseringstjenester med næringsliv som hovedmålgruppe og har en løsning under utprøving hos Statoil. Fellesdata har en dokumentert sertifiseringspolicy (CPA) og er også et sertifiseringsorgan for SET-basert elektronisk handel.

Løsningene til Fellesdata baserer seg på program- og maskinvare fra Software & Systems Engineering, et heleid selskap av Siemens Nixdorf Informasjonssystemer. Etter avslutning av pilotfasen skal løsningen evalueres med tanke på utplassering hos alle brukere som inngår i oljeselskapenes SOIL-prosjekt.

Fellesdata tilbyr sertifiseringstjenester på tre ulike nivåer og varierende styrke på algoritmer. En abonnementsordning tilbyr automatisk fornyelse av sertifikater hvert år.

Uninett har også en TTP-tjeneste som er åpent tilgjengelig for publikum og tjenesten drives av Norsk Regnesentral, men har ennå ikke mange nok brukere til å dekke utviklingskostnadene. Tjenesten benytter X.509v3 sertifikater og har også klientprogramvare som kan generere nøkler til bruk i sertifikater. Tjenesten har vært i drift i et par år. Meningen med tjenesten er å samle erfaring om problemer ved drift av TTP-tjenester.

Infrastrukturtjenestene tilbyr en sammensatt tjeneste under produktnavnet MultiSikkerhet. Det tilbys bl.a. brannmurtjenester mot Internett/andre, kryptering, digitale signaturer og tjenester for autorisasjon, autentisering og forsegling.

Det pågår arbeider i regi av kreditkortselskapene og bankene om nye tjenester, bla. sikker betalingsformidling, betalingskort, telebanking og flerapplikasjonskort. SET-sertifikater har inngått i ett pilotprosjekt, men for det meste betraktes disse nye tjenestene som sterkt konkurransefremmende og "kortene" holdes derfor tett til brystet før tjenestene lanseres.

Produkt- og tjenesteleverandører bør gi tilbud på tjenester som kan testes ut i en nasjonal PKI for næringsliv og offentlig forvaltning med bakgrunn i kravspesifikasjon i Forvaltnings-

nettprosjektet. En utfordring er å legge forholdene til rette rundt utprøvingen slik at man på bred basis får del i erfaringene som gjøres.

Noen eksempler på TTP-tjenester internasjonalt

På tjenestesiden vil utenlandske tjenesteydere på kort sikt neppe ha noen betydelig innflydelse på norske forhold. Samarbeidet i et utvidet NPSS (Nordic Post Security Services) medfører at sertifikater fra postverkene i Norge, Sverige, Finland, Danmark og Irland utgis av kryss-sertifiserte tjenesteytere. Foreløpig er det et svært smalt tilbud av applikasjoner hvor slike sertifikater kan benyttes. Det arbeides også i UPU (Universal Post Union) med utarbeidelse av et CPS-dokument (Certificate Practice Statement) slik at postverk som tilfredsstiller gitte sikkerhetsprofiler kan anerkjenne hverandres sertifikater.

SEIS - et svensk standardiseringsinitiativ

SEIS - Secured Electronic Information in Society er en svensk ideell organisasjon som arbeider for sikker digital kommunikasjon i åpne nett ved hjelp av åpne (offentlige) nøkkelsystem, sertifikat og aktive kort. Det er et mål at kommunikasjonen må skje på et sikkerhetsnivå som er akseptert av de fleste brukere og myndighetene. Akseptansen anses som en forutsetning for en utvikling i retning av sikker e-post, fjernarbeid og elektronisk handel i større omfang, og brukerne må kunne identifisere seg på en sikker måte.

SEIS har mange medlemmer blant de store IT- og industriaktørene i Sverige, bl.a. ABB, Nordbanken, IBM Sverige, Microsoft Sverige, Telia, Riksskatteverket, Rikspolisstyrelsen, Posten, Försvarsmakten. Medlemsavgiften er SEK 20.000 pr.år.

