Elektroniske signaturer

Myndighetsroller og regulering av tilbydere av sertifikattjenester

1 Sammendrag

EU har vedtatt et direktiv om elektroniske signaturer linkinthoveddel00111. Det tas sikte på at direktivet også skal gjennomføres i Norge ved å innlemme dette i EØS-avtalen.

Bakgrunnen for direktivet er at man i kjølvannet av den økende handel over åpne nett så en uensartet tilnærming for rettslig anerkjennelse av elektroniske signaturer og CSP-virksomhet innen fellesskapet. Dette kunne skape betydelige hindringer for elektronisk kommunikasjon og elektronisk handel.

Direktivet skal sikre en felles rammeverk for elektroniske signaturer, fremme disse, og derved bidra til å harmonisere landenes regelverk omkring denne typen teknologi og derved sikre fri bevegelighet av varer og tjenester i det indre marked. Ved bruk av såkalte avanserte elektroniske signaturer likestilles håndskreven underskrift og elektronisk signatur.

Denne utredningen har sett på regulering av og frivillige godkjenningsordninger for tilbydere av sertifikattjenester linkinthoveddel00122 (CSP'er). I tillegg tar den for seg gjensidig anerkjennelse av digitale sertifikater.

Utredningen forutsetter at leseren har grunnleggende kunnskaper om digitale signaturer med tilhørende tjenester. For en introduksjon til emnet anbefales rapporten " *Digitale signaturer gir tillit til elektronisk kommunikasjon: Forslag til tiltak for aksept og utbredelse*" linkinthoveddel001P15_20663>. Se også kapittel 2.4.

Hovedkonklusjonene fra utredningen er følgende:

- Utvalget anbefaler at det utpekes en offentlig tilsynsmyndighet som skal drive tilsyn med alle CSPer som skal utstede kvalifiserte sertifikater. Se kapittel 7.3.
- Tilsynsmyndigheten legges til Post- og teletilsynet. Hovedgrunnen for dette er at blant annet Sverige, Danmark og Tyskland har valgt sine Post- og teletilsyn som tilsynsmyndighet. Se kapittel 5.7 og 7.3
- Det etableres en registreringsordning for CSPer som tilbyr kvalifiserte sertifikater, se kapittel 5.4.3 og 7.4.
- Utvalget anbefaler at det ikke tas initiativ fra myndighetene til en ordning for en total akkreditert sertifisering av CSPer nå. Utredningsgruppen anser at de eksisterende ordningene for sertifisering av IT-sikkerhet i Norge, sammen med muligheten for IT-revisjoner av CSPer, vil gi et tilstrekkelig grunnlag for å vurdere en CSPs tillitsnivå. Se kapittel 5.4, 7.2.4 og vedlegg 2.
- Utvalget anbefaler at det ikke legges opp til noen regulering av samvirke og/eller gjensidig anerkjennelse mellom CSPene fra myndighetenes side. Samvirke og/eller gjensidig anerkjennelse mellom CSPer gjøres best gjennom avtaler. Se kapittel 4.4 og 7.2.5.

- Utvalget ser positivt på frivillige godkjenningsordninger som blir etablert i markedet, men anbefaler at myndighetene ikke tar noen initiativ til å etablere dette. Se kapittel 6.6 og 7.2.4.

Fotnoter

1 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. linkurlhttp://europa.eu.int/cgi-bin/eur-lex/udl.pl?COLLECTION=lif&SERVICE=eurlex&REQUEST=Service-Search&GUILANGUAGE=en&LANGUAGE=en&DOCID=399L0093_blank Offisiell elektronisk utgave

2 Tilbydere av sertifikattjenester er den norske betegnelsen på uttrykket "certification-service-provider" som benyttes i direktivet. Forkortelsen for dette er CSP. Denne forkortelsen vil også bli benyttet i denne utredningen.

3 En elektronisk utgave finnes på: linkurl/odinarkiv/norsk/dep/nhd/1999/publ/024005-990159/index-dok000-b-n-a.html_blank
http://odin.dep.no/odinarkiv/norsk/dep/nhd/1999/publ/024005-990159/index-dok000-b-n-a.html
Rapporten er utarbeidet av et utvalg nedsatt av det tidligere Rådet for IT-sikkerhet.

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

2 Bakgrunn

2.1. Bakgrunn for utredningen

Rådet for IT-sikkerhet (RITS) har utredet spørsmål som knytter seg til organisering og bruk av digitale signaturer og tjenester fra tiltrodde tredjeparter (TTP) for å legge til rette for sikker elektronisk kommunikasjon. En arbeidsgruppe ble nedsatt for å lage en forberedende utredning. Rapporten linkinthoveddel002P32_39504> ble avlevert til rådet i november 1998. Rådet har drøftet rapporten på et seminar og i to møter. Rådet oversendte rapporten til Nærings- og handelsdepartementet (NHD)den 30. november 1998.

Under behandlingen av rapporten uttalte RITS at det er viktig å komme i gang med å klarlegge rammer og modeller for TTP-virksomhet i Norge. Rådet anbefalte ovenfor NHD at spørsmål vedrørende myndighetsroller, finansiering av autentiseringsvirksomhet og godkjenningsordning og krav til TTP-virksomhet burde utredes nærmere. Som ledd i oppfølgingen på dette punktet bør det nedsettes et utvalg med oppdrag å utrede nærmere de spørsmål som er angitt i mandatet nedenfor.

2.2. Mandatet

Utvalget har fått følgende mandat:

Utredningen innhold

Utredningens innhold skal konsentreres om noen hovedspørsmål som reises i forbindelse med etablering av generelle rammebetingelser for bruk av sikker digital signatur i samfunnet. Flere av de angitte problemstillingene er berørt i rapporten om digitale signaturer. Utvalget skal mer utførlig gå inn i spørsmålene, ta hensyn til ny informasjon som evt måtte foreligge og angi mer presise forslag til anbefalinger. Utvalget skal legge til grunn de føringer som gis i EU-direktivet om felles rammeverk for elektroniske signaturer. Det forutsettes at utvalget i nødvendig grad innhenter synspunkter fra næringsliv/tjenesteleverandører.

Hovedspørsmålene som skal utredes omfatter:

*1. **Frivillig godkjenningsordning for TTP-virksomhet og krav til slik virksomhet.** I rapporten om digitale signaturer anbefales det at det etableres en frivillig ordning som tilbyr TTPer å operere i henhold til autorisasjon/godkjenning ut fra anerkjente kriterier, og at det etableres eller utpekes et offentlig eller privat organ som har ansvar for oppfølging og kontroll av TTP'er som på frivillig grunnlag er blitt godkjent. I det kommende EU-direktivet om elektroniske signaturer pålegges dessuten landene å etablere tilsyn med TTPer som utsteder kvalifiserte sertifikater for offentligheten. Utvalget skal vurdere hvilket tillitsnivå som anses nødvendig for at TTP-virksomhet skal kunne anerkjennes rettslig, og med dette som utgangspunkt legge frem konkrete forslag til hvordan en frivillig godkjenningsordning/og eller tilsynsorgan skal etableres, helst med utgangspunkt i allerede etablerte ordninger. Det vises til utkast til "Direktiv om elektroniske signaturer; og art. 3 og 5 spesielt".*

*2. **Anerkjennelse av sertifikater.** Flere leverandører av sertifikattjenester og eventuelt andre tjenester ventes å være i markedet. Utvalget skal legge frem forslag til hvordan gjensidig anerkjennelse av sertifikater mellom tjenesteleverandører i Norge og i forhold til utenlandske leverandører kan sikres på en hensiktsmessig måte.*

*3. **Typer av roller markedet.** Hvilke roller og oppgaver bør utføres som ledd i forretningsvirksomhet i markedet og hvilke som eventuelt bør utføres av sentrale myndigheter?*

*4. **Finansiering av TTP-virksomhet.** Dersom det offentlige gis ansvar for visse oppgaver knyttet til TTP-virksomhet, hvordan bør de finansieres?*

*5. **Modeller i andre land.** Utvalget skal kort gjøre rede for typiske modeller som er anvendt på spørsmålene 1-4 i andre land, som f eks Danmark, Sverige og England.*

*6. **Økonomiske og administrative konsekvenser** bør så langt som mulig utredes.*

2.3. Bruk av begreper

I mandatet brukes begrepet TTP (tiltrodd tredjepart). Internasjonalt har man gått bort fra dette begrepet. I fagmiljøer og innen standardiseringsorganisasjonene har man betegnet den virksomheten som utsteder sertifikater og vedlikeholder en katalogtjeneste som Certification Authority (CA). Den siste betegnelsen som har kommet er Certification-Service-Provider

(CSP). Dette uttrykket blir brukt i direktivet om tilbydere av elektroniske signaturtjenester/ tilbydere av sertifikattjenester. Vi velger å bruke forkortelsen CSP i rapporten, og oversetter denne til "tilbyder av sertifikattjenester". Når betegnelsen CSP benyttes i det nedenstående er det hovedsakelig den delen av CSPens virksomhet som utsteder, vedlikeholder håndterer og går god for sertifikater som behandles. Særlig viktig er sammenhengen mellom en brukers offentlige nøkkel og brukerens identitet (evt rolle ved bruk av såkalte rollesertifikater). CSP kan imidlertid også omfatte andre tjenester som tidsstempling mv. som vi ikke behandler her. (Se direktivet artikkel 2 pkt 11, samt fortalen pkt 9.)

2.4. Utvalgets sammensetning og arbeid

Utvalget har bestått av:

Olav Torvund, prof. dr. juris, Institutt for rettsinformatikk, UiO (leder) Katarina de Brisis, seniorrådgiver, Arbeids- og administrasjonsdepartementet Tore A. Hauglie, avdelingsdirektør, Den norske Bankforening Arne Dag Hestnes, rådgiver, Post og teletilsynet Torgeir Jonvik, underdirektør, Finansdepartementet Øivind Lunde, Secure Computing AS, Rådgiver IT-sikkerhet, som Norsk Hydros representant. Jens Nørve, rådgiver, Nærings- og handelsdepartementet

Sekretariatet har bestått av:

Halvor Oseid, rådgiver, Statskonsult (prosjektleder) Endre Grøtnes, seniorrådgiver, Statskonsult Peter Bøgh, rådgiver, Statskonsult Som observatører har følgende møtt: Arve Kobbersletten, Nærings- og handelsdepartementet Kari Anne Lang-Ree, Nærings- og handelsdepartementet Thomas Myhr, Nærings- og handelsdepartementet Rolf Riisnæs, Institutt for rettsinformatikk, UiO

Utvalget har hatt 8 ordinære møter, inklusive oppnevningsmøtet. I tillegg er det arrangert et møte mellom utvalget og representanter for leverandører av de aktuelle tjenester.

Torvund og Nørve har deltatt i et nordisk arbeid omkring EU-direktivet om elektroniske signaturer linkinthoveddel002P77_96085> og hvordan dette skal tolkes og implementeres.

Videre har flere av utvalgets medlemmer deltatt på et 2 dagers seminar/workshop om digitale signaturer i regi av Arbeids- og administrasjonsdepartementet. Sekretariatet har fulgt arbeidet for en felles standardisering innen EU omkring elektroniske signaturer; EESSI - European Electronic Signature Standardization Initiative.

Rolf Riisnæs, Institutt for rettsinformatikk har bidratt med to notater samt viktige innspill. Notatene er vedlagt rapporten.

Fotnoter

4 Rådet for IT-sikkerhet: "Digitale signaturer gir tillit til elektronisk kommunikasjon: Forslag til aksept og utbredelse."

5 Directive 1999/93 /EC

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

3 Direktivet

3.1. Status og bakgrunn for direktivet

Fra rammenotat fra NHD, Administrativ og juridisk avdeling 12.01.2000 er gjengitt;

"Direktiv fra Europaparlamentet og Rådet om et felles rammeverk for elektroniske signaturer (98/0191 COD).

1. Bakgrunn og status, samt hovedtrekk i forslaget.

EU-kommisjonen la 13. mai 1998 frem forslag til Europaparlament og Rådsdirektiv om et felles rammeverk for elektroniske signaturer, med utgangspunkt i EF-traktatens artikkel 57(2), 66 og 100A, og iht prosedyren i artikkel 189 B.

Forslaget følger opp en henstilling fra Rådet om å utarbeide et forslag til direktiv, basert på en "Communication to the Council" av 8. oktober 1997. Direktivet ble endelig vedtatt den 30. november 1999 (vedlegg 1). Implementeringstiden for direktivet er 18 måneder etter det blitt publisert i Official Journal."

Bakgrunnen for direktivet er at man i kjølvannet av den økende handel over åpne nett så en uensartet tilnærming for rettslig anerkjennelse av elektroniske signaturer og CSP-virksomhet innen fellesskapet. Dette kunne skape betydelige hindringer for elektronisk kommunikasjon og elektronisk handel.

Det indre markedet skal også sikre fri bevegelighet for personer. Dette medfører at personer i økende grad vil ha behov for å kommunisere med myndigheter i andre land enn der de er bosatt. Elektronisk kommunikasjon vil være til stor nytte i denne forbindelse.

Direktivet skal sikre et felles rammeverk for elektroniske signaturer, fremme disse, og derved bidra til å harmonisere landenes regelverk omkring denne typen teknologi og derved sikre fri bevegelighet av varer og tjenester i det indre marked.

3.2. Direktivets virkeområde

Direktivet omfatter kun de tilfeller hvor landene gir adgang til elektronisk kommunikasjon. Direktivet krever ikke at landene må tillate elektronisk kommunikasjon

Direktivet gjelder i utgangspunktet ikke heller for lukkede systemer - *"systems which are based on voluntary agreements under private law between specified number of participants"* *linkinthoveddel003P109_121456*> - f.eks. innen betalingsformidling. Grensene for hva som skal regnes for lukkede systemer, synes ikke å være helt klart. Imidlertid vil det være hensiktsmessig for direktivets virkeområde å tolke lukkede systemer snevert. Imidlertid er det

uklart, ut over den ovennevte formulering, hvilke kriterier som legges til grunn for å anse et system for lukket.

Direktivet får ikke innvirkning på nasjonal rett (eller fellesskapsretten) vedrørende formkrav, som for eksempel krav til håndskreven underskrift, krav til bestemte dokumenttyper, krav til at avtaler skal inngås skriftlig mv. [linkinthoveddel003P112_127557]> Dette innsnevrer direktivets virkeområde betydelig. (Artikkel 1, samt fortalen pkt 17.)

Direktivet er forsøkt gjort teknologiuavhengig og omhandler elektroniske signaturer generelt, herunder digitale signaturer ved hjelp av offentlig nøkkel infrastruktur (PKI). Per i dag synes løsninger basert på digitale signaturer og offentlig nøkkel infrastruktur med tilhørende CSP-tjenester som det mest aktuelle, men en mulig trend er at biometriske løsninger i større grad vil bli brukt i kombinasjon med digitale signaturer. Også her vil det være nødvendig med en tredjepart som kan verifisere en identitet.

Direktivet har en omfattende "definisjonsliste". Det kan være en viss tvil vedrørende hvilke formuleringer som skal brukes på norsk. Nærings- og handelsdepartementet, ved Administrativ- og juridisk avdeling utarbeider for tiden et lovforslag som implementerer direktivet i norsk rett. Dette forslaget vil inneholde en definisjonsliste.

3.3. Hovedpunktene i direktivet

Direktivet berører flere områder i forhold til utvalgets mandat:

I artikkel 3 heter det at landene ikke kan stille krav om forhåndsgodkjenning av sertifiseringstjenestene. Dette er utdypet i fortalen pkt.10 til også å gjelde "enhver anden foranstaltning med samme virkning."

Men landene kan introdusere frivillige akkrediteringsordninger, Dette er utdypet i fortalen, pkt. 11. Motivet er å høyne tillits-, sikkerhets-, og kvalitetsnivået for CSP-tjenester.

Frivillig akkreditering er definert i artikkel 2 pkt 13. Det er tale om en tredjepartsgodkjenning gitt som tillatelse i form av et sertifikat av et organ som kan være offentlig eller privat. Sertifikatet gir visse rettigheter og plikter som ikke kan utøves før sertifisering er gjort. Alle slike vilkår skal være objektive, åpne, rimelige og ikke-diskriminerende. Frivillige akkrediteringsordninger skal ikke organiseres slik at den svekker konkurransen mellom tilbyderene av sertifikattjenester.

Det er uklart om bestemmelsen skal tolkes til å omfatte akkreditert sertifisering som betyr at sertifiseringsorganet et godkjent av Norsk Akkreditering (etter internasjonale standarder) eller om en mener sertifisering utført av et sertifiseringsorgan som ikke er akkreditert. Akkreditering og sertifisering er utfyllende beskrevet i rapporten kapittel 5.4, samt i vedlegg 2.

Landene må sikre at det opprettes et system for å føre tilsyn med tilbydere av "kvalifiserte sertifikater". Definisjonen av kvalifiserte sertifikater er gitt i artikkel 2 pkt 10, og er et sertifikat som oppfyller kravene i bilag I til direktivet og leveres av en CSP som oppfyller kravene i bilag II.

Dette tilsyn kan være gitt et offentlig organ eller en kan delegere offentligrettslig kompetanse til et privat rettssubjekt. Tilsynet skal opprettes uansett om en har opprettet akkreditert sertifisering eller ikke.

Landene kan dessuten stille tilleggskrav til elektroniske signaturer i offentlig sektor. Kravene skal være objektive, transparente, forholdsmessige og ikke- diskriminerende. I tillegg må kravene ikke hindre grenseoverskridende tjenester til borgerene.

Artikkel 4 inneholder et forbud om ikke-diskriminering. Landene kan ikke foreta begrensninger i bruk eller anerkjennelse av sertifikattjenester med opprinnelse i et annet medlemsland. Landene skal også sikre at elektroniske signaturprodukter, som er i samsvar med direktivet, kan sirkulere fritt i det indre markedet (fri bevegelighet).

