INFRASTRUKTUR FOR SIKKER KOMMUNIKASJON - TTP-TJENESTER OG OFFENTLIG ENGASJEMENT

Jon Ølnes, Norsk Regnesentral (NR), NR Notat:OMNI/01/97, april 1997

1. INNLEDNING

Dette notatet er utarbeidet på oppdrag for Rådet for IT-Sikkerhet (RITS) og Planleggings- og Samordnings-Departementet (PDS), og diskuterer hvilke tjenester som kan inngå i en nasjonal infrastruktur for sikker kommunikasjon i nettverk, sett i en internasjonal sammenheng. Viktige spørsmål er hvordan disse tjenestene kan etableres, og hvordan og i hvor stor grad det er behov for offentlige godkjenningsordninger som akkreditering eller lisens. Vi forsøker både å diskutere forskjellige tjenester generelt, og å belyse med eksempler. Eksemplene vil typisk referere til dagens situasjon, og se på hvordan de samme rollene kan overføres til elektronisk kommunikasjon. I dette er det en underliggende forutsetning om at kommunikasjon «på nettet» vil foregå på tilnærmet samme måte som i dag, bare ved hjelp av andre medier. Det er for tidlig å si om dette faktisk er tilfelle på sikt, men i et litt mer kortsiktig perspektiv er nok forutsetningen riktig. Vi har derfor ikke tatt med spekulasjoner om framtidig utvikling av kommunikasjonsmønstre.

Oppbygging av en infrastruktur reiser spørsmål av teknisk, juridisk og politisk art. Dette notatet fokuserer i hovedsak på de tekniske utfordringene, men kan brukes som grunnlag for juridiske og politiske betenkninger. I en del tilfeller pekes det på områder som nødvendigvis må involvere jus og politikk.

Det er naturligvis svært begrenset mulighet for å gå i dybden av problemstillingene i et forholdsvis kort notat. Ambisjonene er heller å presentere noe nødvendig, teknisk bakgrunnsinformasjon, og så fokusere på en bred diskusjon med noe sentral informasjon på hvert punkt.

Dette notatet komplementerer i hovedsak RITS' arbeid innen sertifisering av IT-produkter, tjenester og systemer. «Sertifisering» er i det følgende gitt en mer omfattende mening.

Det er viktig å presisere at innholdet i notatet står for NRs, og ikke RITS', syn. Vi er klar over at innholdet kan være teknisk «tungt» for mange lesere.

2. BEHOV FOR INFRASTRUKTUR - KRAV TIL SIKKERHET

Behov for infrastrukturer kommer først og fremst fra behov for kommunikasjon mellom et stort antall aktører (skalerbare løsninger). Et lite antall aktører kan lett sette opp kommunikasjon seg i mellom, og et lite antall aktører som ønsker å kommunisere på en sikker måte, kan selv finne løsninger for dette.

Norge har i dag en god infrastruktur for konvensjonell telekommunikasjon, og en infrastruktur som kan understøtte framtidas avanserte telekommunikasjonstjenester, er under utbygging. Vi kan regne med at det om noen år i praksis vil være full dekning når det gjelder aksess til slike tjenester, ved at så godt som alle - privatkunder eller organisasjoner - er tilkoblet moderne nettverk.

Infrastrukturen vil bestå av et antall forskjellige, «offentlige» nettverk, som er koblet sammen slik at samtrafikk er mulig. Til dette vil det bli koblet enkeltstående maskiner eller (lokale) nettverk hos kundene. Nettverkene vil være av forskjellige typer, og kan bruke vanlige kabler, fiberoptikk, satellitter, radiobølger eller annen form for trådløs kommunikasjon.

Basert på denne infrastrukturen vil det bli tilbudt kommunikasjonstjenester av forskjellig slag, fra faste samband og «rå» båndbredde, til Internett-type tjenester.

Mye av den kommunikasjonen som vil foregå på disse nettverkene, vil trenge beskyttelse. I stor utstrekning vil dette være trafikk mellom vilkårlige aktører, som ikke kjenner hverandre på forhånd, og ikke har noen forhåndsavtale om hvordan denne kommunikasjonen skal foregå. Det mest nærliggende eksempelet er handel og betaling «på nettet».

Dette peker på et økende behov for en infrastruktur for sikker kommunikasjon. Når det gjelder handel og betaling på Internett, er behovet allerede i dag nærmest prekært. En slik infrastruktur må realiseres gjennom standardisering og gjennom TTP-tjenester (Tiltrodd Tredje-Part).

Sikkerhet kan karakteriseres ved fire parametre[1]:

- Tilgjengelighet er den egenskapen at tjenester / informasjon er tilgjengelig, med tilfredsstillende ytelse, for autoriserte brukere.

  Det viktigste tiltaket for tilgjengelighet er å sikre god kvalitet, stabilitet og tilstrekkelig kapasitet for maskiner, programvare, nettverk osv. Beskyttelse mot såkalte «nektelse av tjeneste angrep» kan kreve spesielle tiltak.

- Integritet (begrepet kvalitet brukes også her) betyr at informasjon ikke skal kunne endres / forfalskes / ødelegges av uautoriserte aktører. Det at komponenter i et system virker som de skal (jfr. virus o.l.), er også en del av integritetsbegrepet (og også viktig med tanke på tilgjengelighet).

  Det viktigste tiltaket for integritet er tilgangskontroll (fysisk og logisk) til systemer som lagrer og behandler informasjon. For informasjon som overføres over nettverk, vil kryptografisk integritetsbeskyttelse (som digital signatur) ofte være nødvendig. Systemintegritet kan kreve spesielle tiltak for å overvåke tilstand og aktivitet i systemet, f. eks. for å oppdage endringer.

- Konfidensialitet betyr at informasjon ikke skal være tilgjengelig for andre enn de den er ment for. Dette kan også gjelde for informasjon om aktiviteter, f. eks. hvem som handler med hvem.

  Som for integritet er tilgangskontroll til systemer det viktigste tiltaket. Kryptering av informasjon som overføres over nettverk, vil ofte være nødvendig. I helt spesielle tilfeller kan det være aktuelt med generering av falsk nettrafikk for å skjule aktiviteter.

- Sporbarhet er muligheten for å tilbakeføre en handling / hendelse til den ansvarlige i ettertid.

  Sporbarhet betyr å kunne framskaffe bevis av tilstrekkelig styrke for en påstand. Dette krever logging. I noen tilfeller vil en vanlig logg være tilstrekkelig. Sterke tjenester for sporbarhet (ikke-fornekting) krever bruk av digitale signaturer og/eller logging hos en TTP.

Tilgjengelighet vil ikke bli berørt i dette notatet, og det er vanskelig å tenke seg at det finnes noen TTP-rolle for å tilby økt tilgjengelighet. Det er imidlertid viktig å velge løsninger som sikrer at adgangen til TTP-tjenestene ikke blir flaskehalser som reduserer ytelsen for brukerne i unødig grad.

Krav til sikkerhet vil variere fra null til meget store. Det er vanskelig å tenke seg at en «offentlig» infrastruktur skal kunne understøtte de aller mest kritiske formene for kommunikasjon, men denne typen kommunikasjon vil vel heller ikke i særlig grad foregå over åpne nettverk. Imidlertid bør en infrastruktur kunne understøtte kommunikasjon med temmelig høye (i hvert fall i sivil målestokk) sikkerhetskrav. Det er verdt å merke seg at forskjellige aktører i en og samme kommunikasjonsinstans kan ha forskjellige, og kanskje til og med motstridende, krav til sikkerhet (f. eks. en kjøper og en selger ved handel).

Brukbar sikkerhet i åpne nettverk krever bruk av kryptografi. Det finnes rett og slett ikke noe alternativ, men til gjengjeld er det ganske mange alternative, kryptografiske løsninger. Sikkerhet krever også:

- Autentisering - bevis for at en oppgitt identitet er korrekt.

[1] De fleste publikasjoner bruker bare tre egenskaper, og nevner ikke sporbarhet. Dette er imidlertid en svært viktig egenskap i mange sammenhenger, og er ikke dekket av de andre parameterne.

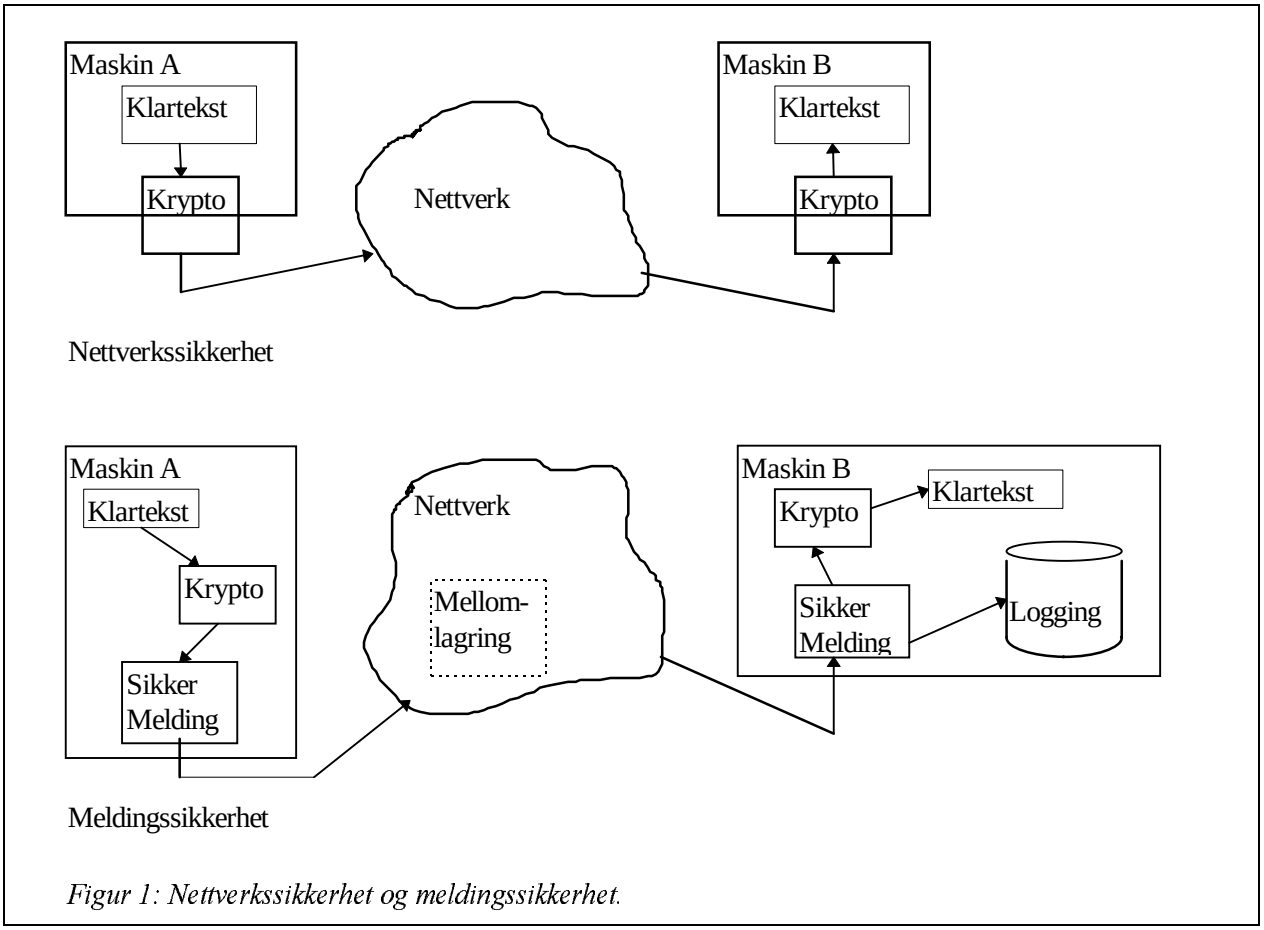
3. TEKNISK BAKGRUNN OG TILLIT

3.1 Nettverkssikkerhet og meldingssikkerhet

Det finnes to forskjellige tilnærminger til sikkerhet for utveksling av data (se Figur 1):

- Nettverkssikkerhet, der sikkerheten enten tilbys av nettverket selv som en tjeneste, eller av basis kommunikasjonsprogrammer på den enkelte maskin[2].
- Meldingssikkerhet, der det bygges opp en «sikker melding» hos avsenderen. Denne sendes over nettverket, uten at en trenger å stille noen krav til hvilken beskyttelse dette kan tilby, og meldingen kan «pakkes opp» etter at den er levert til mottageren.