SEIS arbeider innenfor tre virksomhetsområder; kort, grensesnitt og regler og har resultert i følgende anbefalte spesifikasjoner:

- Elektronisk Identitetskort (EID-kort), www.seis.se/kort/normer/seis1v2.doc , Svensk Standard SS614330 - arbeidet er registrert i IETF som PKCS#15 Smart Card File Formats
- Sertifikat for EID-kort, www.seis.se/kort/normer/seis3v2.doc , Svensk Standard SS614331
- Implementasjonsprofil for EID, www.seis.se/kort/normer/seis4v2.doc
- Sertifikat politikk (Certification Policy) i SEIS, www.seis.se/kort/normer/S10_v10w60.doc

Produkter som blir utviklet i henhold til SEIS-spesifikasjonene vil tilby autentisering av avsender og innholdsintegritet, som kan verifiseres ved bruk av digitale signaturer, og beskyttelse mot uautorisert og ukontrollert aksess.

Vedlegg 5: Oversiktsscenario - Elektronisk samhandling - potensiale og utfordringer ....

Hensikten med denne teksten er å gi noen idéer om hva vi snakker om ved bruk av en annen fortellermåte enn den tørre, faglig orienterte. Nedenfor følger et scenario for elektronisk samhandling mellom innbygger, næringsliv og offentlig forvaltning der sikkerhetsaspekter blir anskueliggjort. Dette handler om man kan stole på hvem den elektroniske informasjonen kommer fra, og hvilken informasjon det er (autentisering), om man kan stole på at den ikke er

forandret underveis (integritet), og om man kan være sikker på at avsenderen ikke i etterkant kan benekte å ha sendt informasjonen (ikke-benekting), samt nyte godt av muligheten for å kunne bevise hva som faktisk er gjort (sporbarhet). I kapitel 3 er begrepene forklart noe nærmere. En advarsel: presisjonsnivået er ikke veldig høyt. Alt som sies er ikke nødvendigvis faglig »korrekt», verken etter dagens eller morgendagens målestokker. Det er kanskje heller ikke den historien som er mest treffende for de fleste behov eller fagområder. Men vi lar det stå til likevel!

Cecilie Lind hadde arbeidet hjemme hele dagen før hun satte seg ned ved sin nye arbeidsstasjon. Klokken var 19.45, drøyt fire timer igjen til årets selvangivelse skulle være registrert på likningskontoret og Cecilie Lind var fortsatt misfornøyd med deler av programvaren som fulgte med den nye maskinen. Ville hun rekke å laste ned ny internettprogramvare eller måtte hun satse på at den gamle gjorde jobben sin?

> Vennligst sett i personlig sikkerhetsmodul

Jovisst, sikkerhetskortet måtte nå benyttes hver gang hun skulle logge seg på maskinen. Det var et lite kort som minnet om de gammeldagse bankkortene, men det ble sagt at de var mye sikrere og erstattet hele bunten av kort som hun tidligere pleide å fylle lommeboken med. Hvordan kortet egentlig fungerte var ikke helt enkelt å forstå, men kortet inneholdt hennes hemmelige nøkler og var også i stand til å utføre viktige operasjoner.

Cecilie Lind satte sikkerhetskortet i den lille sprekken på tastaturet, tastet inn sin personlige kode og plasserte tommelen i fingeravtrykkfeltet på skjermen.

> *Cecilie Lind - Gyldig identifisering - Sikkerhetsmodul aktiv*

Figur 1: Scenario

Det var i grunnen ganske enkelt. Nå kunne hun koble seg direkte opp mot systemet på jobben eller mot hvilken som helst av de andre tjenestene på nettet som hun hadde abonnert på. Cecilie Lind tenkte med gru på alle de gamle brukernavnene og passordene som hun tidligere gikk rundt og husket på. Nå var det kun en kode, resten tok sikkerhetskortet seg av.

