Tiltrodde tredjepartstjenester

Rolf Riisnæs, Institutt for rettsinformatikk

(Problemnotat – skisse til diskusjon om TTP'ens ulike roller og hvilke(n) rolle(r) myndighetene kan/bør ha/ta i forbindelse med etablering av TTP'er i Norge)

Tiltrodde tredjepartstjenester

Rolf Riisnæs, Institutt for rettsinformatikk

(Problemnotat – skisse til diskusjon om TTP'ens ulike roller hvilke(n) rolle(r) myndighetene kan/bør ha/ta i forbindelse med etablering av TTP'er i Norge)

1 INNLEDNING

1.1 Problemstilling

Vi ser i dag en stadig stigende utbredelse av, og stadig økende fokus på, elektronisk handel og bruk av elektronisk kommunikasjon i og mellom offentlig og privat sektor. Det er en uttrykt politisk målsetting at elektronisk kommunikasjon skal oppnå den samme tillit og ha den samme rettslige holdbarhet som tradisjonell papirbasert kommunikasjon. En forutsetning for å oppnå dette er at brukerne har tilgang til hensiktsmessige sikkerhetstjenester. Sentrale i denne forbindelse blir tilbydere av ulike sertifikattjenester og relaterte tjenester for digitale signaturer, her kalt Tiltrodde TredjePartstjenester (TTP).

Næringsdepartementet oppnevnte den 26.05.99 en arbeidsgruppe som fikk i oppdrag å vurdere hvilke(n) rolle(r) myndighetene bør spille i forbindelse med etablering av slike tjenester i Norge, herunder hvilke initiativ som bør tas fra det offentliges side. Nærværende notat er et *innspill til diskusjon* om enkelte sider ved disse spørsmål.

Innledningsvis er det hensiktsmessig å minne om at vi står overfor to hovedproblemstillinger:

1. Når og på hvilke vilkår skal/bør elektronisk kommunikasjon og elektroniske signaturer anerkjennes på linje med tradisjonell papirbasert kommunikasjon.
2. Hva er hensiktsmessige rammebetingelser for de sikkerhetstjenester som trengs for å legge til rette for anerkjenning av elektronisk kommunikasjon.

Problemstillingene er prinsipielt forskjellige og kan for så vidt betraktes uavhengig av hverandre. På den annen side består det et nært samvirke mellom dem. Jo strengere man er med kravene til anerkjenning av elektronisk kommunikasjon, jo strammere blir rammebetingelsene for tjenesteyterne. Og omvendt, jo mindre presis man er med å beskrive kravene til tjenesteyterne, jo mindre blir forutberegneligheten med hensyn til om det er grunnlag for å anerkjenne den elektroniske kommunikasjon i ulike sammenhenger.

Før man går inn på en diskusjon omkring TTP'ens rammebetingelser og myndighetenes rolle er det altså nødvendig å definere målet med tjenestene (nivået).

Vi kan ellers dele partene i markedet inn i tre grupper: Den som signerer, sertifikatutstederen og den som stoler på signaturen. Det er sertifikatutstederen (i vid forstand, jfr nedenfor) som er i fokus i nærværende notat.

1.2 Begrepet anerkjenning

"Anerkjenning" kan forstås på ulike måter. Vi kan muligens skille mellom formell, prosessuell og *de facto* anerkjenning av den elektroniske kommunikasjon.

- Formell – akseptert som oppfyllelse av formkrav der disse er begrunnet ut fra et sett med hensyn som det (fortsatt) er grunn til å anerkjenne og som den elektroniske kommunikasjon kan tilfredsstille.
- Prosessuell – faktisk likestilling (eller i alle fall ikke negativ diskriminering) med papirbasert kommunikasjon i forhold til hvorledes man vurderer skriftlige bevis.
- *De facto* – brukerne forholder seg rent faktisk til elektronisk kommunikasjon som tilfredsstillende uten at spesiell oppmerksomhet rettes mot de mer juridiske forhold.

Det kan ikke utelukkes at behovet for tiltak fra myndighetssiden vil variere avhengig av hvilken form for anerkjenning vi fokuserer på. Den politiske målsetting forutsetter antakelig at alle de tre betraktningsmåter er oppfylt. For å sikre dette kan det være hensiktsmessig at man nå og da forsøker å betrakte dem hver for seg slik at ikke noe "gjemmer seg bort". Til illustrasjon nevnes på den ene siden den utfordring som ligger i å *formidle* et eller flere formelle vedtak om rettslig anerkjenning ut til borgerne på en slik måte at folk flest oppfatter dette, med andre ord det problem at formell og prosessuell anerkjenning ikke uten videre er nok til å oppnå alminnelig aksept og forståelse. På den annen side det forhold at store grupper av brukere kan tilvenne seg en anerkjenning basert på vanen ved å bruke et medium uten at de formelle sider er avklart, jfr for eksempel telefaks som benyttes tilsynelatende ukritisk i mange miljøer, eller at de formelle spørsmål så sjelden kommer på spissen at man slår seg til ro med at det fungerer tilfredsstillende det meste av tiden.

For å oppnå anerkjenning i alle de tre betydningene av ordet kan det være nødvendig å:

- Vurdere regelverkets form- og prosedyrekrav og gjøre de nødvendige tilpasninger, dvs formelt å anerkjenne at den elektroniske kommunikasjon oppfyller lovens krav til form og prosedyrer.
- Sikre at elektronisk kommunikasjon ikke diskrimineres i domstolene, f eks gjennom særlige informasjons- og opplæringstiltak med hensyn til hvorledes elektronisk kommunikasjon kan forstås og vurderes, og/eller legge til rette for enkel bruk av sakkyndige.
- Demonstrere grunnlag for tillit gjennom faktisk bruk av gjennomtenkte løsninger i forvaltningen og domstolene.
- Gjennomføre aktive informasjonstiltak om myndighetenes holdning.

Faktisk anerkjenning er i stor grad et spørsmål om tillit, noe som vanligvis vokser frem over tid og gjennom etablerte relasjoner. Fordi vi her opererer med en målsetting om å oppnå anerkjenning i løpet av forholdsvis kort tid må det antakelig settes i verk offensive tiltak (offensive i betydningen noe som bidrar til å forsere en utvikling).