Nettverkssikkerhet har den fordelen at dette kan tilbys transparent for brukerne, og med høy effektivitet. Ulempen er at det kun tilbys beskyttelse for data under selve overføringen. Siden nettverksinfrastrukturen vil bestå av en rekke forskjellige nettverk, vil sikkerhet tilbudt som en tjeneste fra nettverket ha en svært begrenset verdi. I praksis er en avhengig av at mottageren er tilkoblet samme nettverk for å være garantert at sikkerheten virker ende til ende. Sikkerhet kan i stedet legges i kommunikasjonsprogrammene på hver maskin, og en kan da kommunisere over usikrede nettverk.



Figur 1: Nettverkssikkerhet og meldingssikkerhet.

[2] F. eks. kan data krypteres i det de blir levert til nettverket, og dekrypteres i det de leveres til mottagermaskinen.

Meldingssikkerhet integrerer sikkerheten med dataene som kommuniseres. En sikker melding inneholder all informasjon som skal til for at mottager skal kunne verifisere den, i form av integritets- og konfidensialitets-beskyttelse (beskyttelse av bare utvalgte deler av meldingen er også mulig), og også digital signatur[3]. Meldingene bygges opp fra avsenderens brukerprogram (f. eks. epost program, men kan også være tekstbehandler o.l.), og pakkes opp fra mottagerens brukerprogram. Lagring av meldinger med beskyttelse er mulig, spesielt er dette viktig for sporbarhet ved lagring av signerte meldinger. Meldinger kan også trygt mellomlagres på vei fra sender til mottager, slik epost meldinger vanligvis blir. Ulempen er at det kreves integrasjon med de enkelte brukerprogrammene hvis ikke bruken skal bli for komplisert.

Framtidige kommunikasjonstjenester vil ofte være basert på multimedia. Lite forskning er gjort på beskyttelse av informasjon som bilder, video og tale som deler av multimediadokumenter, og på koordinering av beskyttelsen av forskjellige deler av ett slikt dokument.

I dagens situasjon vil det meste av informasjon som trenger beskyttelse, være i form av tekstdokumenter. Her er meldingssikkerhet nærmest påkrevet for å oppnå et skikkelig sikkerhetsnivå. En infrastruktur for sikker kommunikasjon i åpne nettverk må derfor støtte meldingssikkerhet.

Nettverkssikkerhet er eneste praktiske beskyttelsesmåte for enkelte typer trafikk, som sanntids video og tale. For annen trafikk er nettverkssikkerhet alene ikke tilstrekkelig til å støtte alle sikkerhetskrav, særlig når det gjelder sporbarhet og bruk av signaturer. Nettverkssikkerhet kan være et godt supplement for å sikre at all informasjon får en viss beskyttelse.

For lukkede brukergrupper kan nettverkssikkerhet være tilstrekkelig. Et eksempel er sammenknytting av lokalnett ved hjelp av rutere, der trafikken mellom ruterne er kryptert. En slik løsning er i forsøksvis bruk innen deler av offentlig forvaltning i dag, basert på den norske NSK kryptoalgoritmen.

I det følgende skal vi konsentrere oss om infrastruktur for utveksling av sikre meldinger.

3.2 Krav til standardisering

Kommunikasjon mellom et stort antall parter krever standardisering. Tilsvarende krever sikker kommunikasjon standardisering av sikkerhetsfunksjonene. For meldingssikkerhet gjelder dette:

- Meldingsformater, f. eks. EDIFACT sikkerhetsutvidelser og formater for sikker epost[4].
- Kryptoalgoritmer.
- Protokoller, f. eks. for kommunikasjon med TTPer.
- Sertifikater og annen representasjon av sikkerhetsinformasjon.

«Standard» i denne sammenhengen kan være internasjonale standarder (eksempler er X.509 sertifikater og EDIFACT meldingsformater), eller «de facto» standarder (eksempler er Internett RFC (Request For Comments) dokumenter). Det eksisterer for øvrig ikke offisielle, internasjonale standarder for selve kryptoalgoritmene.

I praksis vil det være et begrenset antall valgmuligheter innen de fleste av disse områdene, med bruk av standard identifikatorer for å angi f. eks. hvilke kryptoalgoritmer som er brukt. Programvare hos brukerne vil typisk kunne støtte et utvalg av alternativer. I mange sammenhenger er det viktig at TTP-tjenester er mest mulig generelle, og ikke knyttet opp til f. eks. bare bruk av enkelte kryptoalgoritmer eller meldingsformater.

---

[3] Digitale signaturer krever meldingssikkerhet. Det er i praksis umulig å få til et brukbart system for signering ved nettverkssikkerhet.

[4] Eksempler fra Internett er PEM (Privacy Enhanced Mail), S/MIME (Secure Multipurpose Integrated Mail Extensions), MOSS (MIME Object Security Services) og PGP (Pretty Good Privacy).

3.3 Om tillit og behov for TTPer

Sikkerheten i et system må utvikles med utgangspunkt i hva en velger å stole på i systemet. Det er teoretisk umulig å konstruere et sikkert system uten minst ett punkt som er definert som ubetinget sikkert.

Det er to aspekter av tillit, og det er formålstjenlig å skille mellom disse:

- Tillit til at aktørene i systemet følger spillereglene, f. eks. at varer som en har betalt for, faktisk blir levert. Dette kan vi kalle organisasjonsmessig tillit.
- Tillit til at aktørenes identiteter er korrekte, at systemet beskytter mot utenforstående, og at det ellers virker som det skal. Dette kan vi kalle teknisk tillit.

Tillit kan etableres ensidig (jeg stoler på banken min, men banken stoler ikke på meg) eller gjensidig (kunde og leverandør velger å stole på hverandre). Et begrenset antall aktører kan på forhånd utveksle informasjon - f. eks. hemmelige krypteringsnøkler - som seinere kan brukes til å etablere en sikker, autentisert kommunikasjonskanal.

Det er umulig å forhåndsetablere slike tillitsrelasjoner når et stort antall vilkårlige parter skal kunne kommunisere. Den generelle løsningen blir da å definere enkelte punkter i systemet som tiltrodde, og realisere disse gjennom TTPer. To parter som har etablert tillit til samme TTP, kan etablere tillit seg i mellom (vi stoler ikke på hverandre, men begge stoler på TTPen). I praksis vil det ofte være mer enn en TTP i systemet, men dersom TTPene etablerer tillit seg i mellom, kan en etablere en tillitskjede (chain of trust) mellom to parter som stoler på hver sin TTP.

De to aspektene av tillit gir opphav til forskjellige typer TTPer. TTPer for teknisk infrastruktur skal gjøre det mulig for vilkårlige parter å kommunisere sikkert. TTPer for organisatorisk infrastruktur skal gjøre det mulig for vilkårlige parter å samhandle om viktige saker - f. eks. saker av stor økonomisk betydning.

3.3.1 Organisasjonsmessig tillit og krav til sporbarhet

Avveininger angående hva en ønsker å kommunisere *om* (eller samhandle om) med den en kommuniserer *med* gjør vi i «vanlig» kommunikasjon, og dette avgjøres av hvor mye vi stoler på motparten.

Ofte krever tillit mellom aktører bare at man vet hvem motparten er (sikker autentisering). I noen tilfeller er ikke identiteten viktig, mens det i stedet kreves bevis for visse rettigheter, f. eks. for retten til å belaste en bankkonto eller et kredittkort. I andre tilfeller er identiteten ikke tilstrekkelig - vi handler ikke hus eller bil av hvem som helst. I disse tilfellene brukes det alt i dag TTPer, f. eks. som meglere eller tiltrodde forhandlere.

«På nettet» er det en del nye momenter å ta hensyn til:

- En kan ikke stole på det visuelle. Dersom en fysisk går inn i en forretning i en skummel bakgate, vet en noe om risikoen. Den samme forretningen kan framstå som meget tillitvekkende på nettet.
- Det at det fysisk eksisterer f. eks. en bankfilial eller et eiendomsmeglerkontor gir tilstrekkelig bevis på at vedkommende har rett til å opptre i denne rollen. På nettet må alle være forberedt på å kunne dokumentere at de kan ha en gitt rolle (akkreditering).
- Det kan være sterke krav til sporbarhet for at to parter skal velge å «gjøre forretninger». Sporbarhet er knyttet til mulighet for å bevise en hendelse, f. eks. at det er betalt, eller at en vare er levert. En klage har gjerne sjanser til å bli godtatt bare hvis sporbarheten er god. Lav tillit mellom aktører krever sterke mekanismer for sporbarhet.

Sporbarhet vil ved middels til høy tillit kunne realiseres gjennom logging av hendelser hos begge aktørene. Dette sikrer ikke mot at en av dem kan gå inn og manipulere loggen, og dersom noe ikke stemmer overens, blir dette en

påstand mot påstand situasjon. Sterke tjenester for sporbarhet vil bare kunne realiseres gjennom bruk av digitale signaturer[5].

En digital signatur kan vanskelig forfalskes, og framvisning av en signert melding vil være et meget sterkt bevis. Merk at meldingen må være tidsstemplet, og at det må føres bevis for at avsenderens signaturnøkkel var gyldig på dette tidspunktet[6].

For en del typer dokumenter er det lovfestet krav om signatur. Slike dokumenter kan ikke utveksles elektronisk uten digital signatur, men i så godt som alle tilfeller kan en digital signatur erstatte en håndskrevet.

3.3.2 Teknisk tillit og krav til sikkerhet

Et kommunikasjonssystem må ha to egenskaper:

- Det må oppfattes som sikkert (og fungere sikkert på den måten at det er liten sjanse for feil bruk).
- Det må faktisk være sikkert.

Ofte regnes det siste kravet som oppfylt dersom beskyttelsen mot utenforstående er god nok. Dette er ikke tilstrekkelig. I mange tilfeller er det nødvendig å kunne beskytte aktørene mot angrep fra hverandre.

De to egenskapene er til en viss grad uavhengige. Et usikkert system kan framstå som tillitvekkende, mens et sikkert system ikke nødvendigvis oppfattes slik. Den første egenskapen inneholder en konflikt mellom å gjøre sikkerhetsløsninger mest mulig usynlige for brukerne, og å formidle hva som faktisk skjer med hensyn på beskyttelse. Uansett er god integrasjon med brukerprogrammer det vesentligste.