Artikkel 5 regulerer rettsvirkningen av elektroniske signaturer. Landene skal sikre at avanserte elektroniske signaturer (som er basert på et kvalifisert sertifikat), anerkjennes på linje med håndskrevne signaturer og kan godtas som bevis i retten. "Artikkel 5 tolket i lys av artikkel 1 innebærer at; dersom det i lov, forskrift eller på annen måte er oppstilt krav om signaturer for at en handling skal få en bestemt rettsvirkning og handlingen kan gjennomføres elektronisk, skal en kvalifisert elektronisk signatur alltid oppfylle et slikt krav. En elektronisk signatur som ikke er kvalifisert *kan* oppfylle et slikt krav."

Landene skal dessuten sikre at elektronisk signatur på et annet nivå ikke fratas rettsvirkning eller nektes fremlagt som bevis bare på grunnlag av at signaturen er i elektronisk form.

For å skape tillit hos de som baserer seg på sertifikatene, har direktivet i artikkel 6 regler om erstatningsansvar for CSPene. Landene skal sikre at en tjenesteleverandør, ved å utstede et kvalifisert sertifikat, er ansvarlig for at informasjon angitt i sertifikatet var korrekt på utstedelsestidspunktet, er i overensstemmelse med direktivets krav, og at det er visshet for at personen som er identifisert i sertifikatet som undertegner var i besittelse av signaturfremstillingsdataene på utstedelsestidspunktet. Imidlertid er tjenesteleverandøren ikke ansvarlig dersom han kan vise at han ikke har vært uaktsom. Det kan angis begrensninger i bruk av sertifikatet, for eksempel en øvre verdigrense. Sertifikatets gyldighet skal linkinthoveddel003P141_179458> være tidsbegrenset. Sertifikattjenesteleverandøren er ikke ansvarlig dersom bruken av sertifikatet går ut over angitte begrensninger eller verdien av transaksjonen overskrider verdigrensen.

Landene skal sikre at kvalifiserte sertifikater utstedt i et tredjeland anerkjennes som rettslig likeverdig med kvalifiserte sertifikater utstedt i EU, dersom tjenesteleverandøren er akkreditert av et medlemsland, eller dersom en tjenesteleverandør i et medlemsland som fyller kravene som er angitt i vedlegg II til direktivet garanterer sertifikatet i samme utstrekning som sitt eget, eller dersom tjenesteleverandøren er anerkjent under et regime etablert ved bi- eller multilateral avtale (artikkel 7).

Landene skal informere Kommisjonen om nasjonale akkrediteringsordninger, navn og adresse på nasjonale organer og akkrediterte tjenesteleverandører, jf artikkel 11.

3.4. Myndighetsoppgaver i henhold til direktivet

Fra direktivet kan vi utlede følgende oppgaver som må eller kan etableres:

Tilsyn:

- Ifølge direktivets artikkel 3 pkt 3 *skal* medlemsstatene sikre at det innføres passende systemer for tilsyn av CSPer som er etablert innenfor statens område og som tilbyr kvalifiserte sertifikater til offentligheten.

Frivillige akkrediteringsordninger:

- Videre følger det av direktivet i artikkel 3 pkt 2 at medlemsstatene *kan* innføre frivillige akkrediteringsordninger(sertifiseringsordninger) av tilbydere av sertifikattjenester på et "høyere" nivå. Det kan ikke utelukkes at nevnte tilsyn og akkreditering skal skje av samme myndighet/organisasjon. Ved diskusjoner med tjenestemenn i EU-kommisjonen (DG XIV) trekker det i retning av at EU mener at det bør være samme myndighet. Men både Sverige og Irland har vurdert det slik at tilsyn og akkreditering bør skilles, og akkrediteringsorganet ønsker ikke oppgaven å utføre det myndighetspålagte tilsynet. Utvalget mener det er viktig å skille tilsyn og akkreditering ut fra at tilsyn er obligatorisk mens akkreditering skal være en frivillig ordning og et verkøy for virksomheten.

Krav til personvern:

- Direktivets artikkel 8 pkt 1 *krever* at medlemsstatene sikrer at CSPer, akkrediterings- og tilsynsorganer oppfyller kravene om personvern etter direktiv 95/46/EF. Dette direktivet er implementert i den foreslåtte lov om behandling av personopplysninger Ot. prp nr 92 (1998-99), og gir Datatilsynet kompetanse som tilsynsmyndighet. Tilsynsmyndighet for personvern tilligger Datatilsynet og dette bør ikke endres. At den enkelte CSP er underlagt forskjellige forvaltningsorganers tilsyn er i henhold til vanlig praksis i Norge.

Kvalitetssikringsorgan:

- Egnede offentlige eller private organer, som utpekes av medlemslandet, *avgjør* om sikre signaturgeneringssystemer oppfyller kravene i anneks III. I Norge er Forsvarets Overkommando/sikkerhetsstaben (FO/s) utøvende myndighet for sertifisering av IT-sikkerheten til produkter og systemer. Det er altså FO/s som utsteder sertifikater til de produkter som har vært gjenstand for evaluering av et evalueringsorgan. Evalueringsorgan blir akkreditert av Norsk Akkreditering som teknisk laboratorium etter EN 45001. Se også vedlegg 2.

3.5. EESSI (European electronic signature standardization initative)

Hovedformålet for etableringen av EESSI er å få utredet hvordan standardisering kan bidra til gjennomføringen av direktivet om elektroniske signaturer.

Direktivet om elektroniske signaturer er et såkalt "ny metode" direktiv. Det betyr at direktivet bare setter opp rammer for kvaliteten på produkter og tjenester, mens det er opp til standardiseringsorganisasjonene og industrien å fylle rammene og etterse at produkter og tjenester er i samsvar med direktivet. Standarder som antas å oppfylle direktivet blir publisert i Official Journal.

Den vanligste formen for samsvarsvurdering for "ny metode" direktiver er egenkontroll og egenerklæringer. Produkter som kan medføre stor risiko for helse og sikkerhet skal derimot i

normaltilfellet kontrolleres av en tredjepart. Det samme gjelder når en produsent ikke har brukt harmoniserte standarder eller det ikke finnes slike standarder.

Industrien og de europeiske standardiseringsorganisasjonene har innenfor rammene av ICTSB linkinthoveddel003P166_221629> blitt bedt av kommisjonen å analysere framtidige behov for standardisering for å støtte opp under direktivet om elektroniske signaturer og spesielt de kravene som er stilt i anneksene til direktivet.

Det er utformet et standardiseringsmandat og Kommisjonen har bevilget penger til dette arbeidet.

For å møte kravene i Kommisjonenes standardiseringsmandat har ICTSB etablert "the European electronic signature standardization initiative" (EESSI).

Det er opprettet en styringsgruppe for det videre arbeidet med EESSI. Styringsgruppen består av representanter for ICTSB, Kommisjonen, industrien og eksperter på området.

Første del av EESSI-arbeidet var å utarbeide en rapport som beskrev status på området og som pekte på en del områder hvor det var behov for framtidig standardisering. Rapporten forelå 20. juli 1999 linkinthoveddel003P175_2338310>.

Rapporten peker ut en rekke områder hvor det er behov for å finne fram til standarder for å tilfredsstille direktivet. Områdene/tiltakene er gruppert etter hvor viktig det er, eller hvor mye det haster å få fram standarder på området.

De viktigste områdene er som følger:

1. Finne et første sett med komponenter som tilfredsstiller rammeverket for kvalifiserte elektroniske signaturer. (Direktivet er teknologinøytralt, men for å standardisere må man velge konkrete teknologier. I dette tilfellet har man valgt digitale signaturer som løsning.) 2. Spesifikasjoner av sikkerhetskrav for "trusthworthy systems linkinthoveddel003P181_2404811>" som benyttes av CSPer som utsteder kvalifiserte sertifikater. 3. Spesifikasjoner av sikkerhetskrav for maskinvare som benyttes som "sikkert signaturframstillingssystem linkinthoveddel003P183_2426712>". 4. Standard for bruk av X.509 sertifikater som kvalifisert sertifikat. 5. Et system for registrering/vurdering av "samsvarsvurdering" av produkter og tjenester for elektroniske signaturer 6. Utvikle krav til administrasjon og drift av CSPer samt krav til sertifikatpolicy og sertifikatutstedelsespraksis. 7. Spesifikasjoner og retningslinjer for signaturframstillings- og signaturverifikasjonsprodukter.

Det videre EESSI arbeidet er delt mellom CEN-ISSS og ETSI. Punktene 1, 2, 3, 5 og 7 ivaretas av CEN mens ETSI ivaretar punkt 4 og 6. Arbeidet koordineres av styringsgruppen. CEN og ETSI vil ha samlokaliserte møter og vil rapportere på hverandres møter for å unngå dobbeltarbeid og ulike standarder.

Både CEN og ETSI har etablert arbeidsgrupper og er i ferd med å leie inn eksperter for å gjøre grunnarbeidet.

I løpet av 9 måneder håper man å komme opp med de første standardene som kan offentliggjøres i Official Journal.

Ser man på de områdene som det er satt igang arbeid på for å komme fram til standarder, vil det være naturlig å vurdere dette som delområder hvor man kan stille krav om sertifisering, eller en annen form for samsvarsvurdering.

Tanken med arbeidet er at det er mulig å stille ulike sett med krav på de forskjellige områdene, og at det kan etableres krav og bli foretatt samsvarsvurderinger på det enkelte området uavhengig av kravene på de andre områdene. Dette er vanlig på produktområdet. Et eksempel er at kravene til sikre signaturframstillingssystemer kan etableres uavhengig av hvilke krav man setter til driften av en CSP.

Resultatene fra disse arbeidsgruppene vil være et sett med standarder som oppfyller vilkårene i direktivet. Disse standardene kan være et grunnlag for vurdering av CSPer også i Norge.

3.6. Andre lands implementering av direktivet

3.6.1. Danmark

Danmark har gjennom flere år i regi av Forskningsministeriet arbeidet med et lovforslag om elektroniske signaturer. Det foreliggende forslag linkinthoveddel003P204_2626113> er sendt på høring med høringsfrist ultimo januar 2000. Det tas sikte på at loven skal tre i kraft fra 1. januar 2001.

Det foreliggende utkast til lov om elektroniske signaturer uttaler at:

" *loven innheholder bestemmelser der gennemfører dele av Rådet og Parlamentets direktiv nr. .....om en fellesskapsramme for elektroniske signaturer..."*

Det er ikke helt klart for oss hvilke deler av direktivet som lovutkastet ikke omhandler.

CSPen, som i utkastet omtales som "nøglesenter" har krav til seg om å sikre pålitelige og velfungerende tilbud av kvalifiserte sertifikater ved løpende sikre juridiske, organisatoriske, tekniske, personalmessige, drifts- og sikkerhetsmessige foranstaltninger. Dette er utdypet i litra videre i bestemmelsen (§7).

Det stilles blant annet krav til *"tilstrekkelige økonomiske ressourcer "* for å drive denne type virksomhet og krav til valg av *ekstern statsautorisert revisor* til systemrevisjon. Tilstrekkelige økonomiske ressurser følger for øvrig direkte av direktivet.

En stiller krav om *registrering* av virksomheten når en *utsteder kvalifiserte sertifikater.* Registrering skjer hos Telestyrelsen. Innholdet i registreringen omfatter navn, hjemsted, selskapsform, ledelse og revisjon. Registreringen skal også omfatte rapport om at nøglecenteret overholder de plikter loven pålegger dem (kapittel 3) Denne skal sendes årlig, samt ved rett etter oppstart av virksomheten

Telestyrelsen skal fungere som tilsynsmyndighet for de nøkkelsentere som tilbyr kvalifiserte sertifikater, samt ellers sørge for at loven overholdes.

Hovedoppgaven for tilsynsmyndigheten er å foreta en vurdering av de revisjonsrapporter som et nøglesenter skal sende tilsynsmyndigheten. På denne måten unngår en oppbygging av en omfattende og kostbar tilsynsmyndighet, samt at de tilsynsbelagte virksomheter svarer

utgiftene i forbindelse med virksomheten. (Det offentlige kan imidlertid påvirke utbyggingen av tjenesten ved å gi økonomiske tilskudd, direkte og indirekte.)

Sanksjonspanoramaet tilsynsmyndigheten besitter består av blant annet av;

- Rett til å kreve relevante opplysninger
- Gi pålegg om å rette opp konkrete forhold
- Gi pålegg om ekstraordinær revisjon
- Foreta stedlig kontroll
- Kompetanse til å frata CSPen retten til å utstede kvalifisert sertifikat.

3.6.2. Sverige

Sverige sendte i primo desember sitt forslag til lov om elektroniske signaturer ut på høring.
linkinthoveddel003P227_2867614>

Utkastet omfatter definisjoner, krav til kvalifisert sertifikat, krav til sikre anordninger for signaturfremstilling, krav til tilbyder av kvalifiserte sertifikater om å melde fra til tilsynsmyndigheten om at en utsteder slike sertifikater, regler om erstatningsansvar mv.

Lovforslaget er overveiende likt det danske forslaget, men er noe mindre detaljert. For eksempel er det ikke krav til at tilbyder av kvalifiserte sertifikater må sende inn en IT-revisjonsrapport til tilsynsmyndigheten. Imidlertid er det gitt en vid kompetanse for tilsynsmyndigheten til å utforme forskrifter vedrørende CSPens virksomhet, jf lovutkastets § 12 .

CSPen må ha tilstrekkelig finansiell styrke til å kunne møte eventuelle erstatningskrav, jf § 9. Dette følger jo også av direktivet, jf annex II.

Tilsynsmyndigheten er gitt kompetanse til å kreve de opplysninger som er nødvendige for å ivareta sin tilsynsfunksjon. De har også adgang til å drive stedlig kontroll, fatte de vedtak som er nødvendig for etterlevelsen av bestemmelsene, samt kompetanse til å kreve at virksomheten opphører hvis CSPen ikke følger pålegg gitt av tilsynsmyndigheten.

Tilsynsmyndigheten foreslås lagt til Post- og telestyrelsen, jf kap 7 i lovmotivene. Her er flere aktuelle organer presentert, som for eksempel Datainspeksjonen, Styrelsen for ackreditering och teknisk kontroll, Patent- och registreringsverket, Riksskatteverket mv. Motivene diskuterer fordeler og ulemper ved de aktuelle kandidater ut fra hvilke oppgaver og funksjoner organene har i dag.

Ingen av lovforslagene utvalget har sett på foreslår å opprette et nytt tilsynsorgan.

3.6.3. Finland

Det foreligger ikke et lovforslag for implementering av direktiv om elektroniske signaturer ennå, men Finland har i høst vedtatt en lov om elektronisk saksbehandling i forvaltningen, samt en lov om elektroniske borgerkort. Borgerkortet inneholder en elektronisk signatur og er ment benyttet i elektronisk kommunikasjon med forvaltningen. Per i dag kan kortet kun anvendes ved melding om flytting til det finske "folkeregisteret", men tilbudet vil utvides ettersom forvaltningsinstitusjonene legger til rette for denne kommunikasjonsformen.

3.6.4. England

England har laget et forslag til regulering av elektronisk handel inklusive elektroniske signaturer " *A Bill to Make provision to facilitate the use of electronic communications and electronic data storage; ...*".

Lovforslaget legger opp til en registrering av kryptografiske tjenestetilbydere " *providers of cryptography support services*".

Det spesifiseres ikke hvem som skal ha ansvar for denne registreringen.

Det skal også etableres ordninger for godkjenning av disse tilbyderne " *arrangements in force for granting approvals*". Det er heller ikke spesifisert hvordan denne godkjenningen skal være.

I forbindelse med godkjenning av tjenestetilbydere er det fremmet et forslag om en frivillig godkjenningsordning drevet av markedet selv. Denne ordningen kalles tScheme. Se kapittel 6.6 for mer informasjon om ordningen.

3.6.5. Spania

Beskrivelsen av det Spanske lovforslaget er tatt med fordi dette var det første lovforslaget som utvalget ble gjort kjent med.

Med utgangspunkt i den engelskspråklige utgaven av utkast til lov om elektroniske signaturer kan følgende kort sies om registreringsordningen i Spania:

Det opprettes et register over CSPer. Registeret legges under Justisministeriet.

Alle tilbydere må søke om innregistrering før oppstart (artikkel 7 samt en egen generell overgangsbestemmelse om at de som allerede er i gang må rette seg etter lovens bestemmelser innen ett år). Registreringsplikten inngår som ett av diverse pålegg som myndighetene retter mot CSPer.

Eventuelle frivillige akkrediterte sertifiseringer skal føres i registeret.

Registeret er offentlig. Det kan utarbeides nærmere forskrifter om gebyr ved utlevering av opplysninger.

Ved opphør av virksomheten må melding om dette sendes registeret. Vedkommende tilbyder skal slettes fra registeret. Justisministeriet tar ansvar for den informasjonen som skal oppbevares for ettertiden i 15 år.

Lovutkastet inneholder en mengde bestemmelser om konsekvenser av lovbrudd, herunder bøter. Lovbruddene er gradert etter alvorlighetsgrad. Overtredelse av bestemmelsen om påbudt innregistrering har en lav alvorlighetsgrad. Alvorlige og svært lovbrudd vil bli ført i registeret. Dersom svært alvorlige lovbrudd gjentar seg to eller flere ganger, vil CSPen bli slettet fra registeret.

Fotnoter

6 Jf direktivets fortale pkt 16

7 Direktivforslaget om elektronisk handel derimot tar sikte på et høyt integrasjonsnivå i Fellesskapet gjennom reguleringer av rettslige rammer innen elektronisk handel. Se forslaget: http://europa.eu.int/comm/dg15/en/media/eleccomm/com427en.pdf

8 Slik tolker både den svenske og danske lovkonsipist direktivet.

9 ICSB - The Information and Communication Technologies Standards Board - er en sammenslutning av de tre europeiske standardiseringsorganisasjonene CEN (European Committee for Standardization), ETSI (The European Telecommunications Standards Institute) og CENELEC (European committee for electrotechnical standardization) med full deltakelse av andre organisasjoner som utformer spesifikasjoner og standarder.