Det er naturligvis et ufravikelig krav at det rent faktisk (teknisk) er grunnlag for å anerkjenne den elektroniske kommunikasjon som tilfredsstillende i ulike sammenhenger. Men her vil vi se at dette kan skje på ulike nivåer. I enkelte sammenhenger er det svært lite som skal til, feks fordi risikoen er liten, i andre sammenhenger skal det mer til, f eks fordi det er av betydning at det ikke i ettertid blir reist tvil om resultatet. Det kan også være ulike funksjoner man ønsker å sikre og med ulike tidshorisonter.

Studier viser at begrunnelsene for signaturkrav i lovgivningen varierer. Det er grunn til å forvente at den pågående norske kartleggingsstudien (regi JD/NHD) vil vise det samme. Klarhet omkring dette er nødvendig før det kan gis detaljerte krav for formell likestilling.

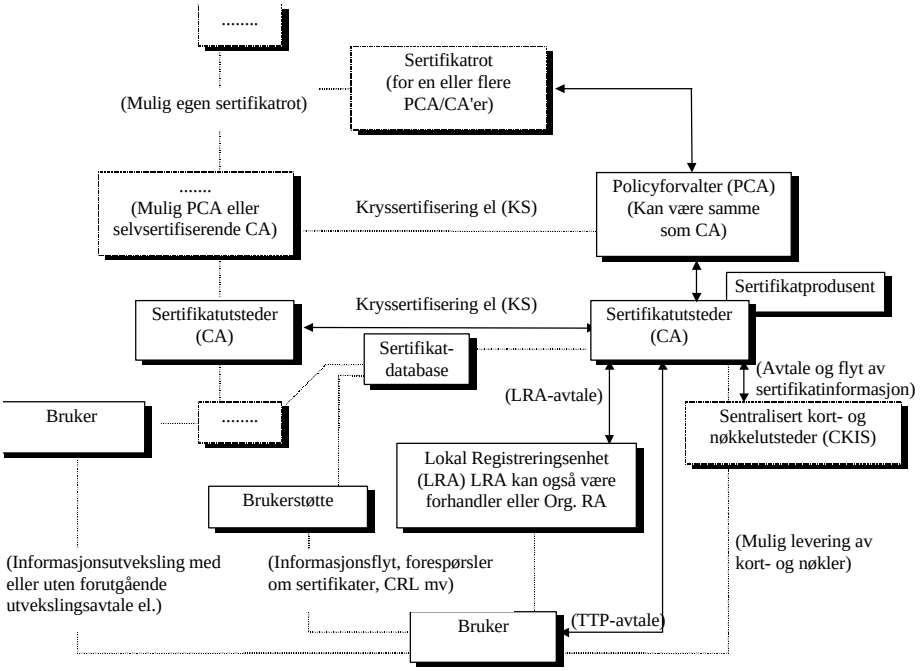
2 TTP'ENS ROLLER OG OPPGAVER - "HVA" OG "HVEM" SKAL REGULERES?

Under betegnelsen TTP finner vi en sammensetning av flere roller og funksjoner. Disse kan ofte være spredt på flere virksomheter. Spørsmålet blir hvilke roller og funksjoner som skal omfattes av eventuell regulering og hvilken eller hvilke tjenesteytere som skal være ansvarlig i forhold til regelverket [myndighetene].

Dette er dels et spørsmål om systematisering/organisering og beskrivelse av rollene, men også om hvilken eller hvilke roller man finner det hensiktsmessig å regulere.[1] De underliggende eller tilliggende funksjoner blir det så "hovedsubjektets" ansvar å kontrollere.

2.1 Oversikt over TTP-tjenesten og interne avtalerelasjoner

Figur 1 nedenfor viser en mulig struktur for en generisk TTP-tjeneste.[2] Det kan tenkes en rekke praktiske avvik fra de strukturer som her presenteres oversiktsvis og jeg vil komme tilbake til noen av disse.



Figur 1: Mulig struktur for en generisk TTP-tjeneste.

[1] Hvordan man velger å dele opp tjenesten er et hensiktsmessighetsspørsmål. Beskrivelsen i det følgende er forfatterens valg.

[2] Med *generisk TTP-tjeneste* menes summen av de funksjoner som samlet tilbyr ikke-anvendelsesspesifikke identitetsertifikater.

2.1.1 Registreringsenhet

Nærmest brukeren finner vi en registreringsenhet (Registration Authority ”RA”) som samler inn de data som er nødvendige i forbindelse med utstedelse av nøkkelsertifikat, kontrollerer og verifiserer den kommende sertifikatinnehaverens identitet eller rolle og formidler de nødvendige data til sertifikatutstederen. RA'en kan etter omstendighetene også være forhandler som formidler avtale mellom bruker og TTP. Man kan f eks tenke seg at en potensiell bruker henvender seg til et postkontor, fyller ut registreringsskjema, identitet kontrolleres av postfunksjonæren, skjemaet registreres og tilbud fra brukeren om å inngå avtale om TTP-tjeneste formidles til TTP'en.

2.1.2 Sertifikatutsteder

Sertifikatutsteder (Certification Authority ”CA”) kontrollerer de data som mottas fra RA og får utferdiget/produsert nøkkelsertifikat. Sertifikatutsteder vil være den sertifikatet utpeker som utsteder. Produksjon av sertifikatet kan teknisk være lagt til en særskilt sertifikatprodusent.

Tildeling av entydige navn kan også være en del av CA'ens oppgaver men denne funksjon kan også tenkes lagt til en egen instans slik at navn tildeles sentralt på basis av opplysninger fra CA. Løsningen vil avhenge bl a av eventuelle nasjonale retningslinjer for hvorvidt hver CA skal administrere sitt eget navnerom eller ikke, typisk ved at CA'ens navn inngår i brukerens entydige navn.

Sertifikatutsteder driver sin virksomhet i henhold til et sett med retningslinjer, en sikkerhetspolicy (Certificate Policy ”CP”), implementert i henhold til en definert sertifiserings praksis (Cerftification Practice Statement ”CPS”). En slik policy kan være pålagt den aktuelle sertifikatutsteder i kraft av sertifiseringsvedtak, den kan være vedtatt gjennom avtale, eller den kan være utformet av den enkelte sertifikatutsteder selv.