Bruk av et system må være enkelt nok til at feil bruk bare kan forekomme ved uaktsomhet, og det må være helt klart hvilket ansvar den enkelte bruker har for å beskytte visse typer informasjon, som passord. Dette tilsvarer f. eks. krav til beskyttelse av PIN-kode ved bruk av bankkort.

Intet system kan være 100% sikkert. Hva som er «sikkert nok», vil variere fra anvendelse til anvendelse. Liten teknisk tillit vil føre til at kommunikasjon ikke kan finne sted.

4. TEKNISKE TTPer OG SERTIFIKATER

4.1 Oppgaven til en TTP

TTPer for teknisk infrastruktur realiserer tillitspunkter i nettverkene. TTPer produserer, validerer eller lagrer bevis for påstander. En påstand kan være «Jeg er NN» eller «Jeg har rett til å benytte bankkonto xxxxx» eller «Jeg har sendt melding M på tidspunktet T». Som en del av dette kan TTPer gis ansvaret for å produsere visse typer informasjon (eksempel krypteringsnøkler), eller lagre eller formidle informasjon mellom aktører.

4.2 Kommunikasjon med TTPer

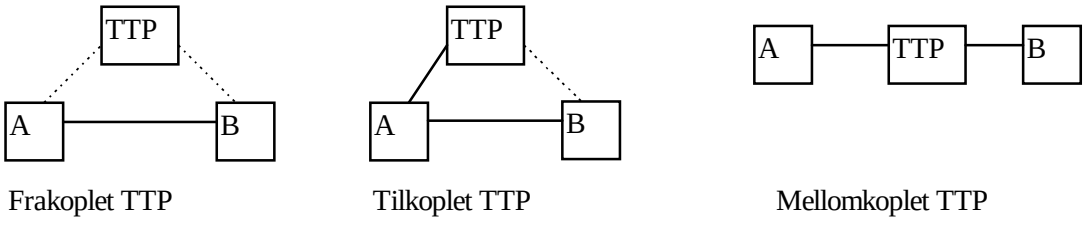
TTPene vil i varierende grad være direkte involvert i kommunikasjonen mellom partene. Teknisk sett kan TTPer med hensyn på kommunikasjon være (se Figur 2):

---

[5] Det eneste alternativet er logging hos en TTP. I praksis vil en slik løsning bare bli brukt ved helt spesielle meldinger, som f. eks. kontrakter, og i tilfelle kombinert med digitale signaturer. En slik TTP vil ha rolle som elektronisk notar, men en megler kan ha en slik rolle ved visse former for handel. Dette diskuteres seinere i notatet.

[6] Den vanligste metoden for å benekte en handling er antagelig å utføre handlingen og signere på dette, for så kort tid etter å rapportere signaturnøkkelen som kompromittert.

- Frakoplet (off-line) - deltar ikke i kommunikasjonen, men partene er avhengige av at TTPen har produsert sine bevis på forhånd.
- Tilkoplet (on-line) - partene kommuniserer med hverandre, men en eller begge parter er også avhengige av å kunne kontakte TTPen underveis, eller i hvert fall i starten av kommunikasjonen.
- Mellomkoplet (in-line) - all kommunikasjon mellom partene går gjennom TTPen.



Figur 2: Kommunikasjon med TTPer.

Tilkoplede TTPer for produksjon av bevis vil skape flaskehalser i systemet, og det vil være meget komplisert å etablere nettverk av TTPer, noe som er nødvendig av hensyn til skalering (se nedenfor om sertifiseringshierarkier). En teknisk infrastruktur for meldingssikkerhet, som skal omfatte et stort antall brukere og organisasjoner og et stort antall nettverk, også internasjonalt, må derfor i hovedsak baseres på frakoplede TTPer. Disse TTPene skal forhåndsprodusere bevis med en viss gyldighetsperiode. Slike bevis er tilstrekkelig til at en sikker kommunikasjonskanal kan etableres, forutsatt at aktørene stoler på bevisene, dvs. på TTPen.

Tilkoplede og mellomkoplede TTP-tjenester vil bare bli brukt i spesielle tilfeller, der frakoplede TTPer ikke kan gi tilstrekkelig tillit. Et eksempel på en tilkoplet tjeneste kan være en garantert tidsstempling av meldinger. Et eksempel på en mellomkoplet TTP kan være en tjeneste som logger alle meldinger mellom to parter. En tilleggstjeneste kan være å garantere anonymitet for hver av partene overfor den andre.

Selv en frakoplet TTP vil som regel tilby tjenester. En sertifiseringstjeneste (se nedenfor) vil ha en database over de sertifikatene den har utstedt, der «kunder» kan hente sertifikater etter behov. Disse tjenestene trenger ikke å være tiltrodde i TTP-forstand, men vil være rene informasjonstjenester.

4.3 Sertifikater og sertifiseringsautoriteter

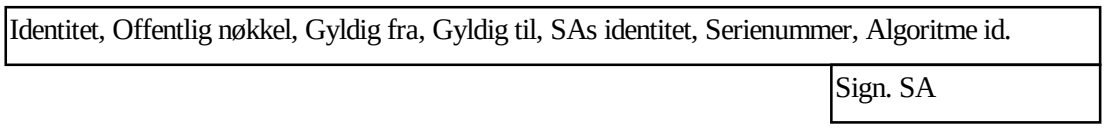
En frakoplet TTP opererer som en sertifiseringsautoritet[7] (SA). Et sertifikat er en «melding» signert av en SA. Det vanligste er identitetssertifikater, som direkte kan sammenlignes med fysiske legitimasjonskort. Et slikt sertifikat inneholder en identitet[8], en offentlig krypteringsnøkkel[9], identiteten til SAen, et tidsintervall som angir gyldighetsperiode, pluss noe mer informasjon som er nødvendig for å behandle sertifikatet (se Figur 3). SAen signerer over koblingen mellom oppgitt identitet og offentlig nøkkel.

---

[7] Det finnes teknologi for «on-line sertifisering» av identiteter og rettigheter, i hovedsak basert på Kerberos systemet. Slike systemer brukes gjerne internt i en organisasjon, men det er vanskelig å se for seg hvordan en større, nasjonal og internasjonal, infrastruktur skal kunne bygges på denne måten, spesielt p.g.a. krav til tilgjengelighet og ytelse, men også p.g.a. krav til sikkerhet i drift av en on-line tjeneste.

[8] Vanligvis virkelig identifikasjon av en person, men kan også være f. eks. bedrift, organisasjon, gruppe, rolle , pseudonym, datamaskin, program, osv. osv.

[9] Sertifisering av denne typen forutsetter bruk av offentlig nøkkel kryptografi. For denne typen kryptoalgoritmer har hver bruker to nøkler, en offentlig som hvem som helst kan kjenne, og en privat som bar er kjent av brukeren selv. Algoritmene har den karakteristikken at informasjon kryptert med privat nøkkel, bare kan dekrypteres med den tilsvarende offentlige nøkkelen. Dette gir autentisering av avsender ved at det bare er denne som kan ha produsert den krypterte teksten, og dataintegritet ved at ingen kan endre den krypterte meldingen uten at dette blir oppdaget - disse egenskapen er karakteristiske for en digital signatur. Dette gir ikke konfidensialitet, siden hvem som halst kan få tak i den offentlige nøkkelen. De fleste offentlig nøkkel algortimer er reversible, d.v.s. at informasjon kryptert med en offentlig nøkkel bare kan dekrypteres med den tilsvarende private nøkkelen. Dette brukes til å oppnå konfidensialitet, siden bare tiltenkt mottager kan dekryptere.



Figur 3: Struktur på X.509 sertifikat.

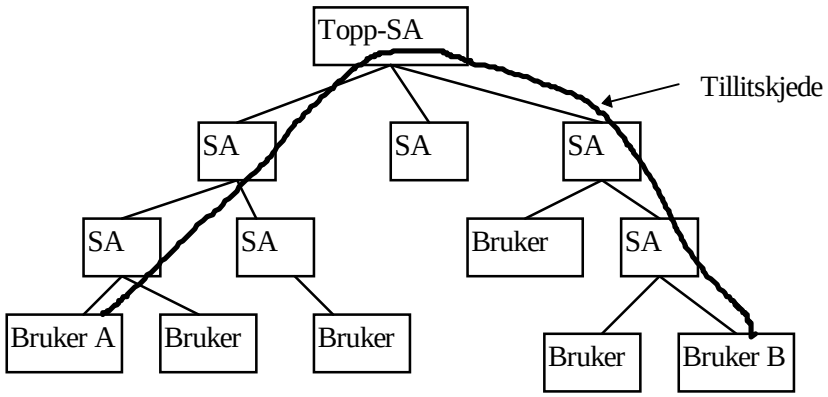
En annen type sertifikat angir rettigheter. Her kan SA signere over en kobling mellom en identifikasjon av den ressursen det gis rettigheter til, og en offentlig nøkkel, uten noen identitet for brukeren. Et eksempel er retten til å disponere en bankkonto, i form av et sertifikat med kontonummeret knyttet til en offentlig nøkkel. Andre rettighetssertifikater kan binde sammen en identitet og en rettighet, og disse må da brukes sammen med identitetssertifikater. Ett eksempel er et «bevillingsbrev» for å autorisere en aktør for en gitt rolle, som f. eks. eiendomsmegler. Dette diskuteres seinere i notatet. Som et annet eksempel kan en bedrift sertifisere signaturrettigheter for noen av sine ansatte.

Et sertifikat inneholder kun helt åpen informasjon, men det er umulig å endre informasjonen siden dette er en signert melding. Et sertifikat kan derfor utveksles og oppbevares på vilkårlige måter. Det finnes et standard format for sertifikater, definert i X.509[10]. Dette formatet bør benyttes av alle SAer, noe som også skjer i praksis i dag.

En identitet (eller en rettighet) bevises ved signering av en melding med privat nøkkel. Et sertifikat knytter den tilsvarende offentlige nøkkelen sammen med identiteten (eller rettigheten). Hvis meldingssignaturen kan verifiseres med den offentlige nøkkelen, og signaturen på sertifikatet kan verifiseres, er identiteten ansett som bevist.

4.4 Sertifiseringshierarkier - hvordan kan en stole på en TTP?

Verifisering av SAens signatur på et sertifikat gjøres med SAs offentlige nøkkel. Det betyr at en trenger å knytte denne nøkkelen sikkert til SAens identitet, på samme måte som brukernes offentlige nøkler må knyttes til deres identitet gjennom sertifikater. Sertifikater kan da også brukes ved at SAen har et vanlig X.509 sertifikat som er utstedt av en SA «på høyere nivå». Denne SAen kan i sin tur også ha et sertifikat osv. (se Figur 4), men det er klart at toppnivået i et slikt hierarki ikke kan sertifiseres av noen.



Figur 4: Sertifiseringshierarki og tillitskjede

[10] X.509 er en del av standardene for katalogsystemer, utarbeidet i fellesskap av Den Internasjonale Standardiseringsorganisasjonen (ISO) og den Internasjonale Telekommunikasjonsunionen (ITU). Det finnes flere versjoner av X.509 standarden. Den siste er versjon 3 (X.509v3), og alt tyder på at denne vil få fullt gjennomslag. X509v3 gir muligheter for «private» utvidelser, som f. eks. kan referere til de betingelsene som gjelder for utstedelse av et sertifikat, eller på annen måte angi «nivået» på sertifikatet.