10 EESSI Final report of the EESSI expert team. 20 july 1999.

11 Direktivet Anneks II omtaler "Trustworthy systems"

12 Direktivet anneks III omtaler "secure signature creation-device"

13 http://www.fsk.dk/cgi-bin/doc-show.cgi?doc_id=19206

14 http://naring.regeringen.se/propositioner_mm/pdf/ds99_73.pdf

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

4 Roller og oppgaver i forbindelse med CSP-virksomhet

4.1. Roller i forbindelse med CSP-virksomhet

CSP-virksomhet omfatter mange ulike oppgaver og roller. Med CSP-virksomhet mener vi i denne rapporten all virksomhet som har med generering, utstedelse, håndtering og vedlikehold av digitale sertifikater som knytter en brukers offentlige nøkkel til en identitet eller rolle linkinthoveddel004P279_3351315>. Det kan være en eller flere virksomheter som til sammen utfører de oppgavene som må til for å utstede et digitalt sertifikat. linkinthoveddel004P280_3368716>

CSPens hovedoppgave er å verifisere den identiteten (autentisere) som er presentert i et digitalt sertifikat og signere sertifikatet slik at det oppstår en binding mellom en brukers offentlige nøkkel og identiteten (eller rollen ved bruk av rollesertifikater), dvs skape tillit til det digitale sertifikatet. CSPene må sørge for at sertifikatene ikke kan endres, at det finnes en oversikt/database over godkjente sertifikater, at sertifikater kan trekkes tilbake, at de som får utstedt sertifikater blir identifisert på en forsvarlig måte, at unikt navn benyttes i sertifikater, etc.

De ulike roller og oppgaver kan deles opp på mange måter, og organiseringen av virksomheten kan variere. De ulike rollene er mer inngående drøftet i Rolf Riisnæs notat, vedlegg 4.

Et eksempel på roller og oppgaver for de administrative funksjonene hos en CSP-virksomhet kan man finne i anbudsmaterialet for digitale signaturer, tiltrodde tredjepartstjenester og meldingskryptering i Forvaltningsnettprosjektet linkinthoveddel004P287_3473017>anbudsutlysning for 1999. Der står det:

"For den administrative funksjonen er rollene:

- *Registreringsautoritet (RA), som står for kontakten med brukerne, mottar og validerer forespørsler om sertifisering, og genererer sertifiseringsforespørsler,*
- *Sertifiseringsautoritet (SA), TTP-tjeneste som behandler sertifiseringsforespørsler og utsteder sertifikater,*
- *Smartkortleverandør / -produsent,*
- *Nøkkelgenerator for par av offentlig / privat nøkkel,*
- *Nøkkeldeponi for sikkerhetskopiering av private nøkler som skal brukes til dekryptering,*
- *Katalog for lagring av sertifikater og tilbakekallingslister."*

En annen mulig oppdeling finnes vi Rolf Riisnæs notat om " *TTPens ulike roller*".

- Registeringsenhet
- Sertifikatutsteder
- Policyforvalter
- Sertifikatrot
- Nøkkelgenerering
- Sertifikatdatabasevert
- Brukerstøtte- og varslingstjeneste
- Markedsføring og merkebygging

Noen forutsetninger for utstedelse og bruk av digitale sertifikater i åpne linkinthoveddel004P308_3568318> nett.

- Et digitalt sertifikat skal være signert av en CSP, dvs det er CSPens navn som står i sertifikatet (i feltet "issuer"). Det er CSPen som brukeren har en avtale med linkinthoveddel004P310_3603619> . En CSP kan overlate til andre å utføre det praktiske arbeidet med å lage nøkler, generere sertifikater, drifte en sertifikatkatalog, med mer. CSPen har da en operatør som utfører de praktiske oppgavene.
- Et sertifikat må entydig identifisere personen eller rollen som sertifikatet er utstedt til.
- Det må være mulig verifisere identiteten ut fra opplysningene i sertifikatet.
- Sertifikater kan ikke endres, de kan bare tilbakekalles og utstedes på nytt.
- Et signert sertifikat er en binding mellom en offentlig nøkkel og et sett med attributter, f.eks. navn på den sertifikatet er utstedt til og bruksområde for sertifikatet, på et gitt tidspunkt. Hva bindingen er, og hva attributtene betyr, kan man kun finne ut ved å se på utsteders (CSPens) *sertifikatpolicy*. Se kapittel 4.3.
- Partene i en utveksling av digitale signaturer trenger ikke være kjent for hverandre eller ha sertifikater fra samme CSP.

4.2. Slik opererer en CSP

Det kan være forskjell på hvordan sertifikater utstedes, om det utstedes til private eller utstedes til enkeltpersoner i en virksomhet. En privatperson tar gjerne kontakt med en CSP direkte mens en ansatt gjerne har kontakt med en CSP gjennom sin arbeidsgiver.

For å komme i kontakt med kunder må en CSP ha en eller flere registreringsenheter som kunden kan ta kontakt med for å "søke" om å få utstedt et digitalt sertifikat. Registreringsenheten kan være et fysisk eller et virtuelt sted, for eksempel et nettsted. Disse registreringsenhetene kan drives av CSPen selv, eller av andre. Registreringsenhetenes oppgave er å identifisere kunden og sjekke at de opplysningene kunden gir er korrekte. Deretter sender registreringsenheten disse opplysningene over til CSPen. Når det gjelder utstedelse av sertifikater på høyt sikkerhetsnivå vil det være nødvendig med personlig oppmøte ved registrering eventuelt ved utstedelse av nøkler. Dette vil være beskrevet i sertifikatpolicyen.

CSPen sjekker igjen at de opplysningene de mottar er korrekte. Deretter finner CSPen ut hvilken informasjon som skal med i sertifikatet linkinthoveddel004P323_3826020>. En CSP sitter ofte med mer informasjon om personene som skal identifiseres i et digitalt sertifikat enn det som framgår av sertifikatet linkinthoveddel004P324_3853921>.

Brukeren skal ha et "kort" som inneholder et sett med private og offentlige nøkler. Genereringen av disse nøklene kan skje hos en ekstern kortprodusent, hos CSPen eller hos kunden. Uansett hvor og hvordan nøkkelparene genereres må CSPen sørge for at de er sikre på at den offentlige nøkkelen på det digitale sertifikatet er den samme som den offentlige nøkkelen kunden har på sitt "kort".

Etter at sertifikatet er utstedt må det plasseres i en katalogbase hvor andre kan få tak i det, slik at de kan sjekke at sertifikater de mottar er gyldige. Drift av disse sertifikatkatalogbasene kan gjøres av CSPen selv eller overlates til andre. CSPen må sørge for at de har et system for tilbakekallelse av sertifikater og plassering av nye sertifikater i sertifikatkatalogen.

I tillegg trenger kunden ofte program- og maskinvare hos seg selv for å kunne nyttiggjøre seg det digitale sertifikatet, dvs signere og verifisere signaturer.

Fra beskrivelsen ovenfor ser vi at det er mange oppgaver i forbindelse med utstedelse av digitale sertifikater. Signering av sertifikater og utsendelse og tilbakekalling av sertifikater i en sertifikatkatalog er CSP-virksomhet i henhold til direktivet. Generering av nøkler og drift av sertifikatkataloger vil også være CSP-virksomhet etter direktivet. Det er ikke klart om *registreringsenhetene* vil bli betegnet som CSP-virksomhet.

4.3. Sertifikatpolicy og sertifikatutstedelsespraksis

Et viktig element når man skal vurdere hvor godt og sikkert en CSP er drevet, er å se på virksomhetens sertifikatpolicy og sertifikatutstedelsespraksis.

En *sertifikatpolicy* er regler for hvordan digitale sertifikater utstedes og behandles, og hvem som har ansvaret for sikkerheten ved dette. Sertifikatpolicyen fastsetter altså sikkerhetsnivået for tjenesten og derigjennom tillitsnivået. En CSP vil ofte ha flere sertifikatpolicyer som den opererer etter. Dette for å tilfredsstille kundenes ulike behov for tillitsnivå. For eksempel avgjør policyen om en bruker trenger å møte fram personlig for å få utstedt et sertifikat eller ikke.

En sertifikatpolicy vil vanligvis omfatte blant annet følgende elementer: Organiseringen av CSPens virksomhet, CSPens generelle forpliktelser, hvordan identitetskontroll ved utstedelse av sertifikater foregår, operasjonelle krav til driften, hvordan de fysiske og administrative sikkerhetstiltakene gjennomføres, hvilket teknisk sikkerhetsnivå tjenesten operer på og hvilke sertifikatprofiler linkinthoveddel004P346_6093722> og tilbakekallsesprofiler tjenesten støtter. Et eksempel på en sertifikatpolicy er Forvaltningsnettsamarbeidets sertifiseringspolicy (FSP - 1:1.0 linkinthoveddel004P347_6117823>).

En *sertifikatutstedelsespraksis* sier noe om den praksisen en CSP følger når den utsteder sertifikater. En CSP utsteder gjerne en beskrivelse av denne praksisen i en "Certification Practice Statement". Det er mulig å ha flere sertifikatutstedelsespraksiser som tilfredsstiller den samme sertifikatpolicyen. (Det er ikke gitt at det kun er en måte å løse et problem på.)

Ved en vurdering av sikkerhetsnivået hos en CSP ser man først på om den sertifikatpolicyen CSPen benytter er hensiktsmessig. Deretter ser man på om sertifikatutstedelsespraksisen er i henhold til sertifikatpolicyen. Det siste man må se på er om sertifikatutstedelsespraksisen er gjennomført slik den er beskrevet.

En sertifikatpolicy og en sertifikatutstedelsespraksis kan være utarbeidet i henhold til internasjonale standarder, et eksempel er RFC 2527 linkinthoveddel004P354_6213124>.

CSPen kan også operere etter internasjonale standarder, for eksempel BS 7799 linkinthoveddel004P356_6236625>, når det gjelder deler av sin virksomhet. Det vil si at en CSP kan basere deler av sin virksomhet på internasjonale standarder og la være der det ikke finnes tilfredsstillende standarder. Per i dag finnes det ikke internasjonale standarder som dekker alle aspekter av en CSP virksomhet.

Innholdet i en sertifikatpolicy kan også henvise til at produktene som benyttes er i henhold til internasjonale standarder. Det er ofte disse standardene som er utgangspunkt for etterfølgende kontroll, sertifisering eller tilsyn fra myndigheter og andre. EESSI-rapporten søker å identifisere disse standardene.

Nærmere beskrivelser av sertifikatpolicy og sertifikatpraksis og tilhørende standarder er gitt i vedlegg 1.

Figur 2- Forholdet mellom sertifikatpolicy og -utstedelsespraksis og mulige kontrollformer

Den vanligste formen for revisjon i dag, er mellom beskrevet praksis og virkelig praksis. Det er kun i spesielle tilfeller at man velger å kontrollere om beskrevet praksis er i henhold til

sertifikatpolicy. Et eksempel på det siste er den revisjonen som er utført i Forvaltningsnettsamarbeidet.

4.4. Gjensidig anerkjennelse av sertifikater og samvirke mellom CSPer

Mandatet, samt direktivet, omtaler *gjensidig anerkjennelse* av sertifikater Det er uklart hva dette begrepet inneholder. Noen muligheter er:

- At sertifikater blir anerkjent rettslig på tvers av leverandører, teknologier og landegrenser.
- At myndighetene, en virksomhet eller en privatperson godtar sertifikater fra andre enn "sin" leverandør.
- At en leverandør anerkjenner sertifikater fra en annen leverandør som like sikre som sine egne.
- At sertifikatene *teknisk* kan utveksles mellom ulike leverandører, slik at kunden kun får et eller et fåtall systemer å forholde seg til; såkalt teknisk interoperabilitet.

Høyst sannsynlig dreier gjensidig anerkjennelse seg ikke om krav om teknisk interoperabilitet, men om at sertifikater skal godtas rettslig av myndighetene i det enkelte land.

Det først kulepunktet vil bli tilfredsstilt når CSPene utsteder "kvalifiserte sertifikater" i henhold til direktivet. Disse må anerkjennes rettslig på tvers av landegrenser og CSPer. Dette må innarbeides i det enkelte lands lovgivning.

Det andre kulepunktet har med den enkeltes tillit til et gitt sertifikat å gjøre og vil ikke kunne reguleres. De øvrige kulepunktene kan det være mulig å regulere eller gi føringer for.

Det tredje og fjerde kulepunktet omhandler mer frivillige ordninger for å skape et helhetlig marked for bruk av digitale sertifikater og en tilhørende PKI. Dette vil omtales nærmere i neste kapittel.

4.4.1. Anerkjennelse av sertifikater mellom CSPer og utvikling av teknisk interoperabilitet

Følgende muligheter for gjensidig anerkjennelse av sertifikater mellom CSPer kan tenkes linkinthoveddel004P383_6514126:

- Kryssertifisering på frivillig basis mellom CSPene. Slike gjensidig anerkjennelse vil kunne baseres på avtaler mellom partene som inngår.
- Rot-CSP som går god for de øvrige CSPene. Alle CSPene opererer etter den samme sertifikatpolicyen eller sertifikatpolicyer som rot-CSPen anerkjenner.
- Nasjonal myndighet som går god for CSPer. Alle må akseptere sertifikater fra en CSP som myndighetene går god for. CSPene operer etter en (av flere) sertifikatpolicy som myndighetene har godkjent.

Må det være *gjensidig* anerkjennelse? Det kan tenkes at en CSP godtar sertifikater utstedet av en annen CSP som stiller høyere krav, men at den CSPen som stiller høyest krav ikke godtar sertifikater fra en CSP med lavere krav.

Når det gjelder teknisk samvirke er det et par hovedmomenter å vurdere.

Det ene er hvilke opplysninger partene skal ha tilgang til hos hverandre, og det andre er hvor og i hvilken form tilgang skal gis.

Noen typer informasjon som det kan være ønskelig å få tilgang til er:

- Tilgang til tilbaketrekkingslister og /eller sertifikater.
- Tilgang til hverandres databaser.
- Tilgang til annen kataloginformasjon vedrørende sertifikatet eller den sertifikatet er utstedt til.

Mandatet sier at utvalget skal komme med forslag til hvordan gjensidig anerkjennelse av sertifikater mellom leverandører kan sikres. I utgangspunktet kan ikke det offentlige pålegge CSPer å anerkjenne sertifikater utstedt av andre CSPer (innenlandske og utenlandske) eller samordne tjenesten sin med andre.

Regjeringens strategi er at utviklingen på feltet skal være markedsdrevet og teknologiuavhengig linkinthoveddel004P401_6681027>. For kundene er det ønskelig at han kan nå så mange som mulig med sitt digitale sertifikat. Det kan bli et markedskrav at leverandørene samordner sine tjenester. Behovet fra kundene om en integrert tjeneste mellom leverandørene taler for å integrere krav til gjensidig anerkjennelse av sertifikater i det sett med krav som for øvrig vil bli stilt til CSPer, for eksempel i forbindelse med eventuell frivillig sertifisering eller i forbindelse kravspesifikasjoner. Slike krav kan både gjelde vilkår som skal være tilstede for at en CSP skal kunne anerkjenne enn annen CSP, og under hvilke omstendigheter en CSP ikke kan nekte anerkjennelse av en annen CSP.

I Forvaltningsnettsamarbeidet har man regulert samvirke mellom CSPer gjennom en avtale.

Noen mulige tekniske måter å skape et felles samvirkende system på er: 1) kontinuerlig tilgang til samarbeidende CSPers informasjonssystem (database); 2) regelmessig overføring av aktuelle opplysninger til hver enkelt CSPs informasjonssystem; eller 3) regelmessig overføring av aktuelle opplysninger til særskilt (felles) informasjonssystem.

For mer informasjon om samvirke mellom CSPer se Rolf Riisnæs' notat vedlegg 5.

Utredningsgruppens anbefalinger på området er at det ikke legges opp til noen regulering av samvirke og/eller gjensidig anerkjennelse mellom CSPene fra myndigheten, når myndigheten er en regulatør eller kontrollør. Samvirke og/eller gjensidig anerkjennelse mellom CSPer gjøre best gjennom avtaler. Her har brukerne (markedet) en viktig oppgave. Det er brukerne som kan tvinge fram samarbeidsformer mellom de ulike leverandørene gjennom de krav de stiller som kunde.

Dog vil konkurransemyndighetene selvfølgelig overvåke konkurranseregelne slik at ikke nye tilbydere av sertifikattjenester i praksis stenges ute fra markedet ved at det oppstår kartelldannelser som utestenger nye aktører fra markedet.

4.5. Aktører i markedet

Siden CSP-markedet er under utvikling er det uklart hvilke aktører som vil opptre framover. Tjenestene som tilbys er også under utvikling. Dette gjør at det er vanskelig å si noe sikkert

om de aktørene og de produktene som vil finnes i tiden framover. Utvalget har tatt kontakt med de aktørene som for tiden opptrer i markedet for å høre deres synspunkter.

Disse er:

- Posten SDS
- Telenor
- Fellesdata
- Bankenes betalingssentral (BBS)
- Strålfors/Merkantildata

Det er avholdt individuelle møter med de fire førstnevnte. De andre på listen var invitert, men kunne ikke stille opp. På bakgrunn av de uforbindtlige synspunktene som ble gitt, kan følgende synspunkter fremheves:

- Ingen av aktørene tilbyr kvalifiserte sertifikater i dag.
- Markedet er umodent (kanskje bortsett fra Forvaltningsnettsamarbeidets tilbud).
- Det er uvisst hva fremtidig marked vil være for kvalifiserte sertifikater. Dette tilsier at man ikke etablerer kompliserte og dyre tilsynsordninger.
- Et offentlig tilsyn vil neppe kunne skaffe seg nok kompetanse alene, men vil være avhengig av rapporter fra andre.
- Leverandørene er i stor grad allerede undergitt ulike former for revisjon og kontroll.
- Det offentlige kan være en pådriver ved selv å ta i bruk kvalifiserte sertifikater.

Fotnoter

15 Det vises til pkt 2.2 Presisering av mandatet

16 Se også Vedlegg 4; Tiltrodde tredjepartstjenester

17 http://forvaltningsnett.dep.no/

18 Åpne nett fordrer krav om tillit under upersonlige forhold, og står i motsats til lukkede nett der partene er kjent for hverandre. Se direktivets fortale pkt 16 om lukkede nett.

19 I arbeidsforhold vil brukeren være arbeidsgiveren og den som står i et kontraktsforhold/kundeforhold til CSPen. Den enkelte arbeidstaker har normalt ikke et kontraktsforhold til CSPen.

20 Sertifikater utstedt etter standarden X.509 v3, gir utstederen stor frihet i å velge hvilke attributter som ønskes tatt med i et sertifikat.