2.1.3 Policyforvalter

Administrasjon av den aktuelle sikkerhetspolicy kan være lagt til en rolle vi kan kalle policyforvalter.[3] Policyforvalter vil utvikle og forvalte den aktuelle policy og drive oppfølging og kontroll i forhold til sertifikatutstederne, f eks når det gjelder valg av sikkerhetsprofiler, kontrollstrategier, krav til kompetanse og sikkerhetsklarering av personell, valg av samarbeidspartnere og underleverandører mv. En policyforvalter kan koordinere og evt sertifisere sertifikatutstedere som driver under samme policy. Policyforvalter kan være sammenfallende med sertifikatutsteder men behøver ikke være det. Policyforvalter kan f eks være en bransjeorganisasjon som forvalter en sikkerhetspolicy for

[3] Policyforvalter kan i enkle strukturer være samme som sertifikatutsteder «CA» og eventuelt også være sertifikatrot.

bransjespesifikke anvendelser og som realiseres gjennom sertifikatutstedere som tilfredsstiller den aktuelle sikkerhetspolicy. Den aktuelle policy vil legge sterke føringer på sertifikatutsteders virksomhet. Dette kan ha betydning både for hva sertifikatutsteder kan gjøres ansvarlig for og for spørsmålet om policyforvalter kan ha et selvstendig ansvar for svikt ved policyen eller oppfølging av denne. Den aktuelle policy vil også danne utgangspunkt for eventuell registrering eller sertifisering av sertifikatutstederen. Policyforvalter vil kunne være det naturlige utgangspunktet for kryssertifisering mellom sertifikatutstedere og vil da selv ha en ”tiltrodd” rolle.

2.1.4 Sertifikatrot

Sertifikatroten (f eks en nasjonal sertifikatrot hvis en slik finnes) gir den sentrale forankring for den kjede av sertifikater som tilsammen utgjør den offentlige nøkkel infrastrukturen. Hvilken (offentlig) instans som eventuelt skal ivareta en slik funksjon er ikke klart. Alternativt kan det finnes mer enn en sertifikatrot innenfor et nasjonalt domene, da slik at hver sertifikatrot er utgangspunktet for en kjede av sertifikater (f eks Telenor og SDS/Posten for hver sin infrastruktur).

2.1.5 Nøkkelgenerering mv

Generering av krypteringsnøkler og nedlasting på nøkkelbærende produkter kan være lagt til en særskilt enhet (Centralised Key Issuing System ”CKIS”) men kan etter omstendighetene også ligge hos brukeren selv.

2.1.6 Sertifikatdatabasevert

Sertifikatdatabaseverten (Repository) systematiserer, oppbevarer og gjør tilgjengelig nøkkelsertifikater fra en sertifikatutsteder i form av en katalogtjeneste. Databaseverten vil normalt også gjøre tilgjengelig opplysninger om sertifikater som er trukket tilbake eller suspendert og kan etter omstendighetene også tilby tilleggsinformasjon om sertifikatinnehavere el.

2.1.7 Brukerstøtte og varslingstjeneste

For den løpende kontakt med sertifikatbrukerne behøves en brukerstøtte- og varslingstjeneste som bl a tar hånd om tilbaketrekking av sertifikater og vedlikeholder tilbaketrekkingsliste (Certificate Revocation List ”CRL”). Brukerstøtte og varslingstjeneste kan være organisert på mange ulike måter og kanskje delt på flere. Kundekontakten kan f eks være lagt til registreringsenheten eller sertifikatdatabaseverten, mens administrasjon av sertifikatene og vedlikehold av tilbaketrekkingslisten utføres av sertifikatutstederen selv. Kundekontakten kan også være plassert sentralt hos den som markedsfører eller fronter tjenesten utad.

2.1.8 Markedsføring og merkebygging

Markedsføring og merkebygging kan ligge til en egen organisasjon som fronter tjenesten utad og administrerer kontraktene med brukere og underleverandører av de øvrige tjenesteelementer. Etter omstendighetene kan denne funksjon ligge til andre enn den som i sertifikatet er oppført som sertifikatutsteder. Registreringsoppgavene kan f eks tenkes ivaretatt av den organisasjon som faktisk opptrer som kunde i forhold til sertifikatutsteder. Typisk ved at en større virksomhet som arbeidsgiver registrerer sine ansatte og formidler de relevante opplysningene til sertifikatutsteder. I denne situasjonen er det ikke åpenbart at den enkelte bruker har avtale med sertifikatutsteder. Enda tydeligere blir dette dersom virksomheten registrerer *egne kunder*, f eks i forbindelse med hjemmebank. Likevel vil det antakelig være nødvendig at sertifikatutsteder pålegger virksomheten å videreføre en del krav til brukeren i form av kontraktsforpliktelser før vedkommende får tilgang til tjenesten, f eks krav til aktsom omgang med kort og koder, bestemmelser om varsling ved tap av kort mv. (Problemstillingene er et stykke på vei kjent fra minibankkort mv.) Tilliten og kontrollen med bruken av tjenesten som helhet kan avhenge av dette. Sertifikatinnehaverne vil kunne avlede sin tillit fra den organisasjon de har inngått avtale med og ikke fra den bakenforliggende sertifikatutsteder selv om dennes identitet fremgår av sertifikatet. For de tredjeparter som handler i tillit til sertifikatets innhold vil imidlertid sertifikatutsteder kunne hefte.