Topp-SAs offentlige nøkkel må distribueres utenom systemet, på en slik måte at det ikke kan være noen tvil om at den er korrekt. Dersom en skal fullt ut verifisere et sertifikat for en bruker, må en verifisere alle sertifikater for SAer «mellom» brukeren og topp-SA.

Det finnes for øvrig andre sertifiseringsstrukturer enn hierarkiske[11], men generelt er hierarkiske strukturer de eneste som virkelig kan skalere til store størrelse.

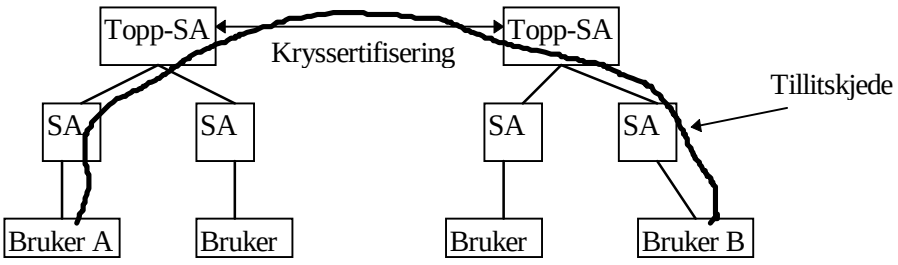
Den enkelte bruker har et forhold til, og stoler på, den SAen som har sertifisert ham/henne, og må også kjenne til og stole på alle SAer opp til topp-SA når det gjelder sin egen sertifisering. I praktisk bruk må en også stole på alle andre SAer i systemet når det gjelder at deres utstedelse av sertifikater er korrekt. Det etableres en tillitskjede mellom to brukere, gjennom alle mellomliggende SAer (se Figur 4).

Dette er basert på at tillit regnes som en transitiv egenskap - når en TTP jeg stoler på, går god for en annen, så stoler jeg også på den andre TTPen. Dersom tillit var en «binær egenskap» (enten 0 eller 100%) ville dette være korrekt. I praksis vil lange tillitskjeder redusere tilliten til et system.

Det er derfor et poeng å redusere «dybden» av sertifiseringshierarkier. Stor dybde gir tunge beregninger (mange sertifikater som skal verifiseres) og mange SAer som en skal stole på. Liten dybde gir SAer med meget stort virksomhetsområde og kanskje liten nærhet til brukerne.

Det er mulig for SAer å kryssertifisere hverandre ved at begge utsteder et sertifikat for den andre. Slik kan en lage snarveier i hierarkiet. Dette gjør det også mulig å koble sammen uavhengige hierarkier ved at topp-SAene kryssertifiserer hverandre (se Figur 5). Kryssertifisering under toppnivå mellom hierarkier er sjelden ønskelig.

De første spesifikasjonene for et sertifiseringssystem for Internett gikk ut på å samle alt under en felles topp-SA, kalt IPRA (Internet Policy Registration Authority). Det kan se ut som om dette likevel ikke vil bli trenden i



Figur 5: Separate sertifiseringshierarkier og kryssertifisering.

framtida. I stedet går utviklingen heller i retning av «flate» (eller «grunne») hierarkier for spesifikke formål, og med separate topp-SAer. Slike hierarkier kan kobles sammen ved at de kryssertifiserer hverandre.

Som ett eksempel kan norske banker sertifisere sine kunder (elektronisk bankkort). Hver bank vil ha sin SA. I utgangspunktet kan hver bank operere sitt eget «hierarki», bestående kun av en topp-SA. Bankene kan få til samtrafikk ved at de kryssertifiserer hverandre, eller ved at det opprettes en overbygning i form av en «nasjonal» SA som sertifiserer alle banker (etter visse retningslinjer).

For internasjonal operasjon kan den nasjonale SAen i sin tur underordnes en europeisk SA for banker, eller en verdensomspennende SA. Eventuelt kan bankene selv legge seg inn under slike internasjonale SAer direkte. For internasjonal operasjon blir kryssertifisering upraktisk fordi antallet banker blir altfor stort. For et eksempel på et slikt sertifiseringshierarki, se avsnitt 6.3 og Figur 6 i dette notatet.

[11] PGP (Pretty Good Privacy) bruker det som kalles «web of trust» modell, der brukerne signerer hverandres nøkler. Dette gir etter vår oppfatning for liten tillit dersom systemet skal brukes ut over en liten mengde brukere.

SAer opererer etter sertifiseringsregler (certification policy) som angir hvilke prosedyrer som skal gjennomgås når et sertifikat skal utstedes, og hvilke krav som skal være oppfylt. En annen grunn til å ha separate hierarkier er at sertifiseringsregler kan være svært forskjellige. Dersom en mener at en SA ikke har forsvarlige regler, vil en ikke godta sertifikater som denne har utstedt[12]. Dette er lettest dersom alle SAer innen et hierarki har noenlunde samme sertifiseringsregler, slik at dersom en kan verifisere et sertifikat, så vet en samtidig at en kan stole på det[13].

5. TTP-TJENESTER FOR ORGANISATORISK TILLIT

5.1 Innledning

Organisatoriske TTP-roller er forholdsvis vanlige i vår fysiske hverdag, selv om vi i mange tilfeller ikke tenker på dem som TTPer. De fleste av disse rollene inngår i verdikjeder for (sam)handel. Grunnen til at disse tjenestene behandles spesielt er at de ikke er nødvendige deler av en infrastruktur for sikker *kommunikasjon*. Men tjenestene er nødvendige (eller i hvert fall ønskelige) for elektronisk *samhandel*.

5.2 Bevillingsbrev

For elektronisk kommunikasjon må aktører være forberedt på å bevise at de har lov til å ha visse roller, som eksempel eiendomsmegler, bank, advokat og annet som er underlagt betingelser i henhold til lover og regelverk. Dette kan oppnås gjennom rettighetssertifikater, som typisk vil utstedes (på vegne) av samme instans som utsteder fysiske bevillingsbrev. Dette vil oftest være en offentlig instans, eller i noen tilfeller kanskje en bransjeforening. Det må utredes hvilke roller som trenger bevilling, og om alle disse er dekket av eksisterende lover og regelverk.

Et slikt sertifikat vil kunne brukes i digitalt signerte vedlegg til all forretningsrelatert korrespondanse, på samme måte som en i dag bruker firmaets brevark, eller sertifikatet kan gjøres tilgjengelig f. eks. gjennom Web-sider. Ofte vil en bevilling gi rett til å inneha en organisatorisk TTP-rolle, se nedenfor.

Et system for elektroniske bevillingsbrev krever offentlig koordinering for å sikre at systemet virker som det skal, og for å ivareta posisjonering i forhold til utlandet. Bevillingsbevis må kunne brukes internasjonalt, ved at norske utstedere posisjonerer seg i et internasjonalt sertifiseringshierarki. En fornuftig organisering kan være en norsk toppnivå-SA, f. eks. under Norsk Akkreditering. Det er mulig å la en SA sertifisere for forskjellige roller, men det kan være ønskelig å ha et antall under-SAer for spesifikke formål. Under-SAer kan i tilfelle drives av andre instanser, som bransjeforeninger.

Det finnes andre, tilsvarende områder. Ett eksempel kan være elektroniske vitnemål (og bevis for oppnådd akademisk grad), som kan utstedes av universiteter og høgskoler, og av videregående skoler.

5.3 TTPer for samhandel

«Prototypen» på en slik TTP er en megler som formidler handel. Vi antar at de samme rollene i stor grad vil bli videreført ved elektronisk kommunikasjon, men kun erfaring vil vise om denne antagelsen er riktig. Det er lite som tyder på at roller vil forsvinne, men nye roller kan komme til, som f. eks. TTPer for godkjenning av programvare.

---

[12] NR har i sitt arbeid med sertifiseringsregler konkludert med at det generelt er nødvendig med personlig frammøte og (fysisk) legitimering for å få utstedt et sertifikat. Det finnes tjenester som tilbyr utstedelse av sertifikater bare etter «elektronisk» kontakt. Dette tilsvarer omtrent at en kan ringe eller sende brev for å få utstedt en fysisk legitimasjon.

[13] Det arbeides med sertifiseringssystemer der SAer innen samme hierarki kan ha forskjellige sertifiseringsstrategier. Dette gjøres ved at en sertifiseringsstrategi gis en identifikator (f. eks. et nummer) som inkluderes i sertifikatene. Etter at sertifikatet er verifisert må en da sjekke mot lokal informasjon om denne identifikatoren er i lista over akseptable sertifiseringsstrategier. Det gjenstår å se om et slikt system vil virke i praksis.

Foreløpig tyder studier[14] på at f. eks. en megler ved elektronisk kommunikasjon vil ha omtrent de samme oppgaver som i dag.

Det finnes en rekke andre eksempler på organisatoriske TTP-roller, som kredittopplysningsbedrifter, advokater, banker og kredittinstitusjoner, forsikringsselskaper, takstmenn osv. En rekke slike roller innehas av offentlige eller offentlig eide instanser, som politi og lensmenn, sorenskrivere, Brønnøysund-registerne mm. Typisk inngår slike roller i verdikjeden for samhandel mellom andre aktører.

I svært mange av disse rollene vil bevilling være nødvendig, eller for offentlige instanser et tilsvarende bevis på at rollen er korrekt. Når det gjelder selve operasjonen av tjenesten, antar vi at dette ofte vil være dekket av eksisterende lover og regelverk, men dette må undersøkes for hvert enkelt tilfelle. Det kan også være aktuelt med tilleggskrav, f. eks. når det gjelder sikkerhetsnivå for å kunne tilby visse tjenester elektronisk.

5.4 Betalingsformidling

Banker og kortselskaper opptrer som TTPer som garanterer overføring av penger mellom parter. Også for elektronisk handel og betaling (se diskusjon nedenfor) vil denne rollen være viktig. Banker trenger konsesjon for å operere, og eksisterende regelverk skulle dekke også deres operasjoner innen elektronisk betalingsformidling. Når denne rollen nevnes spesielt her, er det fordi den er spesielt sentral for kommersiell virksomhet, og den kan være økonomisk meget lukrativ etter hvert som volumet på elektronisk handel øker.

Allerede i dag ser vi at selskaper som opererer markedsplasser på Internett, uttaler at de gjerne også skulle ha kontroll over betalingsformidlingen. Nå er det ikke gitt at den beste løsningen i et nytt marked er å gi et monopol til eksisterende aktører som banker og kortselskaper, men det er grunn til å være på vakt mot useriøse aktører.

Selv om kortselskapene i Norge er eid av bankene, er det også på sin plass å se på forholdet mellom kortbruk og banktransaksjoner. Tekniske løsninger for betaling over nettverk kommer som regel fra USA, og er primært rettet mot bruk av kredittkort. Norge har et meget velfungerende banksystem med et godt samarbeid om transaksjoner mellom banker. For norsk næringsliv vil det være en fordel om dette kan videreføres innen elektronisk handel. Alternativet er et langt større volum på kredittkorttransaksjoner (foreslåtte systemer er ikke så godt tilpasset debetkort), og, uansett norsk eierskap, mer makt til de internasjonale kortselskapene.

5.5 Notartjenester og logging

Med notartjenester menes vanligvis offentlige tjenester for autorisering og oppbevaring av dokumenter. Disse tjenestene kan i svært mange tilfeller videreføres for elektroniske dokumenter og digitale signaturer. Det finnes mange tilfeller der lover og regelverk stiller krav om signatur, men kun en håndfull paragrafer i Norges Lover der det eksplisitt stilles krav til *håndskrevet* signatur[15]. I alle andre tilfeller skal en digital signatur være tilstrekkelig til å oppfylle lovbestemte krav.