Så var det å finne den nye utgaven av internettprogrammet. Det var i grunnen ganske fint at Microscape la ut nye og bedre versjoner for gratis nedlasting. Eneste problemet var at programmene var blitt veldig store og det kunne ofte ta lang tid å hente programfilene direkte fra USA. Nå var det jo full arbeidsdag der borte og nettet var ofte litt tregt; skulle hun prøve programvaretjeneren på universitetet i Finland?

Et par museklikk og det nye programmet fløy fra universitetet i Finland og ned på hennes egen harddisk.

> *Verifisere program signatur? (J/N)*

Cecilie Lind klikket på Ja-knappen og ventet på at maskinen skulle finne fram verifikasjons-nøkkelen til Microscape. Det var i grunnen ganske fint at programvarehusene hadde begynt å

«signere» sine programmer. På den måten kunne vi være sikre på at vi hentet «ekte vare» på nettet.

> ADVARSEL - *feil i signatur. Installasjon avbrutt.*

Hva var dette? Noe var galt og Cecilie Lind unnlot å lagre det finske programmet på maskinen sin. Klokken var allerede over åtte, men det var tryggest å laste ned programmet direkte fra Microscape. Denne gangen gikk det glatt. Knapt 20 minutter senere var hun oppe med det nye programmet. Hun kunne lese senere på nettavisen at en virussmittet versjon av det nye Microscapeprogrammet var spredt over store deler av verden og mange brukere hadde mistet verdifulle data. Takket være signaturkontrollen hadde Cecilie Lind sluppet unna denne gangen.

Cecilie klikket seg fram til likningskontoret sin hjemmeside og gikk inn i området for utkast til selvangivelse. Her måtte hun oppgi sitt navn og personnummer. Det var litt skummelt, men hun var fortalt at sikkerhetskortet krypterte slike data før de ble sendt over nettet. Kort etter lyste likningskontorets forslag til årets selvangivelse opp på skjermen.

Punkt for punkt bladde Cecilie seg gjennom de ulike postene. Likningskontoret hadde samlet data fra ulike elektroniske registre og som ventet var det i overensstemmelse med hennes egne noteringer. Men hadde hun virkelig hatt 75 reisedøgn i fjor? Det måtte kontrolleres. Hun koplet seg opp mot regnskapssystemet på jobben og ved hjelp av sikkerhetskortet var hun raskt inne i «mappa si». Der stod det vitterlig 25 døgn! Cecilie endret likningskontorets 75 til 25. Så var det bare å bla seg fram til side fire. Hun klikket på feltet «Signer data». Den elektroniske selvangivelsen fløy inn i sikkerhetskortet, der ble den blandet med hennes hemmelige signeringsnøkkel til en unik personlig signatur. Sekunder senere lå den signerte selvangivelsen vel bevart i likningskontorets elektroniske system. I morgen kunne likningsfunksjonæren finne fram Cecilie Linds verifiseringsnøkkel i den nasjonale sertifikatkatologen. Frøken Lind hadde nok engang gjort sin borgerplikt.

Cecilie Lind pustet ut. Klokka var litt over elleve. Hva med litt nattmat? Hun åpnet hjemmesiden til «Nettpizza», valgte ut sin favorittpizza og klikket avgårde 570 kroner i «digitale kontanter». Ekte digitale kroner, signert av Den Norske Digitale Bank.

---

47 Websiden til EU om elektronisk handel finnes på: http://www.ispo.cec.be/ecommerce/

48 En pressemelding med opplysninger om Forumet finnes på: http://odin.dep.no/nhd/prm/1998/k3/980904.html

49 Rammebetingelser for elektronisk handel. Problemområder og problemstillinger knyttet til lov og regelverk for elektronisk handel. Nærings- og handelsdepartementet, november 1998. Se dokumentet og delta i høringen frem til 15. januar 99 på følgende webside: http://www.dep.no/nhd/publ/1998/ehandel/html

50 (ATM, Frame Relay, Leased lines, ISDN, GSM, POTS, Internet).