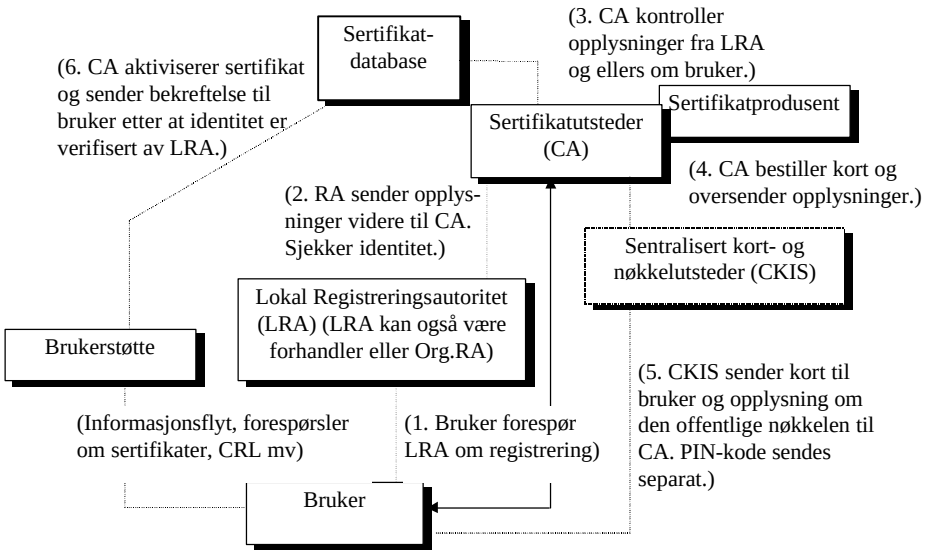
2.1.9 Er TTP-begrepet hensiktsmessig?

Det kan etter dette synes som TTP-begrepet er uegnet som navn på en rolle ettersom det ikke alltid er klart hvorfra brukerne avleder sin tillit. Det kan likevel være forsvarlig å snakke om TTP-tjenester som summen av de funksjoner som utgjør en fungerende sertifikattjeneste. I den utstrekning TTP-begrepet i det følgende er benyttet om en rolle er det den som i sertifikatet er oppført som sertifikatutsteder som menes med mindre noe annet fremgår av sammenhengen.

2.2 Registrering av brukere og nøkler

Den innledende og sentrale oppgave er registrering av brukere og deres krypteringsnøkler. Slik registrering kan skje etter flere ulike modeller. Valg av modell vil kunne påvirke hvilket sikkerhetsnivå man vil tilkjenne nøklene/sertifikatene.

Figuren nedenfor viser prosessen med registrering av brukere steg for steg etter en mulig modell, fra brukeren først henvender seg til en forhandler/RA av TTP-tjenesten og til den offentlige nøkkel infrastrukturen er klar til bruk for kunden.



Figur 2: Registrering av brukere steg for steg.

Registreringen skjer i følgende seks hovedtrinn:[4]

1. Bruker forespør om registrering.
2. RA registrerer opplysninger om kunden og sender disse videre til CA.
3. CA kontrollerer opplysningene fra RA og eventuelle øvrige opplysninger CA'en trenger om brukeren, f eks om vedkommendes kredittverdighet.
4. Dersom alt er i orden bestiller CA'en kort og nøkler til brukeren fra sin samarbeidende sentrale kort- og nøkkelutsteder (CKIS) ved å sende over nødvendige opplysninger.
5. CKIS genererer nøkler som nedlastes på dertil egnet medium, f eks et Smartkort. Kortet sendes til brukeren enten direkte eller via CA. Opplysninger om brukerens offentlige nøkkel sender CKIS til CA.
6. CA utferdiger nøkkelsertifikat tilhørende den offentlige nøkkel og sender melding til bruker om dette. Dersom brukers identitet allerede er verifisert i forbindelse med registrering hos RA og/eller avhenting av kort aktiviseres sertifikatet. I motsatt fall aktiviseres sertifikatet etter at brukers identitet er verifisert ved henvendelse til RA. Nøkkelinfrastrukturen er nå klar til bruk for kunden.

Prosessen med registrering av brukere og utstedelse av kort og nøkler kan på mer detaljert nivå ha flere ulike forløp avhengig av hvordan TTP-tjenesten er innrettet og hvilket sikkerhetsnivå man i det aktuelle tilfellet ønsker å imøtekomme. Noen slike alternativer beskrives nedenfor.

[4] Innenfor hvert registreringstrinn kan det være betydelige variasjoner som også har betydning for TTP'ens rettslige stilling.

2.3 Særlig om ulike registreringsordninger

2.3.1 Registrering hos TTPens egne registreringsenheter

Registrering av brukere kan for det første skje hos sertifikatutsteders egne registreringsenheter. Dette kan være filialer av TTPens egen organisasjon eller en organisasjon TTPen samarbeider med (f eks bank, post eller forhandlere av tele- og datatjenester som ikke opptrer som TTP i eget navn innenfor det aktuelle geografiske området).

Dette er forutsetningsvis organisasjoner som er trenet i kontroll av identifikasjonspapirer og utstedelse av slike og som følger strenge prosedyrer for registrering. (Dette vil f eks kunne tilpasses bankenes og postens utstedelse av legitimajonstegn.) For gjennomføring av transaksjoner med krav til høyt sikkerhetsnivå kan denne modellen være å foretrekke. Ulempen er at den er kostbar og det kan være vanskelig å oppnå en tilfredsstillende geografisk dekning for den enkelte TTP.

Det er imidlertid et tankekors at en slik ordning kanskje vil bli benyttet mest der en trenger det minst, nemlig for registrering av enkeltpersoner uten organisasjonstilknytning. Disse sertifikatene vil nok vanligvis bli brukt for transaksjoner med beskjedent skadepotensiale. Det er nemlig ikke usannsynlig at en rekke organisasjoner selv kommer til å registrere egne ansatte og brukere og at det vesentlige av kommersiell bruk kommer til å være basert på dette.

2.3.2 Registrering i egen organisasjon

Sertifikatutsteder kan autorisere enkelte større organisasjoner til selv å foreta registrering av egne ansatte, medlemmer eller brukere, foreta kontroll av identitet mv og samlet melde opplysningene inn til TTP’en. Som et supplement kan man tenke seg at for bedrifter som er for små eller av andre grunner ikke får anledning til å registrere egne ansatte, kan f eks selskapets revisor bistå TTP’en med en slik oppgave.

Løsningen vil sikre virksomheten kontroll med hvilke ansatte som opererer under sertifikater med peker til virksomheten (i tilfeller der organisasjonsnavn er en del av brukerens entydige navn).

En betydelig fordel er at virksomheten allerede kjenner de registrerte gjennom ansettelses-, medlems- eller kundeforhold og [til en viss grad] kan innestå for hvem de er.