21 Typisk vil et personnummer ikke være representert i sertifikatet, men ligge lagret hos utstederen.

22 Regler og retningslinjer vedrørende for eksempel x.509 sertifikater, om bruk av navnefelt mv.

23 Rapport 8/99 - august 1999 Forvaltningsnettsamarbeidet Se også: http://forvaltningsnett.dep.no/ Bestill rapporter - gå til 1999.

24 Standard fra Internet Enginering Task Force "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," March 1999

25 Se vedlegg 1 og 2 for mer informasjon.

26 Dette avsnittet bygger i stor grad på Rolf Riisnæs sitt notat som er presentert i vedlegg 5.

27 Se Stortingsmelding nr. 41 (19998-99) Om elektronisk handel og forretningsdrift, side 11.

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

5 Myndighetenes tiltak og mulige regulering av CSP-virksomhet

Hvilke tiltak myndighetene setter i verk for å regulere området avhenger av flere faktorer. En faktor er hvilke hensyn det offentlige har for å gripe inn i markedet (kapittel 5.1), en annen faktor er hvilken rolle det offentlige innehar og ønsker å fremme (kapittel 5.2). En tredje faktor er hvilke kriterier og verdivalg som legges til grunn for markedsutvikling og regulering (kapittel 5.3).

Myndighetene kan bruke ulike kontroll- og tilsynsformer, og kombinasjoner av disse. Nedenfor er kontroll- og tilsynsformene definert og beskrevet (kapittel 5.4). Videre er aktuell finansieringsform behandlet (kapittel 5.6), og det foretas en drøfting av om det bør være sektorvis eller felles tilsynsmyndighet (kapittel 5.5). Avslutningsvis er nåværende myndighetsaktører beskrevet (kapittel 5.7)

5.1. Hensyn for myndighetsregulering

Utvalget anser at de hensynene som er nevnt nedenfor er de viktigste ved en regulering av CSP-virksomhet.

For det første å s *tyrke tilliten* til og den generelle aksept av den nye teknologien (jf direktivets fortale punkt 4). Gjennom å etablere ordninger for sertifisering eller gi sin godkjennelse til aktørene i markedet kan myndighetene skape en tillit til CSP-virksomhet generelt og til de enkelte virksomhetene spesielt.

For det andre vil klare regler og et godt regulert marked *skape forutberegnelighet* for bruk av digitale signaturer, spesielt for når disse kan brukes. Et hovedpunkt fra utredningen "Digitale signaturer gir tillit til elektronisk kommunikasjon" var at det måtte skapes et regulatorisk regime hvor man viste i hvilke sammenhenger en digital signatur kunne benyttes og hvilke krav som måtte oppfylles for å bruke en.

I regi av Justisdepartementet, Nærings- og handelsdepartementet og Arbeids- og administrasjonsdepartementet pågår det et arbeid for å kartlegge lover, forskrifter og

instrukser som hindrer eller ikke ligger til rette for elektronisk kommunikasjon. Kartleggingsprosjektet skal finne, analysere og foreslå fjernet ubegrunnet hindringer i regelverket, samt tilpasse regelverket slik at en i størst mulig grad likestiller papirbasert og elektronisk kommunikasjon. Prosjektet tar sikte på å avlevere rapport med analyser og forslag til regulering medio april i år.

For det tredje å *beskytte forbrukerinteresser*. I et marked styrt av noen få sterke aktører kan fort forbrukerne bli den svake parten og trenge spesiell beskyttelse.

For det fjerde å *ivareta personvernhensyn*. Personvernet kan både svekkes og styrkes ved bruk av digitale signaturer. Det er viktig at bruken av digitale signaturer skjer på en måte som opprettholder personvernet. Dette er også eksplisitt nevnt i direktivet, jf artikkel 8.

For det femte å *regulere konkurransen i markedet.* Noen store aktører kan lett dominere markedet slik at mindre aktører ikke får tilgang. For å skape likeverdige forhold for alle bør myndighetene overvåke og regulere konkurransen i markedet.

5.2. Mulige oppgaver og roller for myndighetene

I Riisnæs' notat viser han til følgende potensielle roller for det offentlige:

- *Operatør* - For å skape tillit i markedet, eller operere som en rot-CSP, kan det hende at det offentlige vil operere sin egen CSP-virksomhet.
- *Regulatør* - Dette er en naturlig rolle som det offentlige må ha for å kunne ivareta ulike hensyn og skape forutberegnelighet i markedet.
- *Kontrollør* - Det offentlige kan kontrollere at de CSP-virksomhetene som driver, driver i henhold til krav i nasjonalt regelverk og direktivet.
- *Koordinator* - Det offentlige kan være en koordinator mellom de ulike aktørene i markedet og også være en koordinator mellom brukere og leverandører.
- *Finansieringskilde* - Det offentlige kan finansiere utvikling av ny teknologi og ordninger for å fremme teknologien i markedet
- *Bruker* - Det offentlige vil være en stor bruker av de tjenestene CSPene tilbyr, og derigjennom kunne påvirke utformingen av de tjenestene som tilbys.

Fra denne framstillingen ser man at myndighetenes interesse ikke bare er på den regelgivende siden. Det offentlige er en potensiell storbruker av tjenestene CSPer tilbyr, og kan også være en konkurrent. I denne rapporten fokuseres det på myndighetenes mulige oppgave som regulatør og kontrollør.

5.3. Kriterier for regulering

Utvalget har lagt til grunn, for de valgene som er gjort senere i rapporten, at

reguleringen av området skal følge de prinsipper og strategier som er utformet i St. meld 41 (1998-99) "Om elektronisk handel og forretningsdrift": Markedsdrevet utvikling, teknologinøytral regulering, og at all regulering skal skje i åpenhet og i dialog med berørte parter.

Det skal være et kriterium for valg av tilsynsordning at den fremmer økt bruk av digitale signaturer, og som ledd i dette fjerne usikkerhet og fremme forutsigbarhet.

For øvrig må kravene i direktivet overholdes, og ordninger som etableres skal være så enkle og lite kostnadsdrivende som mulig, jf programmet "Et enklere Norge".

Enhver ordning som etableres for å regulere markedet, eller for å skape tillit, bør i utgangspunktet være selvfinansiert. Det vil si at brukerne og leverandørene av tjenestene må bære kostnadene for tilsyn og andre tillitsskapende ordninger. Opprettelsen av en tilsynsordning og en eventuell sertifiseringsordning skal ikke koste skattebetalerne noe, eventuelt bortsett fra i en overgangsperiode for å hjelpe utviklingen i gang.

5.4. Kontroll- , sertifiserings- og tilsynsformer for CSP-virksomhet

I utgangspunktet kan det for det offentlige tenkes mange måter å føre tilsyn med CSP-virksomheter på. *Forhåndsgodkjenning* av CSPer er imidlertid ikke lovlig i henhold til direktivet.

Tilsyn gjennom a *kkreditert sertifisering* anses ikke som en aktuell kontroll- eller tilsynsform da det ikke innebærer myndighetsutøvelse. Det kan imidlertid være et viktig supplement til den kontrollen som myndigheten selv utfører, se nedenfor.

Meldeplikt for virksomheter som starter CSP-virksomhet kan gi myndigheten en oversikt over aktørene og markedet som grunnlag for å vurdere om det er nødvendig med øvrige tiltak. Vi viser til at det også i andre lands lover/lovutkast på området inngår meldeplikt, se kapittel 3.6.

Etterfølgende kontroll/tilsyn kan utføres av et myndighetsorgan, men mer nærliggende er å la de virksomhetene som sertifiserer CSPer foreta kontroller av virksomhetene og sende kopier av resultatene til et myndighetsorgan.

5.4.1. Akkreditering og sertifisering

Den norske akkrediteringsordningen ble opprettet på bakgrunn av St. prp 106 (1989-90) ved kgl res 7. juni 1991 med senere tilføyelse i kgl res 7. oktober 1993. Akkrediteringsorganet i Norge heter Norsk Akkreditering. Norsk Akkreditering har nasjonalt ansvar for å akkreditere blant annet sertifiseringsorgan, inspeksjonsorgan, tekniske kontrollorgan og attestasjonsorgan linkinthoveddel005P487_7679328>. Nærmere beskrivelse av gjeldende ordninger for akkreditering og sertifisering i Norge er gitt i vedlegg 2.

Rapport av 30.11.98 linkinthoveddel005P490_7724529> foreslår at det opprettes en frivillig ordning som tilbyr TTPer å operere i henhold til en "autorisasjonsordning" (tiltak 4). Videre foreslås det at det skal være et offentlig eller privat organ som skal ha ansvar for oppfølging og kontroll av de TTPer som er gitt autorisasjon.

Eksisterende statlige autorisasjons- eller godkjenningsordninger kan ha som formål å tildele visse rettigheter til dem som er godkjent, mens de ikke-godkjente er utelukket som legale aktører på markedet, og en slik forskjellsbehandling er jo utelukket i dette tilfellet (på grunn av direktivets diskrimineringsforbud). Det kan derfor være uheldig å bruke uttrykket *autorisasjonsordning* når ordningen er tenkt å være frivillig.

Et annet formål med slike ordninger kan være å etablere et kvalitetsskille mellom de "autoriserte" og de "uautoriserte", men der de sistnevnte for så vidt også opptrer legalt. Et

slikt skille vil være forenlig med direktivets artikkel 3:2, der det snakkes om "frivillige "akkrediteringsordninger med henblik på at højne niveauet for ydelse". Formålet med etableringen av en ordning vil være å skape større tillit til de aktørene i markedet som lar seg sertifisere.

Det sentrale spørsmålet er vel om det i Norge vil være formålstjenlig (i forhold til politiske målsetninger om utstrakt bruk av digitale signaturer) å ha en *frivillig sertifiseringsordning* (vi foretrekker dette uttrykket). Vil potensielle brukere av sertifiseringstjenester være usikre på forskjellen mellom sertifiserte og ikke-sertifiserte tjenesteleverandører, med generell lav tillit som konsekvens? Eller vil de tvert i mot oppfatte eksistensen av et sertifisert A-lag som en trygghet, primært bruke sertifiserte tjenestetilbydere og dermed tvinge andre aktører inn i en sertifiseringsprosess?

Behovet for tillit gjennom frivillig sertifisering må vurderes ut fra hvem som er aktuelle brukere, hvem som er aktuelle tilbydere og hvilken tillit aktuelle tilbydere har i markedet i dag med hensyn til andre tjenester. De tilbyderne vi kjenner til (jf kap 4.5) er sertifisert/godkjent i henhold til en del krav allerede, f.eks. Datatilsynets krav til datasentraler, ISO9000-sertifisering, krav fra VISA (for SET-tilbydere) og sikkerhets-/beredskapskrav. De holder løpende rede på, gjennom opinionsundersøkelser og brukerundersøkelser, hvilken image de har i befolkningen generelt og hvordan de oppfattes av eksisterende kunder. Her ligger det et empirisk materiale som tilbyderne av sertifikattjenester er de nærmeste til å tolke. Det må derfor være sentralt hva tilbyderne mener når det gjelder frivillig sertifisering som tiltak for å øke tillit i markedet.

Under gjennomgangen med dagens CSP-leverandører, var det ingen som sa at de ville sertifisere seg hvis det kom et tilbud om dette. Enkelte hadde flere former for sertifisering og mente at dette var nok. I tillegg mente de at deres "navn" og generelle rykte var det som skapte mest tillit, ikke et stempel på et papir. Dagens aktører er store og kjente og har dermed et mindre behov for sertifisering for å skaffe seg tillit i markedet.

I tiden fremover vil det bli laget komplette standarder for sertifisering av CSP virksomhet. Interessen og etterspørselen i markedet vil avgjøre om det anses som hensiktsmessig for CSPene å sertifisere sin virksomhet.

5.4.2. Sertifiseringsordninger som kan benyttes av CSPer

Nærings- og handelsdepartementet (NHD) har gitt Justervesenet ved Norsk Akkreditering i oppdrag å opprette en ordning for sertifisering av informasjonssikkerhet i organisasjoner. Sertifiseringen skal bygge på den britiske standard BS 7799, og sertifiseringsorganene skal akkrediteres etter samme modell som de som sertifiserer kvalitetsstyring etter ISO 9000.

NHD har ønsket at sertifiseringsordningen skal være brukerstyrt og har derfor nedsatt en styringskomité med medlemmer fra etablerte sertifiseringsorganer og offentlig og privat virksomhet.

Dessuten etableres det for tiden en ordning for sertifisering av IT-sikkerheten til produkter og systemer. I Norge er det Forsvarets Overkommando/ sikkerhetsstaben (FO/s) som utøvende myndighet for denne ordningen som forventes å bli operativ i løpet av høsten 2000. Det er altså FO/s som utsteder sertifikater til de produkter som har vært gjenstand for evaluering av

et evalueringsorgan. Evalueringsorgan blir akkreditert av Norsk Akkreditering som teknisk laboratorium etter EN 45001. Disse to ordningene utfyller hverandre.

For mer informasjon om eksisterende ordninger for sertifisering av informasjonssikkerhet i Norge se vedlegg 2.

5.4.3. Registrerings- og meldeordning for dem som står under tilsyn - virksomheter som utsteder kvalifiserte sertifikater

Vi har sett på en del registreringsordninger som har vært utredet i Norge de senere årene linkinthoveddel005P516_8209430>.

I utredningen av stiftelsesregistreringer (NOU 1998:7) ble det argumentert sterkt for at en *frivillig* registreringsordning ikke er bra nok. Det vil da oppstå hull i opplysningene, noe som svekker registerets funksjon som kilde til opplysning.

Vi har derfor som en grunnleggende forutsetning for våre forslag at et tilsyn krever en registrerings-/meldeplikt for tilbydere av kvalifiserte sertifikater

Et register der alle markedsaktører er registrert vil tjene publisitetshensyn, notoritetshensyn og kontrollhensyn. Publisitet betyr at forbrukeren kan få opplysninger om de næringsdrivende innenfor bransjen, både med henblikk på å velge blant disse og med henblikk på å vurdere bruken av en av dem. Notoritet innebærer at de registrerte opplysningene er riktige (vitterlige) opplysninger, noe som er til fordel både for de næringsdrivende selv og for aktuelle forbrukere/kunder. Kontrollhensyn, herunder statistikkføring, offentlig moral, skattlegging og oversikt over reguleringsbehovet, vil i første omgang primært tjene myndighetsinteresser, men vil på sikt kunne medvirke til en seriøsitet som vedkommende bransje er interessert i.

Hensyn til *legitimasjon* og *firmabeskyttelse* vil være dekket av Foretaksregisteret.

Gjennomgangen av registreringsordningene er en påminnelse om at følgende faktorer bør vurderes ved en registreringsordning for CSPer:

- Er antall opplysninger stort nok til å rettferdiggjøre ordningen? Hvis antall aktører er lite og/eller det meste av informasjonen er tilgjengelige i andre registre, vil dette kunne svekke betydningen av et særskilt register.
- Forholdet til Enhetsregisteret/Foretaksregisteret må vurderes. Skal registeret være et tilknyttet register, eller skal det skje regelmessige overføringer av opplysninger fra foretaksregisteret til CSP-registeret?
- Hvilken av CSPens roller er det registreringen skal knyttes til?
- Skille mellom nymeldinger/nyregistrering og endringsmeldinger/ajourføring. Skal registreringsmyndigheten med jevne mellomrom sende ut kopi av opplysningene som er registrert, med krav om at endringer skal påføres?
- Bestemmelsene om registreringsordningen: Lov, forskrift, annet?
- Ansvarlig myndighet for registeret. Blir registeret et eget forvaltningsorgan?
- Utlevering av opplysninger fra registeret
- Sletting av opplysninger. Tilbakekall av registrering. Registrering av sanksjoner.
- Finansiering. Gebyrer.

Som basis for sine vurderinger av alternative modeller (kapittel 6) har utvalget lagt til grunn at ordningen må være *obligatorisk* og at registreringen bør skje sentralt i *ett register.*

Ordningen bør begrenses til registrering av opplysninger som *ikke er registrert annet sted*. Eventuelt slik at de aktuelle opplysninger som myndighetene allrede har innhentet i andre sammenhenger overføres til registeret og oppdateres regelmessig, jf Oppgaveregisteret.

Registreringsplikten knyttes til den virksomheten som *utsteder kvalifiserte sertifikater.* Den som er ansvarlig for registeret må sikre at opplysningene er *riktige*, *komplette* og *oppdaterte.*

Tilsynsmyndigheten bør være ansvarlig for registeret. Registeret må være *åpent* for å fylle sine funksjoner, dvs at opplysningene kan gis ut til tredjemann

Registeret skal være et register over *nåværende godkjente CSPer*.

Virksomheten må *sende inn opplysningene noen dager før planlagt oppstart* av tjenesten, slik at man rekker å legge inn opplysningene i registeret.

En nærmere utdyping og begrunnelse for registreringsordningen er gitt i kapittel 7, der også lovhjemmel og forholdet til andre oppgaver for tilsynsmyndigheten er beskrevet.

5.4.4. Frivillig registreringsordning

En *frivillig* registreringsordning for virksomheter som tilbyr *ikke-kvalifisertesertifikater* kan tenkes i tillegg til en obligatorisk registreringsordning for tilbydere av kvalifiserte sertifikater. En slik frivillig ordning vil kunne registrere hvilke sertifikatpolicyer den enkelte virksomhet har, og samsvarsvurderinger som er gjort i forhold til disse. Dette vil være til hjelp for å orientere seg i markedet, sette i gang tjenester for vurdering av sikkerhetsnivå for de ulike typer sertifikater, vurdering av nødvendig sikkerhetsnivå for ulike typer transaksjoner mv. Hvem som skal forestå slike rådgivingstjenester er ikke vurdert.

Denne ordningen må holdes klart atskilt fra en obligatorisk registreringsordning for kvalifiserte sertifikater. Det kan være naturlig å opprette et slikt register i forbindelse med en eventuell frivillig godkjenningsordning, se kapittel 6.6 og 7.2.3.