51 1) CoreHub Access:- tilgang til «backbone»- valg av aksess teknologi, kapasitet, og tele-leverandør 2) CoreHub Services: - E-mail (Internet SMTP, X.400, Lotus Notes, MS Exchange) - Sikker e-mail (X.509, S/Mime plug-in) - Katalogtjeneste (X.500 basert, LDAP klient / server) - TTP (X.509 sertifikatutsteder). Alle sikker e-mail brukere kan i tillegg få en komponent til Lotus Notes eller MS Exchange/Outlook

klienter for å benytte X.509 sertifikatene. Tett integrasjon med utviklingen av Internet er nødvendig (f eks. utveksling av mail, nye standarder, og Internet som aksess-teknologi).

52 X.509 versjon 3

53 (2048 bit RSA)

54 (128 bit TripleDES)

55 («Non-repudiation»)

56 (LDAP) og X.509).

57 Statskonsult Notat 1997:5, på oppdrag fra det daværende Plan- og samordningsdepartementet. I arbeidet deltok en bredt sammensatt gruppe fra offentlig og privat sektor, ledet av Statskonsult.

58 Til spesifisering av sikkerhetstiltakene knyttet man til seg Peter Landrock, Cryptomathic A/S. Han er i tillegg professor ved Århus universitet.

59 Med 56 bit nøkkellengde for kryptering og 1024 bit RSA-nøkkel for signering, sporbarhet og ikke-benekting - tidsstempling og logging evt. med bruk av digital signatur, konfidensialitet - kryptering av melding (basert på S/MIME v2 med PKCS#7 basert på EDIINT, på sikt med S/MIME v3)

60 Riksarkivet har høsten 1998 NOARK 4 ute til høring på http://www.riksarkivet.no/nyheter.html

61 Se oversikten på websiden: http://www.cordis.lu/infosec/src/study4.htm

62 En hashfunksjon utregner et fingeravtrykk eller en verdi ut av meldingsinnholdet

63 ISO/IEC WD14516 Information technology - Security techniques - Guidelines on the use and management of Trusted Third Party services

64 ISO/IEC WD15945 Information technology - Security techniques - Specification of TTP Services to support the Application of Digital Signatures

65 IT Security Evaluation Criteria (ITSEC) har vært i bruk i sentrale europeiske land på 90-tallet, og ledsages av IT Security Evaluation Manual (ITSEM), som beskriver rollefordelingen i en evaluering og en metodikk for gjennomføringen. Kriteriene og metodikken er anbefalt av EU i en Rådsrekommendasjon fra 1995. En avtaletekst for gjensidig anerkjennelse av sertifikater om evaluering av IT-sikkerhet er anbefalt av EUs Ministerråd i slutten av 1997, og konkret avtale mellom en rekke nasjoner er inngått våren 1998, der også Norge deltar i avtalegruppen.

66 Rådet for IT-sikkerhet, Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner, Sluttrapport 13 november 1997. Vær oppmerksom på at begrepet »sertifisering» her brukes i en annen betydning enn i denne rapporten. Forslagene i rapporten er noe mer omtalt nedenfor i pkt 12.2.2.

67 Samarbeidsgruppen Brønnøysundregistrene, Skattedirektoratet og Statistisk Sentralbyrå utarbeider felles kravspesifikasjoner i forbindelse med offentlig innrapportering.