Hvor aktuell en slik ordning er vil kunne avhenge av hvilket ansvar som til slutt påhviler en «organisasjons RA» og hvilke dekningsmuligheter som finnes, f eks gjennom krav om tvungen ansvarsforsikring for RA'er nedfelt i TTP'ens sikkerhetspolicy. Det kan imidlertid bli vanskelig å selge inn en slik løsning i en organisasjon dersom det medfølger et stor potensielt ansvar for feil som begås.

2.3.3 "Selvbetjent" registrering uten identitetskontroll

Man kan også tenke seg ordninger der hver enkelt deltaker selv genererer sine egne nøkler basert på programvare som f eks er tilgjengelige over internett og får disse registrert hos en tredjepart gjennom automatiserte eller i alle fall datamaskinbaserte prosedyrer, f eks ved å sende inn en "elektronisk blankett" som inneholder opplysninger om hvem avsenderen er og hva som er hans offentlige nøkkel. Utstedelse av sertifikat kan skje automatisk. De direkte kostnadene ved å drive en slik løsning vil være beskjedne og f eks Internett ville ligge til rette for en slik ordning. En slik ordning vil imidlertid representere et meget lavt sikkerhetsnivå i det deltakerne i prinsippet kan registrere seg som hvem som helst. Denne registreringsformen vil derfor ikke bli behandlet i det følgende. I denne modellen finnes heller ingen RA i egentlig forstand. All informasjon utveksles direkte med CA'en.

En slik ordning har likevel den funksjon at *det å være registrert* i seg selv gir en viss sikkerhet fordi et sertifikat som er feilaktig registrert sannsynligvis vil bli gjort ugyldig i løpet av kort tid etter at det er misbrukt. Dette reiser et viktig spørsmål om *CA'ens adgang til på eget initiativ å trekke sertifikater tilbake og mulig ansvar i den forbindelse.* Kan man f eks tenke seg at CA'ens adgang til tilbaketrekking er videre ved selvbetjente ordninger enn ellers?

2.3.4 Registrering via annen TTPs registreringsenheter

Ytterligere et alternativ kan være registrering via en annen TTP. Dersom TTPene gjensidig anerkjenner hverandre, f eks gjennom kryssertifisering, vil det være mulig for dem å etablere registreringsordninger hos hverandre. For en internasjonal aktør (bruker) som ønsker nærhet til hvert enkelt marked, eller ønsker å begrense risiko knyttet til hver enkelt nøkkel, kan registrering hos TTP i lokale områder, for det aktuelle landets brukere, være aktuelt.

2.4 Tilbaketrekking av sertifikater

For å opprettholde et hensiktsmessig sikkerhetsnivå er det nødvendig med prosedyrer som gjør det mulig å trekke tilbake, eller gjøre ugyldige, sertifikater knyttet til nøkler som er blitt kompromitert. Dette kan skyldes at kort og koder er kommet på avveie, at sertifikatene i utgangspunktet ikke skulle vært utstedt pga feil ved registreringen (feil person) eller at kort og koder er misbrukt, f eks ved overlevering til andre.

Det kan tenkes flere prosedyrer for tilbaketrekking av sertifikater. Prosessen kan begynne enten hos sertifikatinnehaver, hos den organisasjon som eventuelt fremgår av sertifikatet eller hos TTPen, f eks etter henvendelse fra en tredjepart som har opplevd svikt ved sertifikatet.

Dersom prosessen starter hos kortholder eller dennes organisasjon kan tilbaketrekking meldes på flere måter. Hvis årsaken er mistanke om at

nøkler er kompromittert eller at forholdet rett og slett skal opphøre, kan forholdet meldes vha signert elektronisk post.

Dersom kort og koder har kommet på avveie er kortholder avskåret fra denne mulighet. I så fall står telefonmelding som det mest nærliggende. Det kan imidlertid tenkes tilfelle der det å ugyldiggjøre andres sertifikater kan forårsake betydelig skade. Det er derfor spørsmål om endelig tilbaketrekking bør kunne skje over telefon eller om det må bekreftes skriftlig eller ved oppmøte hos en registreringsenhet eller annen samarbeidende TTP når det ikke kan skje vha signert elektronisk post. Også denne muligheten kan naturligvis misbrukes hvis kort og koder kommer på avveie. På den annen side, dersom kort og kode kommer på avveie er det vanskelig å tenke seg situasjoner der meldinger generert etter dette tidspunkt *ikke* skal anses som ugyldige (dvs sertifikater *skal* ugyldiggjøres).

Tilbaketrekking kan enten anmerkes i sertifikatet selv (avhengig av oppbygging og anvendt standard) eller anmerkes i særskilte tilbaketrekkingslister som kan lastes ned av den enkelte bruker, såkalte Certificate Revocation Lists «CRL». Anmerkningene må typisk inneholde opplysninger om hvilket sertifikat tilbaketrekkingen gjelder og fra hvilket tidspunkt tilbaketrekking fant sted. Problemstillingen er et langt stykke på vei parallell med det mer kjente problemet med sperring av bankkort.

Det vil måtte stilles strenge krav til TTPens oppfølging av sertifikatdatabasen og tilbaketrekkingslistene. Tankegangen bak denne type tjeneste er jo nettopp at tjenesten skal være ajour og at man skal kunne handle i tillitt til at opplysningene som fremkommer der er korrekte.

I tillegg må det over tid holdes oversikt over tidspunktene for når sertifikater blir trukket tilbake eller skifter status. Dette er nødvendig for i ettertid å kunne verifisere om en signatur ble påført mens sertifikatet fortsatt var gyldig.

2.5 Særlig om kataloger og tilleggsinformasjon

Et spørsmål som ikke har vært mye fremme men som man bør ta stilling til i forbindelse med eventuelle reguleringsinitiativ, er registrering, bruk av og ansvar for kataloginformasjon som er nødvendig for utnyttelse av et sertifikat men som ikke fremgår av sertifikatet selv.[5]

[5] Dette vil til en viss grad avhenge av hvilke opplysninger man velger å legge inn i sertifikatet, men brukernes ulike referanseramme og praktiske kontrollmuligheter kan variere slik at ikke alle kan utnytte den samme informasjonen. For eksempel vil man ikke ha særlig nytte av å få oppgitt et fødselsnummer dersom man ikke kjenner dette fra før og som privatperson vil man ikke uten videre ha adgang til f eks det sentrale personregisteret.