5.4.5. Tilsynsbegrepet

Tilsynsbegrepet kan brukes på forskjellige måter. I heftet Samordning av myndighetenes tilsyn (AD, mars 1994) defineres det slik: *Tilsyn er myndighetenes utadrettede aktivitet for å påse at lover og forskrifter etterleves.*

En annen definisjon linkinthoveddel005P554_8723831> er: *"... å verifisere om en adressat for rettigheter og plikter overholder disse, og eventuelt sette inn korrigerende tiltak."*

Ordet brukes både om aktiviteten tilsyn og om institusjonen som utfører aktiviteten. Vi bruker ordet i begge betydninger i foreliggende rapport.

Tilsyn kan oppfattes som et svakere tiltak enn kontroll linkinthoveddel005P559_8761832>. Eller en kan se det som en mer teknisk aktivitet som et tilsynsorgan kan bruke i en generelt sett bredere tilsynsaktivitet.

En tilsynsmyndighet kan ha mange oppgaver som ikke hører under tilsynsaktiviteten, men som en har funnet hensiktsmessig å legge dit. Dette kan være forskriftsarbeid, godkjennings- og konsesjonsbehandling, faglig utrednings- og rådgivningsarbeid på politikkområdet med mer linkinthoveddel005P562_8807933>.

De konkrete tilsynsaktivitetene vil bære preg av hva som anses som hensiktsmessige virkemidler innenfor det aktuelle lovområdet. Eckhoff linkinthoveddel005P565_8826034>skiller mellom fysiske, normative, økonomiske og pedagogiske virkemidler.

Et utviklingstrekk de senere år er at en forsøker å *samordne de statlige tilsynsfunksjonene* overfor næringslivet, særlig i forhold til stedlig tilsyn. Dette er begrunnet ikke bare i effektivisering på myndighetssiden, men også i reduserte kostnader og økt konkurransekraft. Tendensen kan imidlertid se ut til å være at det opprettes *nye tilsyn på nye områder.*

I Norge har man hatt en utvikling i retning av *internkontroll* linkinthoveddel005P570_8882835> . Den tradisjonelle tilsynsmetodikken der tilsynet stiller krav og så undersøker om kravene etterleves, er erstattet av selvdeklarering og dokumentasjon fra virksomhetens side om at kravene er oppfylt . Dette passer godt overens med EUs kvalitetstenkning og krav f eks til produktkontroll, jf *"ny metode",* kapittel 3.5.

5.5. Sektorvis eller felles tilsynsmyndighet

Et viktig spørsmål er om det bør være sektorvise tilsynsmyndigheter, som f.eks. Kredittilsynet for finanssektoren, eller om det skal være et felles tilsynsorgan.

For CSPer som opererer innen en sektor, og allerede er underlagt en sektorvis tilsynsmyndighet, vil det være naturlig at denne tilsynsmyndigheten også førte tilsyn med CSP-virksomheten. For CSPer som ikke er underlagt tilsyn av en sektorvis tilsynsmyndighet vil det måtte etableres en ny tilsynsmyndighet.

Da flere av dagens aktører ikke er underlagt tilsyn på grunn av sin virksomhet, kun generelt tilsyn som omfatter alle virksomheter i Norge (Arbeidstilsynet, etc) må det tilføres ressurser hos en eksisterende tilsynsmyndighet eller opprettes et eget organ for å ta seg av tilsynet for disse virksomhetene.

Kompetansemessig er det mer fornuftig å samle kompetansen hos en tilsynsmyndighet, gitt at det er sparsomt med den nødvendige kompetansen i Norge.

Økonomisk er det mer fordelaktig å ha en tilsynsmyndighet enn flere myndigheter.

Hvis flere tilsynsmyndigheter skal regulere det samme området kan det utvikles ulik praksis mellom tilsynsmyndigheten. Dermed oppstår det et samordningsbehov.

Det er økonomisk og kompetansemessig fornuftig å bruke tilsynsmyndigheter som allerede arbeider med beslektede områder til også å kontrollere CSP-virksomhet. Dette gjelder uansett om det er en sektorvis tilsynsmyndighet eller en generell tilsynsmyndighet.

5.6. Finansiering av kontroll og tilsyn med CSP-virksomheter

I tråd med hva som er anført i Statskonsultrapport 1997:11 om tilsyn i transportsektoren vil vi anføre at det fra et samfunnsøkonomisk synspunkt vil det generelt være mest kostnadseffektivt å finansiere tilsynsvirksomhet gjennom generelle skatter. Dette har imidlertid også en fordelingspolitisk side, og ut fra dette kan man si at den som generer behov for tilsyn også bør bære kostnadene. Det er derfor ikke uvanlig at det tas inn tilsynsavgifter eller gebyrer for helt eller delvis å dekke kostnadene.

Store tilsynsenheter som Kredittilsynet, Oljedirektoratet, Statens forurensningstilsyn er alle bevilgningsfinansiert. Deres inntekter tilfaller statskassen og påvirker inntektskravet som stilles. Post- og teletilsynet er selvfinansiert ved at aktørene betaler gebyr til dekning av tilsynets kostnader. Konkurransetilsynet og Datatilsynet finansieres på vanlig måte over statsbudsjettet. Vi ser i utgangspunktet ingen grunn til at disse organene skal ha en annen finansiering for de oppgavene som gjelder CSP enn det de har for øvrig.

Ved den konkrete utformingen av finansieringsordningen, herunder nivået på gebyrer og lignende, må en påse at eventuelle gebyrer ikke er så lave at de administrative kostnadene ved å inndrive dem andelsmessig blir for høye. Samtidig må de ikke gebyrene være så høye at de avskrekker noen aktører fra å registrere seg.

Ved fastsetting av en finansieringsordning for tilsyn med CSPer må en imidlertid også se hen til de politiske målene på feltet. I og med at det er en politisk målsetting å fremme sikker elektronisk kommunikasjon, kan det være at den tilsynsfinansieringen som man kanskje ellers ville ha valgt, i en overgangsfase bør vike. Vi viser til de markedsmessige betraktningene i kapittel 7.1.

5.6.1. Kostnader for CSPer

I tillegg til kostnader for myndighetene vil det komme kostander for CSPene i forbindelse med eventuelle sertifiseringer og revisjoner som blir pålagt av det offentlige. Kostnader i denne forbindelse bør ikke være vesentlig høyere for norske CSPer enn for utenlandske CSPer. Dette kan tilsi at kostnadene ved tilsyn i Norge bør harmoniseres med kostnadene for tilsyn i andre europeiske land.

5.7. Aktuelle tilsynsorgan

5.7.1. Konkurransetilsynet

Konkurransetilsynet skal fremme effektiv konkurranse i næringslivet og påse at ulovlig samarbeid og ulovlige reguleringer ikke forekommer. Den praktiske gjennomføringen skjer med utgangspunkt i konkurranseloven, pristiltaksloven, kredittkjøpsloven og markedsføringsloven. Konkurransetilsynet skal også bistå EFTAs overvåkingsorgan og Europakommisjonen, blant annet ved håndheving av EØS-avtalens konkurranseregler og ved å medvirke i arbeidet for effektiv konkurranse innen EØS-området.

Ut fra dette synes det åpenbart at tilsyn i Norge i forhold til direktivets bestemmelser om fri konkurranse per i dag ligger til Konkurransetilsynet. Andre løsninger vil innebære en innsnevring av Konkurransetilsynets virkeområde (gjennom lovendring) og til fare for

gråsoner og dobbeltarbeid i forhold til et eventuelt annet organ, enten dette er statlig eller ikke.

5.7.2. Post- og teletilsynet

Post- og teletilsynet (tidligere Statens teleforvaltning, utvidet med posttilsyn i 1997) skal føre tilsyn med post- og telesektoren i Norge i henhold til postloven og teleloven. Dette innebærer blant annet at tilsynet ska bidra til å nå de overordnede mål om tilbud over hele landet av grunnleggende post- og teletjenester til høy kvalitet og lavest mulig pris.

Ansvarsområdet til Post- og teletilsynet blir stadig utvidet. I dag er virksomheten i hovedsak konsentrert om disse oppgavene:

- føre kontroll med at lover, forskrifter og konsesjonsvilkår blir etterlevde
- ha tilsyn med aktørene på post- og teleområdet
- føre register over aktørene på post- og teleområdet
- utarbeide forskrifter
- forvalte autorisasjonsordninger
- ha ansvaret for typegodkjenning
- gjennomføre markedskontroll av teleutstyr
- ha ansvaret for telestandardisering
- ha ansvaret for radiofrekvensforvaltning
- ha ansvaret for nummerforvaltning
- ta del i internasjonalt arbeid
- drive rådgiving overfor Samferdselsdepartementet

CSP-tjenester faller ikke inn under begrepet "grunnleggende teletjenester", jf telelovens formål om å fremme behovstilpassede teletjenester og forbrukerinteresser (§ 1-3 f og g). Det er imidlertid på det rene at CSP-tjenester forutsetter godt fungerende grunnleggende teletjenester, og at CSP-tjenester på sikt kan bli oppfattet som grunnleggende infrastruktur. Det er dessuten klart at data- og teleteknologien konvergerer til en felles informasjons- og kommunikasjonsteknologi, og at det kan være vanskelig og uhensiktsmessig å prøve å skille mellom data-/informasjonsteknologi og teleteknologi.

5.7.3. Datatilsynet

Datatilsynets oppgaver i dag er:

- Behandle og avgjøre søknader om konsesjon for personregistre og for annen bruk av personopplysninger i visse typer virksomheter.
- Kontrollere at lover og regler som gjelder for personregistre og bruk av personopplysninger blir fulgt.
- Informere om personvern og de reglene som gjelder for personregistre.

EUs direktiv om beskyttelse av personopplysninger (personverndirektivet) ble vedtatt i 1995. Som følge av dette ble det fremmet et forslag til ny personopplysningslov 25. juni 1999.

I henhold til ny lov (§ 42) skal Datatilsynet:

- Føre systematisk og offentlig fortegnelse over innmeldte behandlinger av personopplysninger og gitte konsesjoner
- Behandle søknader og motta meldinger, og vurdere pålegg

- Kontrollere at lover og regler blir fulgt
- Holde seg orientert om utviklingen nasjonalt og internasjonalt med hensyn til behandlingen av personopplysninger
- Identifisere farer for personvernet, og gi råd om hvordan de kan unngås eller begrenses
- Gi råd og veiledning, i forbindelse med utarbeidelse av bransjevise atferdsnormer
- Gi uttalelser
- Avgi årsmelding

Det har vært en utvikling i retning av at *konsesjonsplikten reduseres* og erstattes av *meldeplikt*.

Datatilsynets oppgaver innebærer at det må føres tilsyn med den behandlingen av personopplysninger som skjer hos CSPene og registreringsenhetene.

5.7.4. Kredittilsynet

Kredittilsynet ble opprettet 24. mars 1986 ved en sammenslutning av Bankinspeksjonen, Forsikringsrådet og Meglerkontrollen. Etaten fører tilsyn med alle aktører i finansmarkedet, herunder blant annet bankene, finansieringsselskap, aksjefond, inkassovirksomhet, regnskaps- og revisjonsvesenet, Verdipapirsentralen, livs- og skadeforsikringsselskap, private og kommunale pensjonsordninger mv.

Hovedoppgavene er:

- Tilsyn og kontroll med institusjonene og dere virksomhet
- Overvåking av bransjer, markeder og makroøkonomiske forhold
- Forvaltning av regelverk
- Aktiv faglig rådgivning for overordnet myndighet, tilsynsenhetene og allmennheten

Kredittilsynet ser til at institusjonene fungerer på en betryggende måte. Vurdering av soliditet står sentralt.

5.7.5. Vurdering av tilsynsorganenes egnethet som CSP-tilsyn

Av ovennevnte tilsyn mener utvalget at Post- og teletilsynet er best egnet som CSP-tilsyn. Det er særlig lagt vekt på hva som er hovedformålet med det enkelte tilsynsorganet, og at både Sverige og Danmark har valgt sine Post- og teletilsyn som tilsynsorgan. Vi viser til kapittel 7.3, der det er gitt en sammenliknende vurdering av de aktuelle tilsynsorganene.

Fotnoter

28 Akkreditering er en offisiell anerkjennelse av at *en organisasjon* arbeider i henhold til et dokumentert kvalitetssystem og har demonstrert kompetanse til å utføre nærmere beskrevne oppgaver. Sertifisering er en bekreftelse fra en uavhengig part om at *et produkteller entjeneste* tilfredsstiller kravene i et kravdokument.

29 Digitale signaturer gir tillit til elektronisk kommunikasjon: Forslag til tiltak for aksept og utbredelse, RITS

30 Registrering av oppsøkjande salsverksemd utanom fast utsalsstad (Ot prp nr 61 1998-99), registreringsordninga for videogram og ansvarlig distributør (Ot prp nr 78 1996-97), ordningen med registrering av stiftelser (NOU 1998:7), register over revisorer og revisjonsselskaper (Ot prp nr 75 1997-98), samt registreringsordning for tilbydere av overføringskapasitet og offentlig telefontjeneste (Ot prp 31 1997-98).

31 Hans Petter Graver, Materiell forvaltningsrett, 1996

32 St meld nr 23 (1992-93) Om forholdet mellom staten og kommunane

33 Internt notat Statskonsult, november 1996

34 Statens styringsmuligheter - særlig i ressurs- og miljøspørsmål, 1983

35 Internkontrollforskriften for helse, miljø og sikkerhet gir bestemmelser om at den som er ansvarlig for en virksomhet plikter å sørge for at gjeldende krav fastsatt i lov følges opp.

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

6 Mulige modeller for regulering av CSP-virksomhet

Her vil vi kort beskrive noen mulige modeller for regulering av CSPer. Modellene vil fokusere på tilsyn av CSPer, men også frivillige ordninger for ulike former for sertifisering og revisjon vil bli tatt med. Det er viktig å legge merke til at det er et samspill mellom graden av tilsyn og graden av frivillig sertifisering/revisjon. Jo større grad av frivillig sertifisering og revisjon desto mindre behov for sterkt grad av offentlig tilsyn. Myndighetenes rettslige kompetanse til å utføre kontroll er den samme for alle modellene.

De aktørene som omtales i modellene er: CSPene, tilsynsmyndighet, sertifiseringsorgan, akkrediteringsorgan, privat virksomhet som reviderer CSPene i henhold til sertifikatpolicy og sertifikatutstedelsespraksis (CSP-revisjons firma)

Figur 3 viser en oversikt over forholdene mellom disse enhetene.

Figur 3 - Oversikt over de offentlige og private aktørene som kan delta i en tilsynsordning for CSPer

6.1. Graden av tilsyn

Modellene senere i kapitlet vil vise mulige måter å gjennomføre tilsyn på. Hvor omfattende tilsynet skal være er ikke spesifisert. Omfanget av tilsyn er ikke direkte avhengig av modellen som velges, men modeller basert på gjennomgang av IT-revisor eller sertifiseringsorgan kan medføre et mer omfattende tilsyn en kontroll utført av et tilsynsorgan.

Den minste former for tilsyn en kan tenke seg for å tilfredsstille direktivet er et tilsynsorgan som registrerer CSPene, sjekker den finansielle soliditeten til CSPene, påser at kravene til personvern blir ivaretatt og at CSPen leverer en egenerklæring om at den oppfyller kravene for å utstede kvalifiserte sertifikater (kravene som er spesifisert i anneksene til direktivet).

Den andre ytterligheten er et tilsyn som krever en total årlig gjennomgang av CSPen av et IT-revisjonsfirma eller et sertifiseringsorgan uten å ta hensyn til frivillige sertifiseringer som CSPen har gjennomført.

En mellomvariant er at man krever jevnlige gjennomganger av CSPen av et IT-revisjonsfirma, men at kravene ikke er så strenge og at man alternativt kan benytte frivillige godkjenningsordninger eller sertifiseringsordninger. Her kan frivillige ordninger erstatte behovet for tilsyn.

6.2. Kontrollmodellen

6.2.1. Kort beskrivelse av modellen

Tilsynsmyndigheten er en eksisterende offentlig virksomhet, f.eks. Post- og teletilsynet (PT). CSPer som skal utstede kvalifiserte sertifikater i Norge må melde virksomheten inn til tilsynsmyndigheten. Hva som skal rapporteres inn er besluttet i en egen lov/forskrift, eller bestemt av tilsynsmyndigheten. Virksomheten blir registrert i et eget register med oversikt over CSPer.

CSPer som skal utstede kvalifiserte sertifikater skal jevnlig rapportere til tilsynsmyndigheten hvilken sertifikatpolicy de følger, og hvordan deres sertifikatutstedelsespraksis er. Kravene til sertifikatpolicy og sertifikatutstedelsespraksis er gitt av myndighetene. Dette er en form for selvdeklarering.

Tilsynsmyndighetene kan kontrollere hvis de mener det er nødvendig, eller etter "krav" fra brukere eller andre aktører. Tilsynsmyndigheten utfører kontrollen selv.

En variant av denne modellen er at tilsynsmyndigheten er et privat firma som har fått delegert myndighet til å gjennomføre tilsyn.

6.2.2. Liknende eksisterende modeller

Dette er den tradisjonelle formen for tilsyn, hvor tilsynsmyndighetene bygger opp kompetanse på tilsynsområdet for selv å drive tilsyn. Denne formen for tilsyn utelukker ikke at tilsynsmyndighetene av og til benytter privat ekspertise i forbindelse med enkelte kontroller.

Datatilsynet, Post- og teletilsynet, Arbeidstilsynet er noen av tilsynsmyndighetene som baserer sin virksomhet på denne modellen.

Kontrollmodellen likner modellen som vanligvis brukes for CE-merking og for tekniske kontrollorganer under andre EØS nye-metode direktiver.

6.2.3. Fordeler og ulemper med modellen

Tilsynsmyndighetene må bygge opp kompetanse, blant annet på IT-revisjon og IT-sikkerhet, hvis den skal gjennomføre kontroller. Så lenge alt går bra er det en rimelig ordning som baserer seg på at tilsynsmyndigheten stoler på de opplysningene CSPene gir om sertifikatpolicy og praksis.

Dette er også en modell som kan skape tillit i markedet hvis tilsynsmyndigheten får tilført den nødvendige kompetanse.

Modellen er avhengig av at CSPene gjennomfører nødvendig egenkontroll og at meldingene som sendes tilsynsmyndighetene er i samsvar med den virkelige praksisen hos CSPene.