For elektronisk kommunikasjon kan notarbegrepet gis et litt utvidet innhold. Det er en kjensgjerning at elektroniske dokumenter (uten signatur vel og merke) er svært mye lettere å manipulere enn papirer. I en del tilfeller kan det da være ønskelig å lagre kopi av korrespondansen, eller i hvert fall logge kommunikasjonen, hos en tredjepart. EDI-leverandører gjør dette alt i dag, og det kan tenkes at Internett-leverandører også vil kunne tilby slike tjenester.

Merk at det er seriøse avveininger her med hensyn på personvern. For så vidt er dette et spesialtilfelle av all den logging som foregår i datasystemer, av sikkerhetsmessige og andre årsaker. Det finnes temmelig mange slike «personregistere» rundt omkring, og de færreste har tenkt på konsesjon eller godkjennelse fra Datatilsynet. For

---

[14] F. eks. ved Norsk Regnesentrals ELCOM prosjekt om elektronisk eiendomsmarked, http://www.nr.no/home/gem/ELCOM

[15] Ref. Andreas Galtung ved Institutt for Rettsinformatikk. Dette er som regel tilfeller der det er sterke krav til dokumentets form i tillegg til kravet om signatur. Eksempler er testamente og vielsesattest.

vårt spesialtilfelle er det viktig at dette er en tjeneste som bare brukes når den etterspørres, slik at aktørene selv godkjenner loggingen.

Ved mange transaksjoner er den viktigste rollen til en megler eller advokat å oppbevare en kopi (eller originalen) av dokumenter. Igjen er dette en rolle som kan overføres direkte til elektroniske dokumenter og digitale signaturer, og antagelig uten nevneverdige endringer i lover og regelverk.

5.6 Markedsplasser

Vi ser i dag at selgere og tjenestetilbydere i et elektronisk marked samles i «elektroniske kjøpesentere», eller markedsplasser. Markedsplassene drives i dag i hovedsak av Internett-leverandørene, men andre aktører er på vei inn, som aviser (annonsering med direkte kobling mot selger) og «gule sider» (kataloger med direkte kobling mot selger). Den viktigste motivasjonen for selgere er tilgjengeligheten i forhold til kundene.

Samtidig opptrer mange markedsplasser som en slags TTPer. Selv om ingen markedsplass vil kunne garantere for sine selgere, vil en siling være nødvendig. Markedsplasser med useriøse selgere vil fort miste posisjon. Dette vil antagelig føre til at kunder primært velger å handle med selgere som tilbyr sine tjenester på seriøse markedsplasser. Det er neppe aktuelt med noe offentlig engasjement her.

5.7 Evaluering av programvare, utstyr og systemer

Et velkjent sitat om IT-sikkerhet er: «Sikkerhetstiltak brytes ikke, de omgås». Vellykkede angrep er som regel ikke basert på å knekke krypteringsnøkler o.l., men på å forsøke å utnytte sikkerhetshull i programmer og systemkonfigurasjon, eller på utnyttelse av programmer med bivirkning[16]. Dårlig systemkonfigurasjon og feil i programmer er også de største truslene mot tilgjengelighet av systemer.

Vår påstand, som deles av andre[17], er at sertifisering på komponentnivå, slik eksisterende kriterier (TCSEC, ITSEC, ISO evalueringskriterier) foreskriver, ikke er noen løsning annet enn for helt spesielle komponenter / anvendelser. Evalueringskriterier må i langt større grad ta hensyn til komponentenes omgivelser, og spesielt menneskelige og systemmessige faktorer.

I dette ligger at kriteriene er dårlig egnet for annet enn sentraliserte systemer (som kan sees på som en enkelt komponent), mens en typisk trend lenge har vært distribuerte programsystemer i nettverk. Formell evaluering er meget ressurskrevende, og dermed dyrt. Systemene blir svært statiske, ved at oppgraderinger kan føre til behov for ny evaluering. Både p.g.a. vanskeligheter rundt oppgradering, og p.g.a. at en evaluering ofte kan ta meget lang tid, kan evaluerte systemer ofte ikke bruke siste (og funksjonelt beste) versjon av programvare. Dette kan også føre til problemer med støtte fra leverandører.

Dagens formelle kriterier er godt egnet til evaluering av enkeltstående komponenter, som f. eks. brannmurer for tilkopling til åpne nettverk. De har også sin misjon for komponenter med svært høye sikkerhetskrav, der en sentralisert løsning gjerne uansett er en nødvendighet. Det er derfor absolutt et behov for TTP-tjenester for formell evaluering. En slik tjeneste må kunne utføre egne evalueringer, og også kunne vurdere evalueringer foretatt av andre, f. eks. tilsvarende tjenester i andre land. En akkreditering av evaluatorene er meget ønskelig, tilsvarende som for evaluatorer for kvalitetssikring og revisjon. Det finnes allerede et par bedrifter i Norge med evaluering etter formelle kriterier som forretningsområde. Produktkataloger over evaluerte produkter er ønskelig.

---

[16] Som et eksempel: For sikkerhet av digitale signaturer fokuseres det vanligvis på styrlen til nøkler og kryptoalgoritmer. En langt større trussel er programmer som endrer informasjonen mellom det brukeren ser på skjermen og den representasjonen av dokumentet som faktisk blir signert. Brukeren tror hun signerer over skjermbildet, mens signaturen i virkeligheten blir beregnet over manipulert informasjon.

[17] Utsagnet som følger er nærmest ordrett sitert fra Ross Andersons klassiske artikkel «Why Cryptosystems Fail», http://www.cl.cam.ac.uk/ftp/users/rja14/wcf.ps.gz

Vi ønsker imidlertid å påpeke farene ved å overdrive bruken av formelle evalueringskriterier. Ved høye sikkerhetskrav, der administrativ og fysisk sikkerhet og en skikkelig sikkerhetsstrategi også er på plass, hører evaluerte systemer absolutt hjemme. I de fleste tilfeller, også innen det offentlige, er det helt andre sikkerhetstiltak enn formell evaluering som skal til i dagens situasjon. En fokus på formell evaluering vil føre til føre til unødige kostnader for systemene, og for stor vektlegging av teknisk datasikkerhet i forhold til administrativ sikkerhet.

Når dette er sagt: Teknisk datasikkerhet er selvfølgelig svært viktig. Men et tilfredsstillende sikkerhetsnivå (sett i forhold til kostnader) kan i de fleste tilfeller oppnås ved «vanlige» systemer, forutsatt ryddig og god systemkonfigurasjon og forsvarlige driftsrutiner. Også slike systemer bør evalueres, men da som en mer skjønnsmessig evaluering, og ikke formelt. Hjelpemidler kan være beskrivelse av standardkonfigurasjoner og retningslinjer for drift. Evaluatorer kan være samme type firma som gjør formelle evalueringer, eller evaluering kan inngå i en IT-revisjon[18]. Evalueringen må omfatte både systemtekniske sider og sikkerhetsstrategi (se nedenfor), og kan være basert på håndbøker og retningslinjer for «best practice». Som noen eksempler på viktige punkter kan vi nevne:

- Mest mulig enkel og ryddig systemkonfigurasjon og ingen annen funksjonalitet enn den som er nødvendig,
- mest mulig feilfritt system og gode rutiner for feilretting,
- forsvarlige rutiner for drift, vedlikehold og overvåking av systemet, inkludert sikkerhetskopiering.

Godkjenning av programvare i en slik sammenheng vil kunne gjøres etter en enklere vurdering enn en formell gjennomgang. Både feil og ondsinnede bivirkninger kan være meget vanskelig å oppdage i programmer. En mindre formell godkjenning må gi et grunnlag for å vurdere om programvaren er til å stole på ved at stabiliteten (kvaliteten) er tilfredsstillende, og at det er liten sannsynlighet for at det er lagt inn bivirkninger. Det er fornuftig å publisere offisielle lister over formelt sertifiserte produkter siden en slik evaluering kan oppfattes som «objektiv». Når det gjelder produkter som er evaluert etter mindre formelle og mindre grundige kriterier, kan kanskje slike lister være mer tvilsomme, siden garantien som er implisert av evalueringen, er dårligere, og evalueringer kan gjerne oppfattes som «subjektive».

Leverandørens utviklingsrutiner og seriøsitet ellers har betydning her. De fleste programvareleverandører, i Norge og internasjonalt, har meget dårlige utviklingsprosesser, inkludert prosjektstyring. Dette fører til at svært mye kommersiell programvare (hyllevare) er av dårligere kvalitet enn ønskelig, både når det gjelder funksjonalitet og mengden feil. Utviklingsprosesser ved utvikling av spesiell programvare, enten dette utføres internt, ved kjøp av konsulenttjenester, eller ved ordre til en programleverandør, er oftest på samme ad. hoc. nivå. Feil har først og fremst betydning for tilgjengelighet, men kan også ofte ha andre sikkerhetsmessige implikasjoner. Når det gjelder teknisk datasikkerhet og eksterne angrep, er de to viktigste truslene utnyttelse av:

- Feil i systemkonfigurasjon,
- design- og implementasjons-feil i programmer.

Et meget viktig tiltak for økt IT-sikkerhet er bedring av kvaliteten på den programvaren som benyttes. Dette kan oppnås ved krav til, og evaluering av, utviklingsprosessen hos leverandører og internt i det offentlige. Også her kan det være en rolle for akkrediterte evaluatorer tilsvarende som for annet kvalitetssikringsarbeid.

Mer utstrakt bruk av formelt evaluerte systemer kan gjerne settes opp som et langsiktig mål, men vi tror at det er langt fram før det er fornuftig å prioritere ressurser på dette i de fleste organisasjoner, i forhold til andre tiltak for å bedre sikkerheten. Det er sannsynlig at et krav om formell evaluering kan være fornuftig allerede nå for enkelte spesielle komponenter. Brannmurer for tilkopling til åpne nettverk er ett eksempel, og et annet kan være et system for drift av en sertifiseringsautoritet for identitets- eller rettighets-sertifikater.

---

[18] The EDP Auditors Association (Norway Chapter), sammen med Den Norske Dataforening, utarbeider dokumenter som anbefaling til god IT-skikk, og ser også på anbeflinger for konfigurasjon av visse typer systemer, som f. eks. databaser. Dette er delvis basert på internasjonalt arbeid innen «best practice» for drift av IT-systemer, der særlig «BSI Code of Practice for Information Security Management» skal nevnes.

5.8 Evaluering av sikkerhetsstrategier

Uansett evaluering av datasystemer og programvare vil disse alltid bare være vertøy for organisasjoner som skal behandle sensitiv informasjon. Skikkelig sikkerhet i en organisasjon krever en gjennomarbeidet og effektiv sikkerhetsstrategi som omfatter alle deler av virksomheten. Teknisk datasikkerhet kan aldri være tilstrekkelig, og i svært mange tilfeller ligger de største svakhetene ikke i teknologien, men i arbeids- og kontroll-rutiner. Dette innebærer i høy grad også dårlige driftsrutiner for datautstyr.