Situasjonen kan for eksempel være følgende: Jeg mottar en melding, meldingen er signert, sertifikatet er gyldig og innholdet er kommersielt interessant for meg. Av sertifikatet fremgår sertifikatinnehaverens entydige navn men det er ikke koplet til noen særskilt virksomhet. Det inneholder heller ikke tilstrekkelig informasjon, for eksempel fødselsdato eller privatadresse, til at jeg kan foreta en kredittsjekk på vedkommende. Dette forutsetter nemlig at jeg entydig kan identifisere den aktuelle person overfor kredittopplysningsselskapet.

For å vurdere den kommersielle risiko ved transaksjonen må jeg altså skaffe ytterligere opplysninger om vedkommende som er innehaver av sertifikatet. Han kan naturligvis ha lagt inn ytterligere informasjon om "seg selv" i den aktuelle meldingen, men jeg kan ikke uten videre kontrollere at de opplysningene stemmer med sertifikatinnehaveren. Man kan jo f eks tenke seg at han i meldingen har oppgitt sin økonomisk bedre stilte navnebror (som bor på en annen fysisk adresse), men at han likevel selv vil motta resultatet av transaksjonen fordi det skal leveres over nettet. Alternativt kan problemstillingen være at jeg ønsker å få bekreftet om sertifikatinnehaver virkelig er identisk med den som er oppført som signaturberettiget for den aktuelle virksomhet i Foretaksregisteret.[6]

Jeg kan altså ha behov for å matche opplysninger i meldingen med opplysninger om sertifikatinnehaveren. For det formålet vil det antakelig være nødvendig å få tilgang til informasjon som er registrert om sertifikatinnehaveren utover det som følger av sertifikatet selv. Denne tilleggsinformasjon kan være like kritisk for tilliten til og anvendelsen av sertifikatet/signaturen som de øvrige deler av systemet. Informasjonen, som genereres av TTP'en men som sannsynligvis vil driftes av sertifikat-databaseverten, vil ha en langt raskere oppdateringstakt enn sertifikatdatabasen selv og vil derfor også være mer sårbar. I forbindelse med utvelgelse av sertifikat for bruk til innholdskryptering er det også åpenbart at muligheten for entydig identifisering blir et sentralt poeng.

Retningslinjer for bruk og ansvar for slik kataloginformasjon må vurderes i sammenheng med de øvrige deler av reguleringen.

2.6 Regulatoriske utfordringer

Vi har vist at TTP-tjenesten kan deles opp, beskrives og implementers på flere måter. Dette er en betydelig utfordring når det skal velges organisatoriske grep.

Foreløpig synes bildet relativt oversiktlig. På det norske markedet i dag er de vesentlige funksjoner forankret i samme virksomhet eller i alle fall i samme konsern.

[6] Har kunne man naturligvis tenke seg at det var utstedt et rollesertifikat til den signaturberettigede, men det vil neppe bestandig være situasjonen.

På noe sikt kan man imidlertid forvente at enkelte av oppgavene finnes spredt mens man samarbeider eller kjøper felles ressurser for andre. Man kan for eksempel tenke seg at registrerings- og driftsoppgaver formidles eller kjøpes fra *felles* spesialiserte virksomheter mens sertifikatene utstedes fra ulike TTP'er. Også den som teknisk utsteder eller produserer sertifikatene kan få en perifer rolle i forhold til den aktivitet som antakelig bør begrunne ansvaret, nemlig tillitsbygging i markedet, og som altså kan ligge til en annen organisasjon. Man kan jo meget vel tenke seg en virksomhet som utad fremstår som "selve TTP'en" men hvis virksomhet er begrenset til å administrere en policy, inngå avtaler og organisere en underliggende tjeneste satt sammen av innkjøpte tjenester som omfatter alt inklusive sertifikatprodusenter. I et slikt tilfelle vil det antakelig være naturlig at den som fronter tjenesten utad også hefter for den. TTP-tjenesten kan også være bakt inn som en ”usynlig” del av en annen tjeneste, f eks i forbindelse med hjemmebank el.

I så fall kan man tenke seg at ulike deler av reguleringen vil omfatte ulike roller, for eksempel slik at den som fronter tjenesten utad hefter økonomisk, mens vurdering av de kvalitative krav man må stille for formell anerkjenning av de digitale signaturer skjer etter en vurdering av de underliggende tjenesteleverandører. Hovedmannen vil i så fall hefte også for de opplysninger han gir om de kvalifikasjoner og sertifiseringer tjenesten samlet har.

Arbeidsgrupen må ta stilling til hvilke modeller man skal favne med sine anbefalinger.

Dersom regulering skal utformes må man påse at det er mulig å identifisere subjektet for de ulike deler av reguleringen og at den er beskrevet slik at den kan anvendes på ulike modeller for implementering av tjenestene. Bl a må en ta stilling til om kravene til personellets kompetanse skal finnes i alle ledd eller kun hos sertifikatutstederen, mens den viktige oppgaven med verifisering av relasjonen mellom sertifikatinnehaver og den offentlige nøkkelen kanskje kontrolleres av registreringsenheten. Skal kravene om finansiell styrke gjelde alle ledd i virksomheten eller er det tilstrekkelig at den som i sertifikatet er oppført som sertifikatutsteder har de nødvendige ressurser eller forsikringer. Kravene til håndtering av personopplysninger vil gjelde i alle ledd men plikten etter direktivet til å begrense utlevering av sertifikater må antakelig administreres av sertifikatdatabaseverten. Det overordnede krav om at tjenesten samlet sett oppfyller samtlige krav må hvile enten på den som utad fremstår som tjenesteleverandør eller den som formelt har påtatt seg rollen som samlet tjenesteleverandør overfor rett myndighet f eks i henhold til et system for frivillig evaluering eller godkjenning. Dersom det formelle ansvar/godkjenning skiller seg fra den som utad fremstår som tjenesteleverandør kan en tenke seg en situasjon der erstatningsansvar kan rettes mot dem begge og at kravene til finansiell styrke eller forsikring følgelig bør oppfylles av begge.