68 Se bl a websiden: http://www.cordis.lu/infosec/home.html , som gir tilgang til EU's materiale på området.

Lagt inn 23 desember 1998 av Statens forvaltningstjeneste, ODIN-redaksjonen

Mandat for utredning av spørsmål vedr myndighetsroller og finansiering av ordninger for digitale signaturer og TTP-virksomhet

27.05.1999

Bakgrunn

Under behandling av den forberedende rapporten "Digitale signaturer gir tillit til elektronisk kommunikasjon – 30.11.98", uttalte Rådet for IT-sikkerhet at det er viktig å komme i gang med å klarlegge rammer og modeller for TTP-virksomhet i Norge. Rådet anbefalte overfor NHD at spørsmål vedr myndighetsroller, finansiering av autentiseringsvirksomhet, og godkjenningsordning og krav til TTP-virksomhet burde utredes nærmere. Som ledd i oppfølgingen på dette punktet nedsettes et utvalg med oppdrag å utrede nærmere de spørsmål som er angitt nedenfor.

Utredningens innhold

Utredningens innhold skal konsentreres om noen hovedspørsmål som reises i forbindelse med etablering av generelle rammebetingelser for bruk av sikker digital signatur i samfunnet. Flere av de angitte problemstillingene er berørt i rapporten om digitale signaturer. Utvalget skal mer utførlig gå inn i spørsmålene, ta hensyn til ny informasjon som evt måtte foreligge og angi mer presise forslag til anbefalinger. Utvalget skal legge til grunn de føringer som gis i EU-direktivet om felles rammeverk for elektroniske signaturer. Det forutsettes at utvalget i nødvendig grad innhenter synspunkter fra næringsliv/tjenesteleverandører.

Hovedspørsmålene som skal utredes omfatter:

1. **Frivillig godkjenningsordning for TTP-virksomhet og krav til slik virksomhet.**
   I rapporten om digitale signaturer anbefales at det etableres en frivillig ordning som tilbyr TTPer å operere i henhold til autorisasjon/godkjenning ut fra anerkjente kriterier, og at det etableres eller utpekes et offentlig eller privat organ som har ansvar for oppfølging og kontroll av TTPer som på frivillig grunnlag er blitt godkjent. I det kommende EU-direktivet pålegges dessuten landene å etablere tilsyn med TTPer som utsteder kvalifiserte sertifikater til offentligheten. Utvalget skal vurdere hvilket tillitsnivå som anses nødvendig for at TTP-virksomhet skal kunne anerkjennes rettslig, og med dette som utgangspunkt legge frem konkrete forslag til hvordan en frivillig godkjenningsordning og/eller tilsynsorgan kan etableres, helst med utgangspunkt i allerede etablerte ordninger. Det vises til utkast til "Direktiv om elektroniske signaturer, og Artikkel 3 og 5 spesielt".
2. **Anerkjennelse av sertifikater.**
   Flere leverandører av sertifikattjenester og eventuelt andre tjenester ventes å være i markedet. Utvalget skal legge frem 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 som eventuelt bør 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 skal 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** bør så langt mulig klarlegges.

Det vises bl.a. til følgende arbeider:

- Rapport om digitale signaturer, Rådet for IT-sikkerhet, 30.11.1998.
- Anbefaling fra Rådet for IT-sikkerhet til NHD vedrørende digitale signaturer og tiltrodde tredjeparter, Rådet for IT-sikkerhet 17.03.1999.
- Strategi for det videre arbeidet med digital signatur og TTP-virksomhet i Norge, Notat NHD x.x.1999.
- Grunnlagsdokument for elektronisk handel, NHD 1999.
- Kommende stortingsmelding om elektronisk handel. (Ventes fremlagt våren 1999)
- Det kommende EU-direktiv om felles rammeverk for elektronisk signatur, jf Kommisjonens forslag til slikt direktiv - COM(1998) 297 Final.
- Forvaltningsnettprosjektetets (FNS) anbudsmaterialet for Digitale signaturer og TTP-tjenester 18.02.99 og AADs erfaringer fra dette.
- AAD arbeidsgruppe for "identifikator- og navnespørsmål" ifm rammeavtaler om DS/TTP for Forvaltningsnettsamarbeidet. (Rapport med frist 1 juni 1999)