6.3. Revisjonsmodellen

6.3.1. Kort beskrivelse av modellen

Tilsynsmyndigheten er en eksisterende offentlig virksomhet, for eksempel PT. CSPer som skal utstede kvalifiserte sertifikater i Norge må melde denne virksomheten inn til tilsynsmyndigheten. Hva som skal rapporteres inn er besluttet i en egen lov/forskrift, eller bestemt av tilsynsmyndigheten. Virksomheten blir registrert i et eget register med oversikt over CSPer som tilbyr kvalifiserte sertifikater i henhold til direktivet.

CSPer som skal utstede kvalifiserte sertifikater skal jevnlig bli revidert av et CSP-revisjons firma. Det firmaet som CSPen velger til å utføre revisjonen skal aksepteres/godkjennes av tilsynsmyndigheten. Kravene som CSP-revisjonsfirmaet skal revidere etter er bestemt av tilsynsmyndigheten og/eller av andre myndighetsorganer.

Tilsynsmyndigheten baserer sine tiltak ovenfor en CSP i hovedsak på rapportene fra CSP-revisjonsfirmaene.

6.3.2. Liknende eksisterende modeller

Aksjeselskaper regnskapspliktige etter regnskapsloven, jf § 1-2 og skal ha revisor, jf revisorloven §1. Revisoren kan være en person eller et selskap, jf revisorloven §§ 3og 4. Revisor skal granske bedriftens årsoppgjør og regnskaper mv. Revisor skal videre påse at bedriftens ledelse har oppfylt sin plikt til å sørge for at regnskapet er i overensstemmelse med regelverket og god regnskapsskikk, blant annet av hensyn til den oppgave- og opplysningsplikt som følger av eller i medhold av lov. Revisor skal gis tilgang til de opplysninger og gis adgang til å foreta de undersøkelser han finner nødvendig, jf § 7. Når bedriftens årsoppgjør er avgitt skal revisor legge frem sin revisjonsberetning og i denne forbindelse gi uttalelse om årsoppgjøret er overensstemmelse med lov og god regnskapsskikk. Revisors merknader og påpekinger skal inntas i brev og nummereres fortløpende, jf § 8

Etter kredittilsynsloven § 3a plikter revisor å rapportere til Kredittilsynet ethvert forhold vedrørende virksomheten som kan innebære en overtredelse av bestemmelser som kan

medføre tilbakekall av institusjonens tillatelse til å drive virksomhet, eller forhold som kan medføre at regnskapene ikke godkjennes eller at det tas forbehold.

6.3.3. Fordeler og ulemper med modellen

Revisjonsselskap har allrede en etablert rolle og relasjon til bedriften, revisjonsselskapene, i hvert fall de store, vil være i stand til å revidere selskapets sertifikatpolicy og sertifikatutstedelsespraksis. Disse kan være basert på internasjonale standarder.

Revisjonsmodellen er kostnadskrevende for CSPene som må betale for en ekstra revisjon.

Tar ikke revisjonsselskapene hensyn til andre sertifiseringer og godkjenninger CSPen har, vil det medføre dobbeltarbeid og flere kostnader for CSPen.

Uten gode krav fra myndighetene på hva som skal revideres kan revisjonsselskapene revidere mer en det som er nødvendig.

Revisjon fra et anerkjent firma kan skape tillit i markedet.

6.4. Akkrediteringsmodellen

6.4.1. Kort beskrivelse av modellen

Tilsynsmyndigheten er en eksisterende offentlig virksomhet, f.eks. PT. CSPer som skal utstede kvalifiserte sertifikater i Norge må melde denne virksomheten inn til tilsynsmyndigheten. Hva som skal rapporteres inn er besluttet i en egen lov/forskrift eller bestemt av tilsynsmyndigheten. Virksomheten blir registrert i et eget register med oversikt over CSPer.

CSPer som skal utstede kvalifiserte sertifikater skal innen en gitt tidsfrist sertifiseres av et akkreditert sertifiseringsorgan. Kravene det sertifiseres etter er felles europeiske normer.

Tilsynsmyndigheten baserer sine tiltak ovenfor en CSP i hovedsak på rapportene fra sertifiseringsorganet. I tillegg blir CSPen sertifisert og kan bruke dette i sin markedsføring.

6.4.2. Liknende eksisterende modeller

Det finnes en liknende modell i Europa, inklusive Norge: Miljøstyring etter EMAS-forordningen linkinthoveddel006P756_11186936> Her *må* de såkalte miljøkontrollørene bli akkreditert, dette kreves i forordningen. Disse utfører en funksjon som kombinerer sertifisering og revisjon: De bekrefter at bedriften har et miljøstyringssystem som tilfredsstiller europeiske krav (liknende ISO 14 001-krav) og signerer (godkjenner) en bedrifts miljøredegjørelse.

6.4.3. Fordeler og ulemper med modellen

Modellen vil antakeligvis være i strid med direktivet, siden den innebærer en obligatorisk sertifisering av CSPen som en etterfølgende kontroll. (Man får egentlig kun en utsettelse på

noen måneder for å få en forhåndsgodkjenning). Kravene som CSPen blir sertifisert etter er felles europeiske normer og like fra land til land. Myndighetene i det enkelte land kan derimot ikke direkte influere på kravene noe som kan føre til at myndighetene ikke får dekket alle sine behov for kontroll/tilsyn via sertifiseringen.

Det er per i dag ikke felles europeiske normer for en fullstendig sertifisering av CSPer. Mangelen på normer på alle nivåer utelukker denne modellen. Det finnes eksisterende sertifiseringsordninger, som for eksempel BS 7799:1999, som kan dekke ***deler*** av kravene som stilles til en CSP.

6.5. Kombinasjonsmodellen

6.5.1. Kort beskrivelse av modellen

Tilsynsmyndigheten er en eksisterende offentlig virksomhet, f.eks. PT. CSPer som skal utstede kvalifiserte sertifikater i Norge må melde denne virksomheten inn til tilsynsmyndigheten. Hva som skal rapporteres inn er besluttet i en egen lov/forskrift eller bestemt av tilsynsmyndigheten. Virksomheten blir registrert i et eget register med oversikt over CSPer.

CSPer som skal utstede kvalifiserte sertifikater skal jevnlig bli revidert av et CSP-revisjons firma ***eller*** være sertifisert av et sertifiseringsorgan. Det firmaet som CSPen velger til å utføre revisjonen skal aksepteres/godkjennes av tilsynsmyndigheten ***eller*** må være et akkreditert sertifiseringsorgan.

Tilsynsmyndigheten baserer sine tiltak ovenfor en CSP på rapportene fra CSP-revisjons firmaene eller sertifiseringsorganene. Sertifiseringsordningen vil for de som ønsker det erstatte revisjon av et CSP-revisjonsfirma. Kravene til sertifisering kan være strengere enn kravene som stilles ved en revisjon. Denne modellen er omtrent en kombinasjon av revisjon- og akkrediteringsmodellen.

Kontrollen fra tilsynsmyndigheten baseres på et valgfritt sett av sertifikater og erklæringer fra sertifiseringsorganer og revisjonsfirmaer. Grunnen til at alle de private virksomhetene står oppført som obligatoriske, er at CSPen må velge en av dem. Det er ikke mulig å la være å benytte et revisjonsfirma eller et sertifiseringsorgan.

6.5.2. Liknende eksisterende modeller

Dette er en kombinasjon av revisjonsmodellen og akkrediteringsmodellen. Utredningsgruppen kjenner ikke til modeller i Norge hvor krav om revisjon kan erstattes med sertifisering. Vi vet derimot at arbeidet til revisjonfirmaene ofte blir mindre omfattende når de kan basere sin kontroll på allerede eksisterende sertifikater og godkjenninger.

6.5.3. Fordeler og ulemper med modellen

Denne modellen omfatter flere ulike kontrollmuligheter noe som kan virke forvirrende på markedet. En så fleksibel modell kan være dyr å opprette, administrere og drifte hvis

myndighetene må vedlikeholde og videreutvikle ulike sett med krav og kriterier som CSPene kan benytte.

Modellen er meget fleksibel siden CSPen kan velge mellom revisjon eller sertifisering. CSPen kan også velge å sertifisere deler av sin virksomhet og la revisjonsfirmaer gå igjennom de delene som ikke er sertifisert.

Myndighetene må ha en oversikt over hva de ulike sertifiseringene innebærer. De må også vurdere i hvor stor grad de stoler på de ulike sertifiseringene.

Den faglige kompetansen til tilsynet må også være god, siden de ulike sertifiserings- og godkjenningsordningene må vurderes.

6.6. Frivillig godkjenningsordning

6.6.1. Kort beskrivelse av modellen

Modellen baserer seg på et opplegg utviklet i England som et privat alternativ til evaluering og sertifisering gjennom det engelske akkrediteringssystemet. I England vil Department of trade and industry (DTI) opprette en ordning hvis ikke de private initierer en ordning delevis basert på selvregulering. Ordningen er privat, selvfinansiert og frivillig.

Ordningen forutsetter at det finnes IT-revisjonsfirmaer og sertifiseringsorganer i markedet som kan utstede sertifikater eller erklæringer om ulike forhold ved driften til CSPene. Ut i fra det sett med erklæringer og sertifikater som CSPene har, gir godkjenningsorganisasjonen en godkjenning på et gitt nivå.

Det må etableres en godkjenningsorganisasjon som skal utstede godkjenninger som kan brukes for å skape tillit i markedet. Godkjenningene baseres på sertifikater og erklæringer som CSPen allerede har innhentet. I England er godkjenningsorganisasjonen privat, mens i Tyskland er den lagt til Post og teletilsynet. Myndighet og mandat for en slik organisasjon vil variere alt ettersom det er et privat eller offentlig organ.

Er det et offentlig organ vil det være uklart hvordan man organisatorisk skal skille oppgavene til et godkjenningsorganisasjon fra oppgavene til en tilsynsmyndighet.

Godkjenningsorganisasjonen kan gi godkjenninger på ulike nivåer alt etter hvor mange sertifikater og erklæringer CSPen har skaffet seg. Håpet er at det kan etablere veiledninger eller profiler for ulike sikkerhet-/tillitsnivåer som markedet kan etterspørre. Kunden kan da forhåpentligvis slippe å evaluere CSPens tilbud selv.

Alle CSPer som utsteder kvalifiserte sertifikater må melde sin virksomhet inn til en tilsynsmyndighet. Myndigheten gjør ikke noen aktive kontroller før de får en klage eller en henvendelse om å gjøre noe mot en spesiell CSP.

I England er ordningen drevet fram og vil bli finansiert av markedet.

6.6.2. Liknende eksisterende modeller

Ordningen beskrevet ovenfor eksisterer i England og er kalt tScheme
linkinthoveddel006P813_14244337>.

6.6.3. Fordeler og ulemper med modellen

Det etableres en slags frivillig godkjenningsordning som kan skape tillit i markedet. Det er liten myndighetsregulering, myndighetene griper først inn i etterkant.

Tilsynsmyndighetens oppgaver blir små og kostnadene ved å etablere og drifte en tilsynsmyndighet blir relativt små.

Oppgavene og ansvaret til en godkjenningsorganisasjon er uklar. Forholdet mellom en godkjenningsorganisasjon og en tilsynsmyndighet er uklart. Markedets aksept av en slik godkjenning er ikke kjent.

Markedspotensialet for en slik ordning i Norge er meget begrenset. Skal godkjenningsmyndigheten foreta egne kontroller vil dette koste, og de må ha egne eksperter. Sett ut i fra antall aktører i Norge vil dette antakelig ikke være økonomisk lønnsomt.

Hvis godkjenningsorganisasjonen er et offentlig organ kan det oppstå uklarheter mellom rollen til tilsynsmyndigheten og rollen til godkjenningsorganisasjonen.

Denne modellen er den som gir myndighetene minst oversikt over markedet, og minst mulighet til å gripe inn i forkant. Myndighetene har heller ikke noen mulighet til selv å vurdere om en CSP oppfyller kravene til å utstede kvalifiserte sertifikater.

Skal myndighetene ha den teknologiske og juridiske kompetansen som er nødvendig for å vurderer driften til en CSP må det etableres en tilsynsmyndighet på linje med de øvrige alternativene. Kostnadene og bemanningen ville dermed være som de øvrige modellene.

6.7. Selvdeklarasjonsmodellen

6.7.1. Kort beskrivelse av modellen

Denne modellen bygger på at CSPene er avhengige av at markedet har tillit til sertifikatene, og at markedet derfor i stor grad vil regulere seg selv. Samtidig kan det av hensyn til tilliten til systemet i sin helhet være verdifullt med et tilsyn som kan gripe inn. Tilsynet bør være så markedsorientert som mulig, slik at man ikke legger unødvendige administrative byrder, og derved kostnader på CSPene.

Tilsynet er en eksisterende offentlig virksomhet, f.eks. PT. CSPer som skal utstede kvalifiserte sertifikater i Norge må melde denne virksomheten inn til tilsynsmyndigheten. Denne meldingen skal være en deklarasjon om at CSPen oppfyller kravene til kvalifisert sertifikat, herunder opplyse om hvilken sertifikatpolicy de følger og hvordan deres sertifikatutstedelsespraksis er. Tilsynet kan vise til hvilke policy og praksis som oppfyller kravene. Hva som skal rapporteres inn besluttes i forskrift av tilsynet. Virksomheten blir registrert i et eget register med oversikt over CSP-er.

Deklarasjonen sendes kun inn ved oppstart av virksomheten, og dersom det skjer endringer som gjør at de registrerte opplysningene ikke lenger er korrekte.

Tilsynsmyndighetene kan imidlertid kreve å få alle de opplysninger som de ønsker for å sikre at CSPer som tilbyr kvalifiserte sertifikater oppfyller kravene i loven. Slik kontroll kan skje dersom tilsynet mener det er nødvendig, eller etter "krav" fra brukere eller andre aktører.

6.7.2. Liknende eksisterende modeller

Sverige har valgt denne formen for tilsyn.

6.7.3. Fordeler og ulemper med modellen

Sammenlignet med revisjonsmodellen må CSPene i selvdeklarasjonsmodellen ikke sende inn årlige rapporter om foretatt IT-revisjon til tilsynet. I Sverige har man kommet frem til at revisjonsmodellen vil være et tungrodd og kostbart apparat. Man ønsker ikke en utvikling der CSPer, kun for å unngå et kostbart tilsyn, ikke kaller sine sertifikater for kvalifiserte selv om de oppfyller kravene.

Ved å velge selvdeklarasjonsmodellen vil det heller ikke være behov for å regulere hvem som kan være IT-revisor.

Til forskjell fra kontrollmodellen må CSPen ikke sende inn jevnlige rapporter til tilsynet.

Deklarasjonen som skal sendes tilsynet kan være relativt kort og bør blant annet inneholde garantier vedrørende personvern, økonomi og overholdelse av kravene i anneksene til direktivet. Se for øvrig kapittel 5.4.3 og 7.4 for innholdet i og omfanget av en registreringsordning. stilles krav om bundne midler avsatt for en evt styrt avvikling av selskapet.

Modellen krever en viss kompetanse innen IT-revisjon hos tilsynet, men tilsynsformen utelukker ikke at man innhenter privat ekspertise i forbindelse med enkelte kontroller.

Fotnoter

36 Enviromental Management and Audit System (EMAS). Denne forordningen er implementert i Forurensingsloven (lov 1981-03-13 6). EMAS er for tiden under revisjon (EMAS-2).

37 tScheme Securing Electronic Buisness Prospectus, ver. 2.0a, 6 December 1999

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

7 Utredningsgruppens anbefalinger

7.1. Vurdering av markedet

Dagens norske marked består av en håndfull CSPer. Det er lite trolig at antall CSPer på det norske markedet vil bli særlig større de nærmeste årene. Muligens vil kun et fåtall av disse tilby "kvalifiserte sertifikater" i nær framtid. Innen offentlig forvaltning kan det tenkes at enkelte forvaltningsorganer vil etablere eller videreføre sine egne CSP-ordninger. Eksempler på dette kan være Brønnøysundregisterets tiltenkte oppgaver i forhold til innlevering av næringsoppgaver til skatteetaten linkinthoveddel007P860_14723338>eller Rikstrygdeverkets prosjekt omkring elektronisk innrapportering.

Både aktørene i det norske markedet og utenlandske aktører og analytikere betegner markedet for PKI-tjenester som et gryende marked som ennå ikke har funnet sin endelige form. For sterk regulering vil kunne hemme utviklingen. Kundene er heller ikke fortrolige med de tjenestene som tilbys av CSPer og hvordan de kan nyttiggjøre seg en PKI i egen organisasjon.

Mange kunder vil trolig ikke ønske dyre sikkerhetstjenester, og CSPene må dermed tilby billigere løsninger for å få en tilstrekkelig kundemasse i en innledende fase. For høye priser på tjenester og produkter vil antakelig være et viktig hinder for å kunne få produktene ut i massemarkedet. Det kan tenkes at endel CSPer ikke vil tilby kvalifiserte sertifikater før markedet etterspør dette, på grunn av at de mener at produkter og tjenester med så høy sikkerhet vil være for dyre for markedet i en oppstartsfase.

En regulering av CSPer bør derfor ikke være med på å øke prisene i vesentlig grad på sluttproduktene og -tjenestene. På den annen side er det behov for ordninger som skaper tillit.

De fleste av de etablerte CSPene ønsker en felles tilsynsmyndighet for CSPer som skal utstede kvalifiserte sertifikater.

7.1.1. Vurdering av behov for sertifiseringsordninger

Det mangler foreløpig noen kriterier og standarder for å kunne etablere en full sertifiseringsordning i Norge. Sikkerhetsevalueringen av organisasjoner basert på BS 7799 vil imidlertid bli en standard, også i Norge, for sertifisering av informasjonssikkerhet i en organisasjon. Sertifisering etter BS 7799 tilbys per i dag i det norske markedet og sleve standarden vil foreligge i norsk versjon og oversettelse om kort tid linkinthoveddel007P872_14899439>. Denne sertifiserer imidlertid ikke hele den virksomhet en CSP driver, men utvalget mener at CSPer som skal tilby kvalifiserte sertifikater bør benytte denne standarden for å vurdere sikkerheten i egen organisasjon. Se også kapittel 7.2.4.