Den situasjon kan oppstå at ulike deler av tjenesten kontrolleres/revideres av ulike organer, f eks to konkurrerende revisjonsselskaper, og det er derfor påkrevet at kravene kan deles opp på funksjoner slik at det både er mulig å gjøre en vurdering av om de samlede krav er oppfylt, men også at de enkelte krav i nødvendig grad er oppfylt hos alle eller flere av tjenesteyterne. Det kan derfor være hensiktsmessig å vurdere de enkelte krav i direktivet opp mot en modell av de ulike roller/funksjoner og knytte dem opp mot de ulike roller. Det er ikke med dette sagt at reguleringen bør utformes slik at det i detalj fremgår hvorledes plikter og krav fordeles på de ulike roller, men det bør i alle fall være tilgjengelig opplysninger som viser hvorledes man har tenkt.

Også i forhold til kryssertifisering eller anerkjenning av sertifikater utstedt av andre kan det være spørsmål om hvem som hefter/bør hefte. Anerkjenning (evt gjensidig anerkjenning) vil først og fremst være et kommersielt anliggende, dvs en vurdering av om det er tjenlig å ta risikoen ved å anerkjenne andre sertifikater med de konsekvenser det måtte ha (hvilket bl a vil avhenge av hva man hevder å anerkjenne/innestå for). En slik form for anerkjenning vil naturlig skje på overordnet nivå der kontrakter administreres og der brukere forankrer sin tillit. Som en premiss for dette vil man antakelig finne mer teknisk orienterte vurderinger og samarbeid, f eks i form av samtrafikkavtaler, mellom sertifikatutstedere og databaseverter. Det er betydelig forskjell på å kreve åpenhet i form av teknisk interoperabilitet, det å innestå for andres sertifikater eller rett og slett gi uforpliktende vurdering av om andres sertifikater tilfredsstiller den enkelte brukers definerte sikkerhetsbehov.

2.7 Noen tanker om relevante likheter og forskjeller mellom sertifikatutstedere og andre tiltrodde tjenester

Avslutningsvis i dette kapittelet presenteres stikkordsmessig noen synspunkter på likheter og forskjeller mellom sertifikatutstedere og andre tiltrodde tjenester.

- Bankenes og postvesenets utstedelse av ID-kort:
    - Likheter:
        - Bankene utsteder ID-kort til sine kunder, basert på identifikasjonskontroll ved oppmøte.
        - Det foreligger en etablert kunderelasjon.
        - ID-kortet benyttes som legitimasjon også i andre sammenhenger (generisk legitimasjonstegn) selv om det primært er utferdiget for å tjene som legitimasjon for en kontoinnehaver.
        - Nøkkelsertifikater innebærer en slags ”forhåndsregistrering” av ”signaturer” med en funksjon som har paralleller i bankenes bruk av signaturkort.
    - Forskjeller:

        - Nøkkelsertifikatene er i motsetning til bankenes legitimasjonstegn først og fremst beregnet på bruk ift *andre* enn utstederen (TTP'en).
        - Transaksjonstype i prinsippet ukjent for sertifikatutstederen (med mindre det er lagt inn begrensninger i sertifikatet).

- Kredittopplysning:
    - Likheter:
        - Systematisk utlevering av opplysninger om registrerte til tredjemann.
        - Opplysningene benyttes for vurdering ifm kommersiell transaksjon.
    - Forskjeller:
        - Den registrerte er ofte ikke kjent med registreringen eller hvilke opplysninger om ham som er lagret hos kredittopplysningsbyrået (under endring) mens sertifikatinnehaveren normalt selv vil ha tatt initiativet til registrering og avgitt opplysningene.
        - Virksomheten er konsesjonspliktig.
        - For kredittopplysningsbyråene har man lovregulert ansvaret ift den registrerte, jfr pregl § 40.

- Tinglysingsystemet, Foretaksregisteret mv:
    - Likheter:
        - Registrering av eierforhold (eiendommens identitet) og heftelser (egenskaper). Fullmakter (prokura mv) og styremedlemmer (egenskaper).
        - Systematisk utlevering av opplysninger for bruk i kommersielle forhold.
    - Forskjeller:
        - Offentlig monopoltjeneste i forhold til å oppnå de lovbestemte rettsvirkninger av tinglysing og registrering.
        - Lovregulert ansvar.

- Postsektoren:
    - Likheter:
        - Posten TTP ifm f eks rekommandert post. (Sjekker mottakers identitet på vegne av avsender.)
        - Utsteder legitimasjonstegn, jfr om bankene ovenfor.
    - Forskjeller:
        - Lovregulert monopoltjeneste.
        - Lovregulert ansvar.

- Eiendomstakster, prospekter mv:
    - Likheter:
        - Utarbeider opplysninger der en annen enn oppdragsgiver er tilsiktet mottaker av opplysningene - hensikten er at tredjemann skal disponere i tillit til at opplysningene er korrekte.

- Forskjeller:
  - Bruken av opplysningene er i større grad bestemt på forhånd (salg, låneopptak eller refinansiering mv) enn den ubestemte bruk av sertifikater. Forutberegneligheten mht skadepotensiale er større enn for nøkkelsertifikater.

3 MYNDIGHETENES MULIGE ROLLER

Myndighetenes mulige rolle(r) i forbindelse med etablering av sertifikattjenester kan deles opp f eks slik:

- Operatør
- Regulatør
- Kontrollør
- Koordinator
- Finansieringskilde
- Bruker

Nedenfor følger noen betraktninger om enkelte av disse rollene. Dette er utelukkende ment som innspill til debatten og er (som man vil se) ikke på noen måte ment å være uttømmende drøftelser av spørsmålene.