Sammensetning

Institutt for Rettsinformatikk – Olav Torvund, leder
FIN - (avventer navn, kontakt person u.dir. Torgeir Jonvik)
AAD - Katarina de Brisis
NHD - Jens Nørve
Post og teletilsynet – Arne Hestnes
Den norske Bankforening - Tore A. Hauglie
Hydro data - Øivind Lunde
Statskonsult sekretariat

Administrative forhold

- Utvalget velger selv arbeidsmåte og organisering.
- Utvalget gis et driftsbudsjett.
- Delutredninger kan innhentes, innenfor rammene av driftsbudsjettet.
- Utvalgets medlemmer honoreres etter satsene for utvalgsarbeid i staten. Oversikt over medgåtte timer utfylt på skjema for utvalgsarbeid sendes utvalgets sekretær.
- Reiser til utlandet skal forelegges departementet før de utføres.

Frist

Utvalget avleverer rapport til Nærings- og handelsdepartementet innen 31.12.1999. Avd. ledelsen i NHD har understreket at ingen forlengelse vil bli gitt, og ber om at arbeidet og møtte opplegget tilpasses dette fra begynnelsen.

Lagt inn 25. juni 1999 av Statens forvaltningstjeneste, ODIN-redaksjonen

Dato 26.05.99

Adressater i henhold til liste

Oppnevning av medlemmer til utredning av spørsmål vedrørende myndighetsroller og finansiering av ordninger for digitale signaturer og TTP-virksomhet

1. Oppnevning av medlemmer til utredningsgruppen

Vi viser til tidligere kontakt i saken.

Det vises videre til vedlagte;

- Utredningsgruppens mandat og sammensetning.
- Rapport om digitale signaturer, Rådet for IT-sikkerhet, 30.11.1998.
- Anbefaling fra Rådet for IT-sikkerhet til NHD vedrørende digitale signaturer og tiltrodde tredjeparter, Rådet for IT-sikkerhet 17.03.1999.
- Det kommende EU-direktiv om felles rammeverk for elektronisk signatur, jf Kommisjonens forslag til slikt direktiv - COM(1998) 297 Final.
- Blankett, ”Medlemmer til St. meld. nr.7” (må fylles ut av hver enkelt)
- Blankett, PM 14/98 ”Bestemmelser om godtgjøring til leder og sekretærer i statlige utvalg”

2. Innkalling til konstituerende møte.

Nærings- og handelsdepartementet innkaller til konstituerende møte i NHDs lokaler 23 juni, kl 11.00 til 14.00, i rom 6084, 6 etg. Det vil bli servert en enkel lunsj.

Til grunn for møte ligger de papirer som følger denne utsendelsen. Nærings- og handelsdepartementet v/ Avd dir. Eivind Jahren vil innlede og orientere om arbeidet. Det vil bli anledning til å stille spørsmål.
I andre del av møte, legges det opp til å diskutere og planlegge det videre arbeid. Gruppens leder Olav Torvund, vil her innlede.

Gruppens medlemmer bes sette av tid, før lunsj 28 juni, da det planlegges et seminar i AAD regi, hvor bl.a. Richard Schlechter fra DG XIII vil redegjøre for direktivet om elektronisk signaturer.

Med hilsen
Jan Fredrik Lockert (e.f.) avdelingsdirektør

Jens Nørve Rådgiver

Adresseliste:

Institutt for Rettsinformatikk
Postboks 6702 St. Olavs plass
0130 OSLO

FIN
Postboks 8008 dep
0030 OSLO

AAD
Postboks 8001 dep
0030 OSLO

Post- og teletilsynet
Postboks 447 Sentrum
0104 OSLO

Den norske Bankforening
Postboks 1489 Vika
0116 OSLO

Hydro Data
Drammensvn. 134
0277 OSLO

Statskonsult Sekretariatet
Postboks 8115 Dep
OSLO

Lagt inn 25. juni 1999 av Statens forvaltningstjeneste, ODIN-redaksjonen