Derfor er det svært ofte på dette området det er mest fornuftig å sette inn ressurser for å få etablert fornuftig sikkerhetsnivå. Etablering av sikkerhetsstrategier er et komplisert og tidkrevende arbeid. Dette tilsvarer kvalitetssikringsarbeid, og en kan da også godt si at sikkerhetsopplegget er en del av organisasjonens kvalitet. Det er ellers aldri tilstrekkelig å *etablere* et tilfredsstillende sikkerhetsnivå. En sikkerhetsstrategi skal utarbeides og implementeres, men det er også nødvendig med periodiske gjennomganger for å sjekke at alt fungerer som det skal, og for å fange opp behov for endringer.

En godkjent sikkerhetsstrategi bør være et krav for å få lov til å behandle informasjon av gitte typer (Datatilsynet vurderer å stille krav om at det skal eksistere sikkerhetsstrategier). Det er et stykke fram før dette kan være et realistisk krav, men retningen burde være klar nok. Slikt arbeid tilsvarer i stor grad «ISO 9000 type» sertifisering (uten at det er gitt at nettopp ISO 9000 alltid er passende), og bør utføres av akkrediterte evaluatorer. Andre mulige evaluatorer av sikkerhetsstrategier er IT-revisorer.

6. TEKNISKE TTP-TJENESTER, EN DISKUSJON

6.1 Innledning

Tekniske TTP-tjenester utgjør en nødvendig infrastruktur for å etablere sikker kommunikasjon mellom et stort antall aktører. Til en viss grad vil dette kunne være rene telekommunikasjonstjenester, men det er en flytende overgang mot organisatoriske anvendelser av TTP-tjenestene. F. eks. kan identitetssertifikater brukes ved bruk av teletjenester, aksess til datasystemer mm., men også for å bevise identitet overfor en motpart en ønsker å samhandle med.

6.2 Identitetssertifikater - elektronisk legitimasjon

Den vanligste typen sertifikater er identitetssertifikater, eller elektronisk legitimasjon. Selv om det har vært lansert ideer i retning av at en bruker bare trenger ett sertifikat, tror vi neppe dette blir tilfellet. Dette tilsvarer dagens situasjon, der en har en rekke legitimasjoner for ulike forhold, og regler for hvilke legitimasjoner som godtas i forskjellige sammenhenger. Eksempler på elektronisk legitimasjon kan være:

- Elektronisk bankkort og kredittkort,
- elektronisk identitetskort fra jobben,
- «borgerkort» for kommunikasjon mot det offentlige,
- annet etter behov.

Vi antar at hver slik legitimasjonstype vil bli utstedt innen et separat sertifiseringshierarki. Kryssertifisering vil angi hvilke hierarkier som anerkjenner hverandre, omtrent slik vi i dag har regler for hvilke legitimasjoner som godtas i en gitt sammenheng (jeg kan ikke gå i banken med id-kortet mitt fra jobben).

Det er klart at det for enkelte anvendelser er ønskelig at det offentlige selv driver SA-tjenestene. I andre tilfeller kan det være ønskelig med offentlig akkreditering eller i hvert fall et regelverk. Uansett må det finnes regler for

hvilke legitimasjoner som skal godtas ved kommunikasjon mot det offentlige. En diskusjon om dette følger seinere i notatet.

Et spørsmål som må avklares, er hva som menes med en «identitet». Det er klart at dette må være en unik identifikasjon, slik at navn alene ikke er tilstrekkelig, mens navn/organisasjon kan være nok. Personnummer kan være aktuelt i enkelte sammenhenger, men være lite ønskelig i andre. I noen tilfeller kan elektronisk postadresse være den best egnede identifikasjonen. I henhold til X.509 standarden skal navnet i utgangspunktet være et såkalt «Distinguished Name»[19], men dette har i praksis ofte vist seg å være en lite hensiktsmessig, siden slike navn ikke brukes i andre sammenhenger.

For nettverkssikkerhet er det ønskelig med identitetssertifikater som autentiserer datamaskiner eller spesielle programmer (f. eks. Web-klienten på en gitt PC). Denne typen sertifisering diskuteres ikke spesielt i dette notatet, men mye av diskusjonen nedenfor skulle være gyldig også for dette tilfellet.

6.3 Rettighetssertifikater - betaling

I en del tilfeller er ikke identiteten til den en kommuniserer med viktig, men en trenger å være sikker på at vedkommende har visse privilegier. Dette kan oppnås gjennom sertifikater der en SA har signert over koblingen mellom en rettighet og en offentlig nøkkel. Bevis for kjennskap til tilsvarende privat nøkkel beviser rettigheten.

Det er også mulig å sertifisere koblingen mellom identitet og rettighet, og bruke dette sammen med et identitetssertifikat for å bevise en rettighet. Dette kan f. eks. være aktuelt for å bevise signaturrett for en person på vegne av en bedrift eller organisasjon, eller for å bevise retten til å opptre i en gitt rolle. Dette er delvis diskutert tildligere under avsnittet om «bevillingsbrev».

Her skal vi kun diskutere en form for rettighetssertifikater, nemlig knyttet til betaling og elektronisk handel. Her er identitet ofte irrelevant, men betaleren trenger å bevise retten til å disponere en bankkonto eller et kredittkort.

Hvis vi ser bort fra abonnement og andre modeller der det må foreligge en forhåndsavtale mellom kjøper og selger, finnes det tre betalingsmåter for elektronisk handel:

- Belastning av kredittkort,
- elektroniske kontanter,
- elektronisk sjekk.

Rettighetssertifikater er aktuelt kun for det siste tilfellet. Elektroniske kontanter diskuteres også kort nedenfor fordi slike systemer reiser en del juridiske og politiske problemstillinger av interesse. Belastning av kredittkort gjøres rett og slett ved at en sender en digitalt signert autorisasjon til å belaste et oppgitt kortnummer med et gitt beløp. Dette tilsvarer dagens bruk av kort. Her brukes bare et identitetssertifikat, og ikke noe spesielt rettighetssertifikat.

Elektroniske kontanter vil mest realistisk realiseres ved «småpengekort»[20] - smartkort som kan «fylles opp» i noe som ligner minibanker, eller over nettet fra brukerens bank. Ved betaling trekkes beløpet fra kjøperens kort, overføres, og «settes inn» på selgerens konto (eller på selgerens smartkort). Den største utfordringen ved slike systemer er å sikre en kobling til den «virkelige» økonomien, og sikre at ingen oppretter egne instanser for utstedelse av «penger» som kan godtas som gangbar mynt «på nettet». De fleste systemer for elektroniske kontanter legger vekt på anonymitet. Mens dette er en ønsket egenskap i mange tilfeller, reiser det en del problemstillinger rundt hvitvasking av penger og eksport av penger. Systemene krever i varierende grad bruk av TTPer for å sikre at misbruk kan oppdages og for loggføring. Det antas at systemer for elektroniske kontanter vil

[19] X.509v3 er endret i forholdt til tidligere versjoner, slik at andre navn nå kan brukes med X.509 sertifikater.

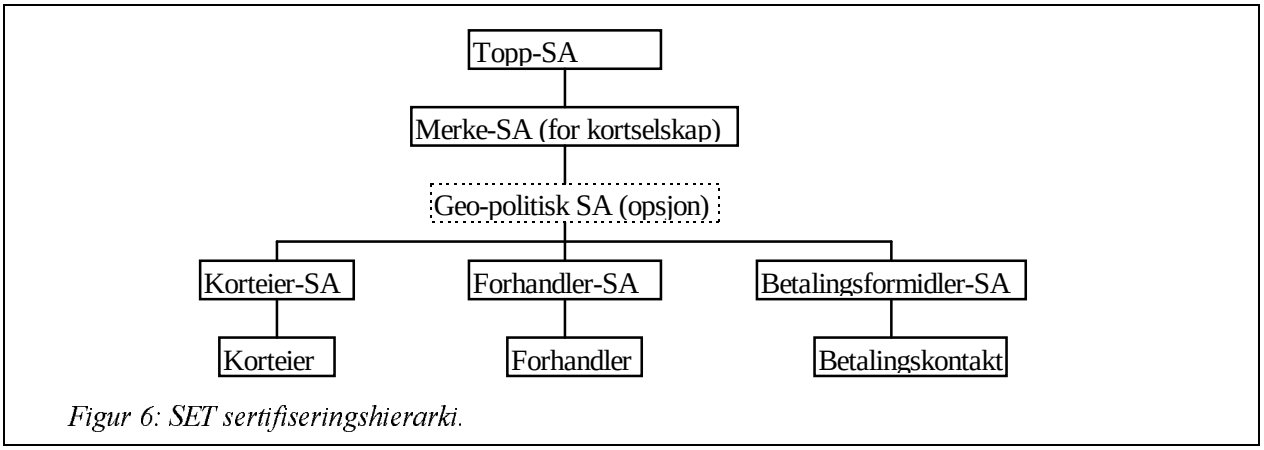
[20] Det finnes systemer, også til en viss grad i bruk, som realiserer elektroniske kontanter bare ved hjelp av programvare. Det benyttes meget avanserte kryptografiske teknikker.

være underlagt banklovgivningen. Det er usikkert når, og i hvor stor grad, elektroniske kontanter vil bli tatt i bruk, men veien fra dagens bonuskort for handling og til kontantkort er ikke nødvendigvis så lang.

En elektronisk sjekk er en signert melding som autoriserer overføring av et gitt beløp mellom to konti. Her knyttes signeringen opp til retten til å disponere konto, og ikke til identitet. Vi kan tenke oss at framtidas bankkort (eller kredittkort) kan brukes i smartkortleseren i PCen. Kortet vil inneholde en signeringsnøkkel og et sertifikat som kobler den tilsvarende offentlige nøkkelen med kontonummer. En elektronisk sjekk fylles ut med til-konto og beløp, og bankkortet brukes til å generere resten av informasjonen og til å signere.

Det arbeides med spesifikasjoner, Secure Electronic Transactions (SET), for å standardisere belastning av kredittkort[21] (eller bankkonti) på denne måten. Ca. 1/3 av disse spesifikasjonene omhandler sertifisering, der det forutsettes at den som skal sertifiseres, har et kundeforhold med kortselskap / bank fra før. Sertifiseringshierarkiet for SET er vist i Figur 6. Et felles toppnivå sertifiserer hvert kortselskap, som i sin tur har separate SAer for å sertifisere kunder/brukere, forhandlere og betalingsformidler (acquirer payment gateway). En mulig oppbygning av dette i praksis er at kortselskapet selv driver betalingsformidler-SA, og gjennom denne sertifiserer sin(e) norsk(e) representanter, f. eks. en bank. Forhandler-SA for Norge drives av denne banken, eller kanskje heller av bedrifter som Fellesdata, NOVIT eller BBS på vegne av banken. Kundesertifisering kan drives på samme måte som forhandler-SA, men i dag ser vi at kortselskapene gjerne henviser til firmaer som Verisign (se seinere i notatet).

Fellesdata, IBM, Visa m.fl. har allerede annonsert et samarbeid om bruk av SET i Norge, og flere vil antagelig følge etter om kort tid.



Figur 6: SET sertifiseringshierarki.

Antagelig er (eksisterende) lover og regelverk, som bankloven, tilstrekkelig for offentlig kontroll av elektronisk handel og betaling. Tekniske løsninger for å sikre tilstrekkelig innsyn vil kunne være nødvendig i enkelte tilfeller, som ved elektroniske kontanter, men dette avhengig av i hvor stor grad betaling er knyttet til bruk av «vanlige» konti. Utstedelse av rettighetssertifikater stiller de samme sikkerhetskrav som utstedelse av identitetssertifikater, se neste avsnitt.