Det norske markedet anses dessuten i dag for lite for en akkreditert sertifiseringsordning for sertifisering av alle sider av CSPers virksomhet. Utvalget anbefaler at myndighetene ikke tar initiativ til etablering av en slik ordning nå, men anbefaler bruk av de ordningene for sertifisering av IT-sikkerhet som er etablert eller under etablering, se kapittel 5.4.2.

CSPer som ønsker en akkreditert sertifisering kan også foreta denne i utlandet. Baseres en kontrollordning på uttalelser fra akkrediterte sertifiseringsorgan, må norske myndigheter godta revisjonsrapporter utført av utenlandske selskap. Dette vil være en effekt av ordningen.

7.2. Forslag til regulering

7.2.1. Forslag til modell for tilsyn av CSPer

Ut i fra kunnskapene om at en omfattende tilsynsordning med sterk kontroll er dyrt, at markedet er i utvikling, at kundene er få og etterspør billige løsninger, anbefaler utvalget at myndighetene viser varsomhet vedrørende regulering av CSP-virksomhet. Utvalget konkluderer derfor med å velge selvdeklarasjonsmodellen. Se kapittel 6.7.

Denne modellen bygger på at CSPene er avhengige av at markedet har tillit til sertifikatene, og at markedet derfor i stor grad vil regulere seg selv. Samtidig kan det av hensyn til tilliten til systemet i sin helhet være verdifullt med et tilsyn som kan gripe inn. Tilsynet bør være så markedsorientert som mulig, slik at man ikke legger unødvendige administrative byrder, og derved kostnader på CSPene.

Det utpekes en offentlig tilsynsmyndighet som skal drive tilsyn med alle CSPer etablert i Norge som skal utstede kvalifiserte sertifikater. Tilsynsmyndigheten legges til Post- og teletilsynet, se kapittel 7.3. Tilsynsmyndighetene kan kreve å få alle de opplysninger som er nødvendig for å sikre at CSPer som tilbyr kvalifiserte sertifikater oppfyller kravene i loven. Slik kontroll kan skje dersom tilsynet mener det er nødvendig, eller etter "krav" fra brukere eller andre aktører.

7.2.2. Obligatorisk registreringsordning

Det etableres en registreringsordning for CSPer som tilbyr *kvalifiserte sertifikater*. CSPer som skal utstede kvalifiserte sertifikater i Norge må melde denne virksomheten inn til tilsynsmyndigheten. Denne meldingen skal være en deklarasjon om at CSPen oppfyller kravene til kvalifisert sertifikat, herunder opplyse om hvilken sertifikatpolicy de følger og hvordan deres sertifikatutstedelsespraksis er. Tilsynet kan vise til hvilke policy og praksis som oppfyller kravene. Dersom en tilbyder ønsker å anvende en annen policy/praksis som ikke er godkjent må tilsynet gjøre en realitetsvurdering av den. Denne realitetsvurderingen bør være tilgjengelig for tredjemann. Også policy som ikke er godkjent bør være tilgjengelig.

Virksomheten blir registrert i et eget register med oversikt over CSPer som utsteder kvalifiserte sertifikater.

Deklarasjonen sendes kun inn ved oppstart av virksomheten, og eventuelt ved endringer i registrerte opplysninger, se kapittel 7.4 for nærmere spesifisering.

7.2.3. Frivillig registreringsordning

Det bør på et senere tidspunkt vurderes å opprette en *frivillig registreringsordning for andre enn kvalifiserte sertifikater*, hvis det viser seg at markedet for denne typen sertifikattjenester er voksende. Det vises for øvrig til omtale i kapittel 5.4.

7.2.4. Frivillige godkjenningsordninger

Utvalget ser positivt på at det etableres *frivillige godkjenningsordninger* for CSPer i markedet, men anbefaler at det ikke tas noen initiativ fra myndighetene for å få etablert dette. En frivillig godkjenningsordning kan kombineres med en frivillig ordning for registrering av CSPer. Se kapittel 5.4 og 7.3.

Frivillige godkjenningsordninger kan baseres på de standarder som finnes for å sertifisere deler av en CSP-virkosmhet. Videre kan de baseres på andre krav som kan bidra til å styrke tilliten til CSPer. Se kapittel 5.4, 6.6 og vedlegg 1 og 2.

Det tas ikke initiativ fra myndighetene til en ordning for en total *akkreditert sertifisering* av CSPer nå. Det er to hovedgrunner til dette: Det er per i dag et for lite marked til å etablere en slik tjeneste i Norge, og CSPene anser at sertifisering blir for dyrt nå i en oppstartsfase. Det finnes ikke internasjonalt anerkjente standarder for en total sertifisering av CSPer som en sertifiseringsordning kan baseres på, kun etablerte ordninger for sertifisering av *deler* av CSPens virksomhet.

Utredningsgruppen anser at de eksisterende ordningene for sertifisering av IT-sikkerhet i Norge, sammen med muligheten for IT-revisjoner av CSPene, vil gi et tilstrekkelig grunnlag for å vurdere CSPens tillitsnivå. Hvis andre land igangsetter akkrediteringsordninger på dette området bør Norge følge opp og gjøre det samme. Likeledes hvis *nye* akkrediteringsordninger blir etablert i sammenlignbare land, bør man vurdere å gjøre det samme i Norge.

7.2.5. Gjensidig anerkjennelse

Utredningsgruppen anbefaler at det ikke legges opp til noen regulering av samvirke og/eller gjensidig anerkjennelse mellom CSPene fra myndighetene, når myndigheten er en regulatør eller kontrollør. Samvirke og/eller gjensidig anerkjennelse mellom CSPer gjøres best gjennom avtaler. Her har brukerne (markedet) en viktig oppgave. Det er brukerne som kan tvinge fram samarbeidsformer mellom de ulike leverandørene gjennom de krav de stiller som kunde.

Konkurransemyndighetene bør spille en viktig rolle ved en overvåking av markedet slik at det ikke oppstår kartelldannelser som utestenger nye aktører fra markedet.

7.3. Tilsynsmyndighet

Vi har i kapittel 5.5 argumentert for at det bør være *ett* tilsynsorgan for CSP-virksomhet.

På grunn av usikkerheten rundt utviklingen og lite tilsynsaktivitet i startfasen, og for å unngå spredning av kompetanse samt gråsoner og dobbeltarbeid mellom eventuelt nytt organ og eksisterende organer, vil vi anbefale at tilsyn med CSPer legges til et *eksisterende tilsynsorgan* *linkinthoveddel007P919_15891040*>.

Vi har i kapittel 5.7 nevnt myndighetsaktørene på området: Konkurransetilsynet, Post- og teletilsynet, Datatilsynet og Kredittilsynet.

Det vil være naturlig å velge et organ som allerede har en viss kompetanse når det gjelder de tekniske og faglige sidene ved de aktuelle aktørenes virksomhet. Videre bør den nye tilsynsoppgaven falle noenlunde naturlig in i den eksisterende oppgaveporteføljen.

Når det gjelder Konkurransetilsynet, har vi i kapittel 5.7.1 påpekt at direktivets bestemmelser om fri konkurranse vil måtte håndheves av dette organet. Andre aktuelle tilsynsoppgaver overfor CSPer ligger imidlertid utenfor Konkurransetilsynets virkeområde. Kredittilsynets tilsynsoppgaver gjelder utelukkende finanssektoren, og CSPer vil både kunne være innenfor og utenfor denne sektoren. Dermed vil det også for Kredittilsynets del bety å gå utenfor nåværende virkeområde dersom tilsyn med CSPer blir lagt til dette organet.

Datatilsynet og *Post- og teletilsynet* synes derfor å være mest aktuelle.

Grunner som taler for Datatilsynet som CSP-tilsynsmyndighet er:

- CSPene må allerede søke om konsesjon for opprettelse av personregistre hos Datatilsynet (etter den kommende loven vil det bli utvidet meldeplikt)
- Datatilsynet har en kontrolloppgave ovenfor alle CSPer siden de behandler personopplysninger.
- Datatilsynet har kompetanse på området datasikkerhet.

Grunner som taler for Post- og teletilsynet er:

- Post- og teletilsynet (PT) har allerede ansvar for å føre tilsyn med aktørene på post- og teleområdet. PT forvalter i dag et større antall forskrifter og utøver tilsyn på mange områder.
- PT fører allerede register over aktørene på post- og teleområdet.
- PT har en bred kompetanse både på det juridiske, økonomiske og teknologiske området, og er i sin virksomhet vant til å arbeide i grensefeltet mellom disse områdene.
- Med dereguleringen av telemarkedet har PT, i forbindelse med opprettelse og forståelse av samtrafikkavtaler mellom Telenor og de nye aktørene i telemarkedet, hatt rollen som mekler mellom partene.
- Sverige og Danmark har valgt sine Post- og teletilsyn som tilsynsmyndighet.

PT har også et bredt og omfattende internasjonalt kontaktnett og arbeider aktivt med internasjonale spørsmål. For flere av aktørene vil også PT være en kjent organisasjon å forholde seg til. PT vil derfor være et godt egnet sted å plassere tilsynet. PT er også en relativt stor organisasjon med ca 200 ansatte som lettere vil kunne innpasse nye områder i sitt arbeidsfelt. Datatilsynet har på sin side kun 22 tilsatte.

I valget mellom disse to eksisterende tilsyn konkluderer utvalget med å anbefale Post- og teletilsynet. Det legges særlig vekt på hva som er disse institusjonenes *hovedformål*. Post- og teletilsynets generelle formål er å sikre rimelige og gode post- og teletjenester. Å føre tilsyn med CSPer kan ses på som en del av dette. Datatilsynets hovedformål er mer avgrenset, nemlig å sikre personvernet. Tilsyn med CSPer vil være en oppgave som ligger på siden av hovedformålet.

7.3.1. Finansiering av tilsynet

Utvalget mener at tilsyn med CSP-er skal være *selvfinansiert*, slik som Post- og teletilsynet tilsynsoppgaver generelt er. Vi viser imidlertid til at det kan gjøres unntak fra bestemmelsene om gebyrer i det forslag til forskrift om gebyrer til Post- og teletilsynet som nylig er sendt på høring (svarfrist 11. februar 2000). Et slik unntak kan være aktuelt for å hjelpe markedet i gang.

Når bruken av CSP-tjenester eventuelt tar seg opp, vil gebyrer for CSPer kunne innarbeides. På grunn av raske endringer i telekommunikasjonssektoren må det uansett foretas hyppige endringer i gebyrstrukturen til Post- og teletilsynet.

Vi forslår at det inntil videre ikke legges gebyr på CSP-virksomhet. De relativt lave utgiftene som PT vil ha på dette området inntil dette eventuelt har utviklet seg til en ordinær kommersiell virksomhet, må enten kunne dekkes inn gjennom andre gebyrer eller ved en mindre, særskilt bevilgning til PT.

Valg av Post- og teletilsynet som tilsynsmyndighet medfører at *klager* rettes til Statens teleforvaltningsråd. Samferdselsdepartementet fatter vedtak i saker av prinsipiell karakter.

7.4. Innholdet i en registreringsordning

I henhold til direktivet skal myndighetene påse at det etableres et passende tilsyn overfor tilbydere av CSP-tjenester, se kapittel 3.4.

Et tilsyn vil måtte basere seg på en registreringsordning, slik at tilsynsmyndigheten har oversikt over de institusjonene det skal drives tilsyn med. Nedenfor foreslås det hvordan en registreringsordning kan legges opp, og hvordan tilsynet for øvrig bør være innrettet.

Ordningen må være *obligatorisk* for de virksomheter som *utsteder kvalifiserte sertifikater* og som sådan bør ordningen forankres i lov. Registreringen bør skje sentralt i *ett register*. Både aktørene og tilsynet vil ha hele landet som virkeområde, og det er derfor uaktuelt med en oppdeling i flere registre i henhold til en geografisk inndeling.

Alle relevante opplysninger samles i registeret. De relevante opplysninger myndighetene har i andre registre hentes der, jf oppgaveregisteret. Det vil være obligatorisk at virksomheten er registrert i Enhetsregisteret og Foretaksregisteret. For øvrig må registreringsordningen tilpasses til de registreringsordningene som det valgte tilsynsorganet allerede har.

Registeret må være *åpent* for å fylle sine funksjoner, dvs at opplysningene kan gis ut til tredjemann (publisitetshensyn). Felt som inneholder forretningshemmeligheter må dog skjermes for innsyn. Slik sett vil deler av virksomhetens sertifikatutstedelsespraksis være utilgjengelig for tredjemann.

Den som er ansvarlig for registeret må sikre at opplysningene er *riktige*, *komplette* og *oppdaterte* (notoritetshensyn). Registeret skal være et register over *nåværende godkjente virksomheter*. Det vil imidlertid være behov for å ta vare på opplysninger om tidligere registrerte CSPer så lenge sertifikater utstedt av disse fortsatt er gyldige. Dette medfører at tilbakekall av registreringer og andre sanksjoner må fremgå av registeret, og tas vare på et visst antall år etter at tilbakekallet/sanksjonen eventuelt er opphevet.

Virksomheten må *sende inn opplysningene noen dager før planlagt oppstart* av tjenesten, slik at man rekker å legge inn opplysningene i registeret.

Tilsynsmyndigheten bør være ansvarlig for registeret, med andre ord opprettes det ikke noe nytt forvaltningsorgan for registreringsformålet alene.

Registrerings- og meldingsordningen bør inkludere *status med hensyn til soliditet, egnethet* og *status i forhold til kravene i direktivets bilag II og III*[linkinthoveddel007P972_16562941]> .

Status i forhold til soliditet og egnethet kan ta utgangspunkt i de dokumentasjonskravene som settes i forbindelse med prekvalifisering av leverandører ved store offentlige IT-innkjøp.

Status i forhold til kravene i nevnte direktivbilag foreslås konkretiserte av virksomheten gjennom opplysning om:

- Sertifikatpolicy og sertifikatutstedelsespraksis.
- Foretatte revisjoner, verifikasjoner, sertifiseringer mv angående hele eller deler av CSP-organisasjonen iht til anerkjente standarder, for eksempel ISO 9000, BS 7799.
- Foretatte sertifiseringer mv angående signaturutstyr/ signaturgenereringssystemer iht standarder offentliggjort i Official Journal (jf artikkel 3:4 og 3:5)

Så lenge antall CSPer er meget lavt, og fordi Post- og teletilsynet allerede holder oversikt over aktører på post- og telemarkedet, vil omfanget av registreringsordningen i praksis bli beskjedent i starten.

Fotnoter

38 System for likning av næringsdrivende, SLN

39 Se http://www.justervesenet.no/na/

40 Det er kun tilsyn med den *spesifikke CSP-virksomheten* vi kommer med forslag om. Forslaget innebærer ingen innskrenkning i de eksisterende tilsynsorganers myndighet overfor CSPer.

41 Vi viser til at det er en myndighetsoppgave iht direktivet å påse at kravene i direktivets bilag III etterleves, jf kap 3.4

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

8 Økonomiske og administrative konsekvenser

Konklusjonen i kapittel 7 innebærer at det etableres en obligatorisk registreringsordning og at Post- og teletilsynet får nye tilsynsoppgaver.

Fordi markedet er umodent og det generelt er stor usikkerhet knyttet til utviklingen av CSP-tjenester, er det enkle løsninger som foreslås. Disse kan utvikles etter hvert til mer omfattende løsninger. Imidlertid vil den foreslåtte tilsynsordning bety at det må bygges opp kompetanse på dette området hos PT. Dette vil medføre kostnader for tilsynet.

Dette betyr ikke at statens utgifter til registreringsordning og tilsyn blir større etter hvert. Tvert i mot vil det ut fra statens ønske om å bidra til mer utstrakt bruk av elektroniske signaturer være nødvendig at staten bidrar mest i en startfase. I en startfase vil det for leverandører og brukere være en viss risiko, og leverandørene bør da ikke møte en ekstra økonomisk barriere i form av høye registreringsgebyrer, tilsynsavgifter og lignende.

Post- og teletilsynet (PT) er i dag selvfinansiert. Prinsipielt bør PTs tilsyn med CSP-virksomhet finansieres på samme måte som resten av virksomheten, men vi foreslår at det gjøres unntak fra gebyrplikten inntil man ser at den kommersielle utviklingen har kommet lengre.

I en overgangsfase vil PT da ha utgifter forbundet med CSPer som ikke dekkes gjennom gebyrer. Vi antar imidlertid at disse utgiftene blir svært beskjedne.

Hvorvidt registrering av CSPer i startfasen vil kunne skje ved å bygge ut PTs eksisterende registre, er ikke konkret vurdert, men blant annet på grunn av kravet om åpenhet antar vi imidlertid at det bør være et eget register.

Dersom det fattes en beslutning om at PT blir tilsynsmyndighet, kan det bevilges et *engangsbeløp* til dekning av de utgiftene tilsynet har fram til gebyr innføres. Statens rolle som finansieringskilde er med andre ord begrenset.

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

Vedlegg 1 - Kriterier og standarder

1.1. Mulige standarder for sertifisering av SAers sikkerhetsprodukter

1.1.1. ITSEC (Information Technology Security Evaluation Criteria).

Dette er den standarden som i dag benyttes i Europa ved evaluering av sikkerhetsprodukter.

Standarden ble ferdig i 1991 og har vært stabil etter dette. Ved evaluering velger produsenten et sikkerhetsnivå som produktet skal evalueres mot. Det finnes seks nivåer, nivå E1 til nivå E6. Det er også utviklet en egen evalueringsmetode som heter ITSEM (Information Technology Security Evaluation Method). Ved evaluering ser man både på produktets funksjonalitet, hvor effektivt produktet er og hvor godt produktet er implementert (De to siste egenskapene betegnes ofte som tillit). ITSEC angir ikke ferdig spesifiserte sikkerhetsfunksjoner. Funksjonalitet og tillit er heller ikke knyttet sammen . Dermed står produsenten ganske fritt til å spesifisere den funksjonalitet og tillit produktet skal evalueres mot.

Det finnes etablerte ordninger for evaluering mot ITSEC både i Tyskland og i England. En evaluering vil i disse landene normalt koste fra 400.000 - 700.000 kroner for en evaluering av et sikkerhetsprodukt på E2 nivå, mens et produkt på E3 nivå vil ligge på fra 1 million og oppover.