3.1 Operatør

Det vil naturligvis være mulig å fylle flere av rollene samtidig, men det er åpenbart at ikke alle kombinasjoner er like heldige. Ettersom tjenestene utvilsomt vil bli tilbudt i konkurranse mellom ulike leverandører vil det f eks kunne være problematisk om det offentlige skulle opptre både som regulatør, kontrollør og som konkurrerende operatør (organisert innenfor rammen av et offentlig organ). Slikt kan lett skape grobunn for rykter om forskjellsbehandling. Tilsvarende gjelder forholdet mellom finansiering og rollen som konkurrerende operatør. Dersom virksomheten organiseres innenfor rammen av en eksisterende offentlig virksomhet vil det oppstå diskusjon om ”subsidiering” fra statens side og derved skjeve konkurranseforhold som kan hindre adgangen for nye leverandører. Selv om tilfellet ikke skulle rammes av eventuelle forbud mot kryssubsidiering ol tilsier målsetningen om å legge til rette for sunn konkurranse og flere tilbydere at man ikke involverer seg direkte i operativ virksomhet. Man kan imidlertid tenke seg at det offentlige opererer enkelte sentraliserte tjenester som tilbys på like vilkår til alle sertifikatutstedere, f eks rollen som navneautoritet.

Siden rollene som regulatør og kontrollør naturlig (men ikke nødvendigvis) vil falle på det offentlige bør man være varsom med å la det offentlige delta som konkurrerende operatør. Disse motforestillinger gjør seg ikke gjeldene i samme grad overfor statseide selskaper som drives som selvstendige virksomheter (selv om enkelte statseide selskapers fremferd kan gi grunn til ettertanke).

3.2 Regulatør

Det offentlige er naturlig bærere av rollen som regulatør. På den annen side har det på TTP-området vært ytret ønske om selvregulering, markedstilpasning og selvjustis gjennom markedets egne sanksjoner mot tjenester som ikke fortjener tillit. Ulempen med en slik ordning er den lave grad av forutberegnelighet som løsningen gir den alminnelige bruker, i alle fall i en oppbyggingsfase.

En mellomløsning kan være å forankre bransjens selvregulering i en rammelovgivning, slik f eks advokatbransjens regulering og selvjustis (med sine mulige feil og mangler) er forankret i domstolsloven. På TTP-området er det utvilsomt et særskilt behov for dette tatt i betraktning behovet for fleksibilitet mht til teknisk utvikling og standardisering.

3.3 Kontrollør

Det er ikke åpenbart at myndighetene skal ha noen sentral rolle i forbindelse med kontroll av TTP'er.

En mulig kontrollmodell kan være basert på prinsipper om internkontroll og selvdeklarering som følges opp av selskaper som i dag driver IT-revisjon. Revisjonsselskapene kan i sin tur ha en begrenset meldeplikt overfor et dertil egnet offentlig organ, f eks Post- og teletilsynet. På denne måten oppnår man å holde kostnadene ved etablering og gjennomføring av kontroll i virksomhetene og bare i liten grad i offentlig sektor. I tillegg åpner det et marked for kontrollvirksomhet der aktørene selv kan velge kontrollør. For å opprettholde tilliten til systemet i en slik modell kan det være nødvendig å stille særskilte krav til og eventuelt autorisere revisorene som også vil være ansvarlig for at det drives forsvarlig kontroll på samme måte som i dag. Svikt i kontrollvirksomheten kan danne grunnlag for å gjøre erstatningsansvar gjeldende mot kontrolløren.

[Om rollen som kontrollør og løsninger av den se ellers sekretariatets utkast til rapport.]

3.4 Koordinator

Rollen som koordinator og tilrettelegger gjennom sin posisjon som storbruker av tjenester er antakelig den viktigste myndighetene har. Faren er naturligvis at det offentliges valg som storkunde, i alle fall i en tidlig fase, kan virke konkurransevridende. Det er derfor av stor betydning at man holder åpning for ulike løsninger.[7] En sentral side ved dette er at man gjennom storkunderollen sikrer at leverandørene etablerer reelle samtrafikkavtaler (kryssertifisering) som virkelig gjør det mulig å benytte

[7] Forvaltningsnettsamarbeidet synes å ivareta dette.

ulike leverandører. En side ved dette er å få leverandørene til å forplikte seg til å åpne for teknisk samtrafikk også med *senere* leverandører. Likestilling mht de kommersielle vilkår, som f eks bestemmelser om ansvar, er det derimot vanskeligere å påtvinge leverandørene i forhold til nye aktører. Her vil en individuell vurdering av nykommerens ”godhet” (teknisk, administrativt og økonomisk) måtte spille en rolle og den enkelte TTP må antakelig innrømmes en friere stilling enn mht ren teknisk samtrafikk. Det kan ligge en ikke ubetydelig kommersiell risiko i formell anerkjenning av andre tjenesteleverandører.

3.5 Hvem ivaretar sårbarhetsspørsmål?

Teknologiske løsninger, og sikkerhetsteknologi i særdeleshet, foreldes ettersom nye løsninger kommer til. Dette er en utfordring for materiale som skal oppbevares og sikres over lengre tid.

Informasjonstjenester knyttet til en åpen infrastruktur vil også være gjenstand for uvennlige angrep utenfra. For tjenester som har som sin oppgave å "selge tillit" kan spredning av ondsinnede rykter, selv om de ikke er forankret i faktiske forhold, være tilstrekkelig til å sette en tjeneste helt eller delvis ut av spill i et internasjonalt marked. Dersom tjenestene er store og betjener sentrale deler av norsk næringsliv kan dette få samfunnsøkonomiske konsekvenser. Da kan det bli et myndighetsanliggende å sørge for at bedriftene samlet ivaretar tilstrekkelige sikkerhetsmekanismer, jfr de krav som i dag er stillet til etablering av bl a industrivern og som på myndighetenes vegne følges opp av næringslives sikkerhetsorganisasjon (NSO).

Dersom man gjennom myndighetsinitiativ skal bidra til å *forsere* utvikling og etablering av elektronisk kommunikasjon og TTP'er bør følgende spørsmål derfor behandles parallelt:

- Samfunnsøkonomiske og kulturhistoriske utfordringer knyttet til langtidslagring av elektroniske dokumenter og signaturer.
    - Krav til langtidslagring hos den enkelte TTP, herunder prosedyrer for avvikling og sikkerhetsstillelse.
    - Sentraliserte avleveringsordninger av typen "Nasjonal BitBank", jfr prosjekt hos SINTEF Tele- og Data.
- Samfunnsøkonomisk risiko knyttet til at store TTP'er kompromitteres.