6.4 Krav til drift av sertifiseringsautoriteter

Dersom en sertifiseringstjeneste virkelig skal være tiltrodd, er det en del krav som må oppfylles. Disse kan oppsummeres som:

[21] I SET brukes ikke kortnummeret direkte som identifikasjon i meldinger og sertifikater, men en transformasjon av nummeret. Dette fører til at selger ikke får tilgang til nummeret, mens dette likevel kan verifiseres av kortselskap / bank.

- Klart definerte sertifiseringsregler[22],
- sikker drift, som en forutsetning for å kunne stole på tjenesten,
- i en del tilfeller objektivitet i forhold til det området det skal kommuniseres om.

Det siste er ikke noe absolutt krav. Allerede i dag kan bankene selv utstede bankkort til sine kunder, selv om bankene i høyeste grad er involvert i de økonomiske transaksjonene. På samme måte bør banker selv kunne utstede sertifikater til sine kunder. I andre tilfeller ønsker en definitivt ikke at en av partene skal kunne ha denne rollen.

De sertifiseringstjenester som drives i dag, gir tjenester med forskjellig sikkerhetsnivå[23], avhengig av formål, og av sikkerheten i brukernes systemer. Som ett eksempel kan det tenkes forskjellige tjenester for brukere som har smartkortbaserte systemer (privat nøkkel mm. lagret på smartkort), i forhold til brukere med rene programvareløsninger.

Vi antar at sertifiseringstjenester svært ofte vil leies fra organisasjoner som har spesialkompetanse på sikker drift, og at drift av sertifiseringstjenester vil være et forretningsområde. Her vil tjenestene drives i oppdragsgivers navn. Driften av tjenestene bør ha vært gjenstand for en evaluering, og det kan være fornuftig å stille krav om at det skal brukes datasystemer som har undergått formell sikkerhetsmessig evaluering (omtalt tidligere i notatet).

Det som imidlertid har skjedd, er at private firma (stort sett amerikanske, med Verisign[24] som det ledende) tilbyr TTP-tjenester, særlig SA-tjenester, i eget navn. Dette tilsvarer omtrent «A/S Legitimasjon» for utstedelse av fysiske legitimasjonskort, der en satser på å få disse godkjent i praktisk bruk. Disse firmaene ønsker å tjene penger i et marked, og utnytter at tradisjonelle aktører for utstedelse av legitimasjon (offentlige instanser, banker osv.) ikke har kommet i gang med slike tjenester. Det er ikke nødvendigvis noe galt i dette. Hvis markedet fungerer slik at kun seriøse aktører blir godtatt, kan slike tjenester være like gode som andre, men en del faktorer gjør det nødvendig å være på vakt:

- Dersom antallet slike tjenester blir høyt uten at det er noen kontroll, er det en risiko for at useriøse tilbydere kan komme inn.
- Sikkerhetsnivået, spesielt sertifiseringsreglene, må være tilfredsstillende.
- Dersom aktørene ikke anerkjenner hverandre gjensidig, kan samtrafikk bli problematisk.
- Det kan være i nasjonal interesse å sørge for at markedet ikke blir tatt av utenlandske aktører.

I øyeblikket er trenden at amerikanske leverandører av Internett-teknologi henviser til Verisign (som regel) når løsningene krever at en aktør må ha et sertifikat. Vanligvis vil brukerne skaffe seg et Verisign-sertifikat av laveste klasse, der sertifiseringsreglene etter vår mening er langt fra tilfredsstillende for seriøse formål. Det er heller ingen grunn til at f. eks. en norsk bank skal stole på Verisign. I dagens produkter er det ofte vanskelig å få installert andre sertifikater enn de som er utstedt av Verisign, men det ser ut til at produktene vil bli mer «åpne» i nær framtid. Risikoen for at en eller et fåtall kommersielle aktører tar markedet med løsninger som tilbyr for dårlig sikkerhet, er likevel helt klart til stede.

Dette kan peke i retning av at det er ønskelig med en viss kontroll med TTP-aktørene, i hvert fall for enkelte anvendelser. Det er ikke noe poeng å hindre norske brukere i å skaffe seg f. eks. Verisign-sertifikater, men det er viktig å spesifisere i hvilke situasjoner slike sertifikater ikke er gode nok. Mer spesifikt kan dette gjøres ved å definere sertifiseringsdomener med gitte retningslinjer for de tilfellene det er ønskelig med offentlig kontroll. Et

---

[22] For et eksempel på sertifiseringsprosedyrer og retningslinjer for drift, se dokumentasjonen for UNINETTs UNISA tjeneste under http://www.uninett.no/pca og http://www.uninett.no/pca/rfc1875.txt

[23] Det amerikanske firmaet Verisign, som utsteder offentlig nøkkel sertifikater, opererer med fire forskjellige klasser (sikkerhetsnivåer) sertifikater avhengig av hvor sikre prosedyrene er for å få utstedt et sertifikat. Se http://www.verisign.com

[24] Verisign og et par andre firmaer i USA tilbyr slike SA-tjenester i et internasjonalt marked.

domene kan realiseres gjennom et separat sertifiseringshierarki, med kryssertifisering mot andre hierarkier hvis ønskelig. Offentlig kontroll kan da oppnås ved at det offentlige selv oppretter rot-SA for hierarkiet, og gjennom det har kontroll over sertifiseringsregler og over hvem som kan drive SAer. Rot-SA i dette tilfellet kan også være nasjonalt toppnivå underlagt en internasjonal SA.

Det vil føre for langt å gå inn på alle mulige områder der det er ønskelig med et slikt offentlig engasjement, men for det offentlige selv kan et forslag være:

- Sertifisering av enkeltpersoner og bedrifter / organisasjoner for kommunikasjon mot det offentlige kan legges under Skattedirektoratet, med Folkeregisteret som ansvarlig for sertifisering av enkeltpersoner.

6.5 Akkreditering av sertifiseringstjenester, juridisk ansvar

Kontroll med sertifiseringstilbyderne kan gjøres gjennom akkreditering, eller tildeling av lisens for å operere innen et virksomhetsområde. Her kan en godt si at TTP-tilbydere kan klassifiseres som verdiøkende tjenesteleverandører i en telekommunikasjonssammenheng. Det kan skilles mellom to typer akkreditering:

- Retten til å drive sertifiseringstjenester i eget navn, spesielt retten til å utstede legitimasjon.
- Retten til fysisk å drive sertifiseringstjenester, for egen del eller på vegne av andre.

Det første punktet bør i stor grad være under offentlig kontroll, avhengig av for hvilke formål legitimasjonen skal kunne brukes. Dette kan kontrolleres gjennom lover og regelverk, eventuelt kombinert med tildeling av lisenser for å operere. Siden legitimasjoner må være gyldige i en internasjonal sammenheng, og Norge må kunne godkjenne legitimasjoner utstedt i utlandet, er det viktig med en harmonisering, spesielt mot EU[25]. I praksis er det ingenting som kan hindre en norsk borger (og neppe heller norske bedrifter) i å benytte tjenester fra en SA i utlandet. Det offentlige kan som et minimum spesifisere hvilke Saer (eller hvilke hierarkier), nasjonalt og internasjonalt, det selv godkjenner. Det er i større grad et åpent juridisk spørsmål hvilke begrensninger som kan legges på annen bruk av sertifiseringstjenester. Akkrediteringsinstans / lisensgiver kan i noen tilfeller være Statens Teleforvaltning, i andre tilfeller andre instanser. Lisensbetingelser kan knyttes til virksomhetsområde, hvem «kundene» skal kunne være, og hva sikkerhetsnivået skal være. Det kan f. eks. stilles som betingelse at SAer skal holde seg innen et gitt domene, f. eks. slik at norske bedrifter skal sertifiseres i Norge, og at norske SAer ikke skal akseptere utenlandske kunder.

Det finnes en del momenter som har med samordning å gjøre, som navngivning, der det må sikres at det benyttes entydige navn. Samordning vil i mange tilfeller kunne legges til Statens Teleforvaltning.

Et annet spørsmål er adgangen til å bruke samme offentlige nøkkel i flere sertifikater, slik at brukere kan greie seg med en privat nøkkel (f. eks. bare ett smartkort). Det kan tenkes situasjoner der dette ikke er ønskelig, f. eks. av personvernhensyn fordi bruken av en nøkkel i et rettighetssertifikat kan spores til identiteten gjennom et idnetitetssertifikat med samme nøkkel.

Fysisk drift av TTP-tjenester kan knyttes til et «stempel» på at en organisasjons tjenester drives tilfredsstillende, dvs. en sikkerhetsmessig evaluering. Dette vil antagelig være markedsdrevet, slik at det vil bli et krav fra kundene. Det kan tenkes et offentlig engasjement her, men antagelig er dette ikke nødvendig annet enn i de tilfellene der det offentlige selv driver (eller er kunde hos) TTPen. Sikkerhetsmessig evaluering, av organisasjoner og datasystemer, er diskutert tidligere i dette notatet.

Et beslektet spørsmål er hvilke juridiske forpliktelser en TTP påtar seg ved f. eks. å utstede et sertifikat. I hvor stor grad kan en TTP bli stilt ansvarlig for skader som oppstår p.g.a. feil i sertifiseringsprosedyrer eller brudd på TTPens sikkerhet? Avgrensning i dette ansvaret kan gjøres i lisensbetingelsene, eller i kontrakter mellom TTPen

[25] UNINETT, med NR som underleverandør, er norsk partner i EUs ICE-TEL prosjekt innen Telematics forskningsprogrammet. Dette prosjektet arbeider for å etablere en europeisk sertifiseringsinfrastruktur. Se: http://www.darmstadt.gmd.de/ice-tel

og kundene. Det kan være ønskelig å beskytte kundene mot urimelige kontrakter. Ved internasjonal operasjon blir de juridiske spørsmålene fort uoversiktlige, spesielt dersom det kan reises tvil om hvilken jurisdiksjon som skal gjelde.

6.6 Andre tekniske TTP-tjenester

6.6.1 Garantert tidsstempling

Sporbarhet krever tidsstempling av hendelser. Som regel vil avsender selv sette tidspunktet for sending, og mottager tidspunkt for mottak. Dersom en ikke stoler på motpartens tidsangivelse, kan en sende meldinger til en tilkoplet eller mellomkoplet TTP. En tilkoplet TTP vil legge på et tidsstempel, signere over tidsstempelet pluss den opprinnelige meldingen[26], og returnere dette. En mellomkoplet TTP kan også signere på samme måte, men her kan i stedet partene velge å stole på TTPens loggføring av når meldingen ble mottatt og videresendt.

Det er lite trolig at det vil opprettes egne TTPer for garantert tidsstempling, men organisasjoner som driver andre TTP-tjenester, kan tenkes å tilby dette som en «bi-tjeneste».

6.6.2 Garantert programvare i nettverk

Distribusjon av programvare i nettverk har vært gjort i årevis. Men nettverksteknologien kan nå se ut til å gå i en retning der brukerne kan ha meget enkelt utstyr (NCer - Network Computer) som bare inneholder et minimum av programvare i utgangspunktet, og i stedet laster programvare over nettet etter behov. Ett eksempel på denne typen teknologi er bruk av Java Applets eller Active-X objekter[27] i Internett WWW-tjenester. Dette er (vanligvis små) biter programkode som overføres fra en WWW-tjeneste til brukerens maskin, og kjøres hos brukeren uten at brukeren merker noe til dette. Med økt nettverkskapasitet kan slike teknikker etter hvert brukes også for store og kompliserte programmer. Programmer kan også sendes fra klienten til tjenermaskiner i nettet[28], f. eks. for å utføre et søk i en serie databaser, der programmet selv flytter seg fra tjener til tjener, og til slutt returnerer resultatet til klienten.

Etablering av et visst sikkerhetsnivå for en datamaskin krever at en vet hva slags programvare som går på maskinen, og at en stoler (i hvert fall til en viss grad) på programvaren (se også diskusjon tidligere i notatet om evaluering av programvare og systemer). Dersom aksess til vilkårlige tjenester i nettverkene fører til at en kan få over «vilkårlig» programvare til sin egen maskin, blir dette meget komplisert.

Det arbeides med teknikker for signering av programvare (som applets). Programvare kan signeres av forfatter, leverandør, kilde (f. eks. WWW-tjeneren som leverer en applet) eller en TTP i rollen som evaluator. Signatur fra f. eks. forfatter autentiserer forfatteren og garanterer at programmet ikke er manipulert seinere, men dette garanterer ikke mot programvare som er ondsinnet (eller inneholder feil som har sikkerhetsmessige effekter) i utgangspunktet. Dette krever at en stoler på forfatterens og dennes vurderinger, og det er noe helt annet enn å stole på *autentiseringen* av forfatteren. Signatur fra leverandør / kilde, som da opptrer som en slags TTP, vil vanligvis være mer å stole på. Dette tilsvarer det en i praksis ofte gjør i dag ved henting av programvare på Internett. Ved alltid å hente programmer bare fra tiltrodde programvarearkiver kan en med rimelig sikkerhet regne med å gå fri for virus o.l. TTPer for denne typen evaluering og distribusjon av programmer vil antagelig ikke kreve noe offentlig engasjement, men vil f. eks. bli drevet av anerkjente tjenesteleverandører.

---

[26] I praksis vil ikke hele meldingen, men bare en kryptografisk sjekksum (hash-verdi) av denne sendes til TTPen. TTPen får dermed ikke tilgang til innholdet i meldingen.

[27] Java er utviklet av Sunsoft: http://www.sun.com./java Active-X er utviklet av Microsoft: http://www.microsoft.com/activex

[28] Dette kalles ofte «agenter», eller «servlets» i Java-terminologien.

Imidlertid har ikke nødvendigvis en leverandør den nødvendige kompetansen til å evaluere koden, slik at det i mange tilfeller kan være ønskelig med en signatur fra en TTP i stedet. Så lenge dette dreier seg om små programmer, kan en ekstern evaluering gjøres forholdsvis greit. En slik TTP kan være drevet av en organisasjon som er akkreditert for å gjøre formell evaluering (se tidligere i notatet).

Active-X baserer hele sin sikkerhet på signering. Alt tyder på at dette er utilstrekkelig, og at sikkerhet også må inkludere komponenter på hver enkelt maskin for å sørge for at applets o.l. ikke kan gjøre skade. Java har denne tilnærmingen, men kommer også til å legge vekt på signering i tillegg.

Merk at sikkerhetsmessige trusler fra informasjon som hentes (eller mottas) over et nettverk langt fra er begrenset til programmer. Mange dokumenter inneholder i virkeligheten former for programkode som blir eksekvert når dokumentet blir åpnet. Det beste eksempelet er Word og Excel dokumenter, som kan inneholde virus. PostScript brukes for formattering av dokumenter for utskrift, men er nærmest et fullt programmeringsspråk. Det kan vanskelig tenkes noen TTP-tjenester for å garantere slike dokumenter, men det er nødvendig med sikkerhetsrutiner for beskyttelse i hver organisasjon.

6.6.3 Lovlig avlytting - kontroll av nøkler

Kommunikasjon som er konfidensialitetsbeskyttet ved kryptering, kan vanskelig avlyttes. Dette er selvfølgelig formålet når det gjelder beskyttelse mot utenforstående, men skaper problemer når det gjelder lovlig «tapping» av informasjon, f. eks. av politiet etter en rettskjennelse.

Avlytting er et meget kontroversielt tema. Retten til avlytting i visse situasjoner er hjemlet i norsk lov, som er mer restriktiv enn loven i de fleste land det er naturlig å sammenligne seg med. Det er (eller vil bli) et reelt problem dersom forbrytere kan kommunisere kryptert.

Samtidig må dette veies opp mot de inngrep som må gjøres i kommunikasjon mellom lovlydige borgere og bedrifter, og den sikkerhetsrisiko dette tross alt innebærer for dem.

Her skal vi la prinsippdiskusjoner om slike spørsmål ligge. Vi nøyer oss med å slå fast at dersom avlytting skal være mulig, kreves det både tekniske og organisatoriske tiltak, som vil være nødt til å omfatte TTPer. Dessuten ønsker vi å peke på de tekniske problemer som avlytting medfører.

Det finnes grovt sett to måter å muliggjøre avlytting:

- Sikre at krypteringsmetodene er så svake at de kan knekkes - dette anbefales definitivt ikke, siden det er umulig å sikre mot at krypteringen kan knekkes også av angripere.
- Sikre at avlytterne kan få adgang til nøklene som brukes, ved en såkalt «key recovery» metode (begrepet «key escrow» brukes også).

Både i USA og Europa arbeides det med krypteringsmetoder som kan avlyttes gjennom key escrow, og med organisasjonsmodeller (TTP-organisasjoner) som skal sikre at dette ikke misbrukes. De fleste modeller opererer med to TTP-organer, som holder hver sin del av nøklene, som bare kan utleveres etter en rettskjennelse. Disse TTPene skal være totalt uavhengige, og det kan være et krav at de ikke drives av noen offentlig instans. Utnevnelse av TTPene vil skje gjennom lovverket.

I praksis vil det være umulig å få til et system som åpner for lovlig avlytting, med mindre:

- Det innføres forbud mot omsetning og bruk av visse kryptoalgoritmer.

Et slikt forbud vil antagelig møte så mye motstand at det vil være vanskelig å få vedtatt. Det vil også medføre hindringer for fri forskning og utvikling av nye sikkerhetsløsninger, og et forbud vil være meget vanskelig å håndheve, annet enn for personer og organisasjoner som likevel er lovlydige.

«Problemet» er at den offentlig nøkkel algoritmen som i hovedsak er i bruk i dag[29], er reversibel[30]. Den har den egenskapen at tekst kryptert med offentlig nøkkel, kan dekrypteres med tilsvarende privat nøkkel. Dette brukes slik at avsender selv velger en hemmelig (sesjons-)nøkkel for kryptering av informasjonen, og sender denne nøkkelen beskyttet av mottagers offentlige nøkkel. Kun mottageren kan få tak i sesjonsnøkkelen og få dekryptert informasjonen. Dette er teknisk sett det enkleste, og på mange måter det sikreste, systemet for nøkkelutveksling..

Det finnes ingen mulighet for å avlytte et slikt system med mindre de private nøklene er kjent. Dette vil igjen være meget kontroversielt, spesielt fordi disse også brukes for signering av meldinger[31]. Et forbud vil ramme svært mange av de løsningene som er i bruk i dag.

Dersom en skal få gjennomslag for avlyttbare algoritmer må disse «tvinges gjennom» i framtidige systemer basert på smartkort og spesialelektronikk ved at kort og elektronikk kun implementerer disse algoritmene. Generelt må algoritmene kunne brukes internasjonalt, slik at det er begrenset hvor mye Norge kan gjøre på egen hånd.

Åpning for avlytting er et politisk spørsmål. Teknisk sett medfører lovlig avlytting økt kompleksitet i løsningene. Sikkerheten kan også, om enn kanskje ikke i vesentlig grad, bli dårligere fordi:

- Økt kompleksitet gir større sannsynlighet for sikkerhetsrelevante feil.
- Det innføres nye komponenter (TTPene) som en må stole på.

7. KONKLUSJONER

Det er stor aktivitet internasjonalt særlig når det gjelder identitetssertifikater (PKI - Public Key Infrastructure). Det finnes noen tilgjengelige tjenester, eksperimentelle, men også kommersielle som Verisign. Likevel er en også internasjonalt langt unna å ha noen formening om hvordan en infrastruktur skal se ut. Det er også et faktum at utviklingen drives av teknologien og teknologer (til en viss grad av økonomer), og ikke av politikere og byråkrater. Til en viss grad kan det være ønskelig med en grad av «anarki» i en startfase for å vinne erfaring før det tas for drastiske beslutninger, men det er etter vår mening meget viktig at det offentlige engasjerer seg i dette området, og etter hvert tar de nødvendige beslutninger når det gjelder regulering og kontroll av sertifiseringstjenester.

Også i Norge er det aktivitet. Statens Datasentral (for Posten) og Telenor Bedrift er to bedrifter som sikter mot markedet for sertifiseringstjenester. Innen EDI/EDIFACT er spørsmålet om TTP-tjenester og digitale signaturer utredet av Norsk EDIPRO. UNINETT A/S, som driver nettverket som kobler sammen (og til Internett) universiteter, høgskoler og forskningsinstitusjoner i Norge, har en operativ sertifiseringstjeneste som drives av NR. Gjennom denne utstedes paralleller til studiekort og jobb-id. kort for personer innen denne sektoren. UNINETTs SA er sertifisert av SAer på høyere nivå i Internett. Bankene og deres datasentraler er også på banen. Innen det offentlige har arbeidet mer hatt fokus mot anvendelser av digitale signaturer enn mot sertifiseringstjenestene.

Dette notatet omtaler langt mer enn sertifiseringstjenester for identitetssertifikater. Innen noen av disse områdene er det aktivitet internasjonalt rettet mot kommersialisering, mens andre ikke er tatt opp annet enn i forskningssammenheng. For organisasjonsmessige TTPer er det nødvendig å opparbeide en forståelse av hvordan elektronisk samhandling og et elektronisk marked vil fungere, og dette krever erfaring med slike markeder. Vi har antatt at dette i første omgang vil fungere omtrent som vanlig kommunikasjon og handel, og gir oss ikke inn på spekulasjoner om framtidig utvikling gitt mer og mer avanserte kommunikasjonstjenester.

---

[29] RSA etter oppfinnernes initialer (Rivest, Shamir, Adleman).

[30] En ikke-reversibel algoritme kan kun brukes til signering, ikke til nøkkelutveksling. Den amerikanske DSS (Digital Signature Standard) er ett eksempel.

[31] Alternativet er å bruke et nøkkelpar (privat / offentlig) til signering og et annet til nøkkelutveksling, og sørge for at det finnes en kopi av den siste private nøkkelen. Dette er vanskelig å gjennomføre i praksis.

Tjenester som høyvolum elektronisk handel krever TTP-tjenester. TTP-tjenester krever rammebetingelser som de kan virke innenfor. Dette er et offentlig ansvar gjennom akkreditering, lisensiering (med tilhørende betingelser), lover og regelverk. Det offentlige kan også tenkes å drive enkelte tjenester selv, som f. eks. en sertifiseringstjeneste i regi av Folkeregisteret for «elektronisk borgerkort».

Når det gjelder evaluering av IT-sikkerhet, har vi anbefalt ikke å legge vekt på formell evaluering annet enn for spesielle komponenter med store krav til sikkerhet. I de fleste situasjoner er en evaluering mer i retning av en IT-revisjon å anbefale, sammen med en grundig evaluering av den gjeldende sikkerhetsstrategien.