1.1.2. CC (Common Criteria).

CC foreligger nå i versjon 2.1. Den er også blitt utgitt som en ISO standard, ISO 15408.

CC ble utviklet for skaffe felles harmoniserte kriterier for sikkerhetsevaluering. CC er basert på kravene fra ITSEC, TCSEC og CTCPEC. CC benytter såkalte beskyttelsesprofiler for evalueringen. Hensikten er at interessegrupper kan utgi sine egne beskyttelsesprofiler ut fra regler gitt i CC. Disse profilene kan så valideres og registreres. Produsenter kan så velge å produsere utstyr som tilfredsstiller kravene til en eller flere profiler.

1.2. Mulige standarder for sertifisering av SAers grunnleggende sikkerhetsarbeid

1.2.1. BS 7799 : 1999 - British Standard 7799

BS 7799 er en standard som omhandler området "Information Security Mangement".

BS 7799 ble utviklet som et resultat av det offentliges, industriens og handelens behov for et felles rammeverk, slik at virksomheter kunne utvikle, implementere og måle virksomhetens sikkerhetsarbeid og rutiner. I tillegg skulle BS 7799 gi tillit ved handel mellom virksomheter; man hadde et mål på hvor godt det organisatoriske sikkerhetsarbeidet var ivaretatt. BS 7799 er basert på den beste nåværende praksis innen arbeidet med informasjonssikkerhet i en rekke store virksomheter i England (og senere også andre land). Det vil bli gjort forsøk på å få BS 7799:1999 anerkjent som en ISO standard.

BS 7799 består av to deler:

- BS 7799 Information security management - Part 1: Code of practice for information security management
- BS 7799 Information security management - Part 2: Specification for information security management systems

Del 1 er et veiledningsdokument, mens del 2 er et kravdokument som det kan sertifiseres etter.

BS 7799 er også blitt valgt som standard i Sverige og betegnes der som "SS 66 7799".

1.3. Mulige standarder for SAer sertifikatpolicy og -praksis

Et viktig element når man skal vurdere hvor godt drevet en CSP er å se på virksomhetens sertifikatpolicy og sertifikatutstedelsespraksis. En sertifikatpolicy er regler for utstedelse av digitale sertifikater. Sertifikatpolicyen fastsetter sikkerhetsnivået for tjenesten og derigjennom tillitsnivået. For en CSP som skal utstede kvalifiserte sertifikater bør det være et kav om at sertifikatpolicyen definerer en tjeneste på et høyt sikkerhetsnivå. Her kommer behovet for krav om standarder inn.

En sertifikatpolicy vil vanligvis omfatte blant annet følgende elementer: Organiseringen av CSPens virksomhet, CSPens generelle forpliktelser, hvordan identiteskontroll ved utstedelse av sertifikater foregår, operasjonelle krav til driften, hvordan de fysiske og administrative sikkerhetstiltakene gjennomføres, hvilket teknisk sikkerhetsnivå tjeneste operer på og hvilke sertifikatprofiler og tilbakekallsesprofiler tjenesten støtter.

En sertifikatutstedelsespraksis sier noe om den praksisen en CSP følger når den utsteder sertifikater. En CSP utsteder gjerne en beskrivelse av denne praksisen i en "Certificatin Practice Statement". Det er mulig å ha flere sertifikatutstedelsespraksiser som tilfredsstiller den samme sertifikatpolicyen.

Ved en vurdering av sikkerhetsnivået hos en CSP ser man først på om den sertifikatpolicyen CSPen benytter er hensiktsmessig. Deretter ser man på om sertifikatutstedelsespraksisen er i hht sertifikatpolicyen. Det siste man må se på er om sertifikatutstedelsespraksisen er gjennomført slik den er beskrevet.

1.3.1. RFC 2527

RFC 2527 (Standard fra Internet Enginering Task Force "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," March 1999) gir generelle føringer for hva som skal inngå i en sertifikatpolicy. Flere eksisterende

sertifikatpolicyer er basert på denne standarden, blant annet SEIS-policyen og policyen for "the government of Canada PKI"

1.4. Mulige standarder for innholdet i et kvalifisert sertifikat

Den generelle standarden som brukes for sertifikater er X.509v3. Denne standarden er meget generell og det er nødvendig å lage ulike profiler for å få sertifikater som kan benyttes innen gitte områder. Den vanligste standarden for å lage sertifikatprofiler og profiler for tilbakekallingslister er RFC 2459 "Internet X.509 Public Key Infrastructure Certification and CRL Profile". Dette er den generelle Internettstandarden for sertifikater. I tillegg finnes det profiler for spesielle sertifikater herunder kvalifiserte sertifikater. Profilen for kvalifiserte sertifikater finnes som et Internet-draft. "Internet X.509 Public Key Infrastructure Qualified Certificates Profile <draft-ietf-pkix-qc-01.txt>"

1.4.1. IETF-arbeide

Innen IETF finnes det en egen arbeidsgruppe som skal komme fram til et RFC for "Qualified certificates" basert på RFC 2459 for å lage X.509 profiler. Fra Internet-draftet som foreligger heter det:

" *This Internet-Draft forms a certificate profile for Qualified Certificates, based on RFC 2459, for use in the Internet. The term Qualified Certificate is used to describe a certificate with a certain qualified status within applicable governing law. Further Qualified Certificates are issued exclusively to physical persons represented by a registered unmistakable identity.."*

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

Vedlegg 2 - Ordninger for samsvarsvurdering av informasjonssikkerhet i Norge

Det finnes to ordninger for samsvarsvurdering (sertifisering) av informasjonssikkerhet i Norge. En ordning som går på sertifisering av produkter og en annen ordning som går på sertifisering av informasjonssikkerhet i organisasjoner.

2.1. Generelt om akkreditering og sertifisering

Den norske akkrediteringsordningen ble opprettet på bakgrunn av st prp 106 (1989-90) ved kgl res 7. juni 1991 med senere tilføyelse i kgl res 7. oktober 1993. Akkrediteringsorganet i Norge heter Norsk Akkreditering. Norsk Akkreditering har nasjonalt ansvar for å akkreditere blant annet sertifiseringsorgan, inspeksjonsorgan, tekniske kontrollorgan og attestasjonsorgan.

Norsk Akkreditering definerer selv akkreditering, sertifisering og akkreditert sertifisering slik (våre uthevelser):

- *Akkreditering* er en offisiell anerkjennelse av at en organisasjon arbeider i henhold til et dokumentert kvalitetssystem og har demonstrert kompetanse til å utføre nærmere beskrevne oppgaver. Akkreditering foregår ved at et objektivt organ, akkrediteringsorganet, vurderer virksomheten og bekrefter at den er i samsvar med internasjonale krav. Hensikten med akkreditering er å skape tillit til organisasjonen ved at den har fått dokumentert at den tilfredsstiller strenge krav beskrevet i internasjonale standarder.
- *Sertifisering* er en bekreftelse fra en uavhengig part om at et produkt eller en tjeneste tilfredsstiller kravene i et kravdokument. Sertifisering er en kommersiell aktivitet som i prinsipp hvem som helst kan utføre.
- *Akkreditert sertifisering* betyr at sertifiseringsorganet er akkreditert.

Den norske akkrediteringsordningen er del av en større europeisk ordning. Slik beskriver Norsk Akkreditering (NA) denne ordningen:

"NA er norsk representant i de internasjonale organisasjonene European cooperation for Accreditation (EA), International Laboratory Accreditation Cooperation (ILAC) og International Accreditation Forum (IAF). NA deltar i GLP-samarbeidet i OECDs GLP-panel og i EØS-samarbeid på området.

Norske akkrediteringer og norske akkrediterte tjenester anerkjennes i utlandet, fordi NAs arbeid tilfredsstiller kravene til akkrediteringsorgan gitt i flg standarder:

- *NS-EN 45003/ISO Guide 58 for akkreditering av laboratorier*
- *prEN 45010/ISO Guide 61 for akkreditering av sertifiseringsorgan.*
- *EMAS-forordningen, NS-EN 45503 og OECDs GLP-prinsipper stiller også krav til akkrediteringsorganet/inspeksjonsmyndigheten.*

NAs arbeid er bekreftet å tilfredsstille internasjonale krav ved vurdering fra EA, og NA har signert multilaterale avtaler (MLA) med et antall andre land i Vest-Europa om gjensidig anerkjennelse. Dette betyr at alle akkrediteringsorganene som har signert, anerkjenner akkrediteringer og akkrediterte tjenester fra de andre signatarene på lik basis som egne akkrediteringer og akkrediterte tjenester under egen ordning. Flere lands akkrediteringsorgan har søkt om å bli tatt opp i avtalene og er under

evaluering. Enkelte land utenfor Vest-Europa er assosiert til avtalene. GLP-inspeksjoner utført av NA anerkjennes også i alle EØS-land. NA kan gi utfyllende informasjon."

2.2. Sertifisering av informasjonssikkerhet i organisasjoner

Norsk Akkreditering har fått i oppdrag av Nærings- og handelsdepartementet å etablere en norsk ordning for akkreditering og sertifisering av informasjonssikkerhet i organisasjoner.

Det finnes i dag ingen internasjonal standard for krav til informasjonssikkerhet i organisasjoner. Den britiske standard BS 7799 er imidlertid tatt i bruk i en rekke land og er i ferd med å bli en "de facto" internasjonal standard. Det er denne standarden (BS 7799:1999 - part 2) som benyttes for å sertifisere en virksomhets sikkerhetsarbeid.

Framgangsmåten og strukturen i sertifiseringen er den samme for BS 7799 som f eks ISO 9000 sertifisering.

Bilde som beskriver gangen i sertifisering av en virksomhet etter f eks BS 7799.

Vi har her fire ulike nivåer. På det øverste nivået har vi de nasjonale myndighetene som er ansvarlig for akkrediteringsordningen. I Norge er dette NHD.

På nivå 2 ligger akkrediteringsorganet. I Norge finnes det et organ, Norsk Akkreditering. Norsk Akkreditering tar betalt for sine tjenester.

På nivå tre finner vi akkrediterte sertifiseringsorgan. Når et sertifiseringsorgan er akkreditert kan det utstede sertifikater til virksomheter som ønsker å sertifisere seg etter BS-7799. Dette skjer på lik linje med virksomheter om ønsker å sertifisere seg etter ISO-9000. Sertifisering etter ISO 9000 og BS 7799 omtales gjerne som sertifisering av kvalitetssystemer. Det er foreløpig ingen virksomheter som er akkreditert for å utføre sertifisering etter BS 7799 i Norge. Firmaer som er akkreditert for å utføre ISO 9000 sertifisering er blant annet: Det Norske Veritas Region Norge AS, Dovre Sertifisering AS, Grøner Certification A/S, Norwegian Certification System A/S, Scandpower Certification AS og TI Sertifisering A/S.

På nivå fire finner vi den enkelte virksomhet som ønsker å bli sertifisert.

Akkreditering av sertifiseringsorgan skjer etter EN45012. Dette er en generell europeisk standard (EN) som utpekte akkrediteringsorgan benytter for å akkreditere sertifiseringsorgan. I tillegg finnes det spesielle krav som er unike for de forskjellige sertifiseringsområdene. Kravene til f eks medarbeidernes kompetanse vil være forskjellig for sertifiseringsorgan som skal sertifisere etter ISO-9000 og sertifiseringsorgan som skal sertifisere etter BS-7799.

Veiledning til EN 45 012, som Norsk Akkreditering benytter ved akkreditering av sertifiseringsorganene som skal sertifisere etter BS-7799 er gitt i dokumentet: "EA Guidelines for the Accreditation of bodies operating certification/registration of Information Security Management Systems."

Eksempler på sertifiseringsorganer som foretar sertifisering etter BS 7799 i England og Nederland:

- KEMA Registered Quality Nederland B.V. (NED)
- KPMG Certification (NED)
- Lloyd's Register Quality Assurance Ltd (UK)
- Det Norske Veritas Quality Assurance Ltd (UK)
- National Quality Assurance Ltd (UK)

2.3. Sertifisering av IT-sikkerheten til produkter og systemer

FO/s er utøvende myndighet for sertifiseringen av IT-sikkerheten til produkter og systemer. Dvs at det er FO/s som utsteder sertifikater til de produkter som har vært gjenstand for evaluering av et evalueringsorgan. Evalueringsorgan blir akkreditert av Norsk Akkreditering som teknisk laboratorium etter EN 45001.

Sertifiseringen av IT-sikkerhetsprosukter er litt annerledes en sertifisering av øvrige produkter. I denne prosessen operer det med et sertifiseringsorgan som er utpekt av myndighetene og som ikke er akkreditert av et akkrediteringsorgan. Akrrediteringsorganet akkrediterer derimot evalueringsorganene som skal gjennomføre den faktiske testen av produktet. NB. Sertifiseringsorgane (FO/s) skal også godkjenne evalueringsorganet før det kan foreta evalueringer av IT-sikkerhetsprosukter. Dette avviker fra den normale prosedyren for akkreditering av testlaboratorier hvor akkrediteringsorganet er enerådende.

En vanlig sertifiseringsprosess vil være som følger. En virksomhet tar kontakt med et evalueringsorgan for å få vurdert IT-sikkerheten til produktet. Evalueringsorganet tester produktet og lager en evalueringsrapport. Evalueringsrapporten sendes sertifiseringsorgane som vurdere rapporten og utsteder sertifikat til produktet.

Vær oppmerksom på at FO/s har en utvidet godkjenningsmulighet når det gjelder godkjenning av kryptoprodukter.

Bilde som beskriver gangen i sertifisering av IT-sikkerhetsprodukter.

2.4. Samsvarsvurdering ved selvdeklarering

Man bør være klar over at en vanlig form for samsvarsvurdering av produkter er selvdeklarering. Her utføres samsvarvurderingen av produsenten selv. Vi må ta stilling til om selvdeklarering er tilstrekkelig for å validere at de produktene de kvalifiserte sertifikatutstederne CSPene benytter holder det sikkerhetsnivået myndighetene forlanger av denne typen tjenester.

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen

Vedlegg 3 - Definisjoner og ordforklaring

Hensikten med denne begrepslisten er primært å presisere i hvilken betydning utredningsgruppen har brukt ordet, sekundært hvordan andre bruker ordet. Det er videre et håp at måten utredningsgruppen bruker begrepene på, kan bidra til hensiktsmessige begreper på norsk og en god oversettelse til norsk av utenlandsk materiale, f eks direktivet.

Ingen av opplagsordene nedenfor er med i Norsk dataordbok (6. utgave, 1997)

Begrepslisten har vært forelagt Norsk språkråd, som i brev av 2.12.99 har gitt foreløpige kommentarer. Det er nedenfor opplyst eksplisitt om hvilke av begrepene Norsk språkråd har uttalt seg.

Accreditation (engelsk)

Akkreditering (dansk, norsk)

Ordet brukes i to betydninger:

a) I direktivet brukes ordet om en tillatelse som retter seg mot CSP, og som gir disse rettigheter og plikter, jf artikkel 2 - 13. b) Av Norsk Akkreditering brukes begrepet i forhold til sertifiseringsorganene. Akkreditering er en offisiell anerkjennelse av at en organisasjon arbeider i henhold til et dokumentert kvalitetssystem og har demonstrert kompetanse til å utføre nærmere beskrevne oppgaver. For betydningen a) bruker Norsk Akkreditering begrepet *sertifisering* (se dette). *Akkreditert sertifisering* betyr her at sertifiseringsorganet er akkreditert.

CA

Certification Authority:

Sertifikatenhet som går god for identiteten til en bruker (kunde?) og som utsteder et sertifikat om dette til brukeren (kunden?). CA kan være avhengig av en egen CKIS (den praktiske kort- og nøkkelutstedelsen), av produsenter av sertifikater og av separat sertifikatdatabasevert (repository).

"Sertifiseringsautoritet" bør unngås fordi ***autoritet*** gir gale assosiasjoner. I og med at det ikke er noen overordnet rolle det er snakk om, foretrekker vi enhet (i betydningen organisatorisk enhet). "Sertifisering" bør unngås fordi sertifisering (se dette) er noe annet enn utstedelse av sertifikater.

Norsk språkråd foreslår "sertifikatutsteder" (som bokmålsterm).

Certificate Policy (CP), se sertifikatpolicy

CKIS, se CA

CPS

Certification Practice Statement: Norsk betegnelse "Sertifikatutstedelsespraksis"

En erklæring (egenerklæring?) om hvilken praksis en CA (CSP?) bruker ved utstedelsen av sertifikater.

Norsk språkråd antyder "prakiserklæring om sertifikatutstedelse" (som bokmålsterm).

CSP

Certificate Service Provider: Norsk begrep "Tilbyder av sertifikattjenester"

Tilbyder av sertifikattjenester, en virksomhet som tilbyr utstedelse av sertifikater for digitale signaturer, og som selv eller i samarbeid med/etter avtale med andre virksomheter håndterer identitetskontroll (se RA), tildeling av navn, utsteder elektroniske sertifikater (se CA) og vedlikeholder informasjon om sertifikatene (se CRL). For hver av disse funksjonene/rollene kan det være samarbeidspartnere/underleverandører.

Digitale sertifikater

En digital signatur er en binding mellom en offentlig nøkkel og et sett med attributter.

Digital signatur

Elektronisk signatur

"An electronic signature, or digital signature, is an electonic analogue of a written signature in that can be used to assure a user that a document was, in fact, signed by the person who claims to have signed it (i.e. authentication). However, unlike its written equvalent, it can also prove that the content of an electronic document ha not been altered (i.e. it provides assurance of integrity)." (fra "Glossary of terms")

Norsk språkråd: "Her bør det helst velges én term. "Elektronisk signatur" passer best sammen med "electronic analogue" i forklaringa."

Frivillig akkreditering, se Akkreditering betydning a)

Kryssertifisering

To eller flere CSP i ulike PKI (se dette) som anerkjenner hverandres sertifikater. Dette kan skje frivillig basis, ved at en "topp CSP" går god for de øvrige CSP eller ved at myndighet går god for CSP (alle må akseptere sertifikater fra en CSP som myndighetene går god for).

Kvalifisert sertifikat

Sertifikat utstedet av virksomhet som mener å kunne dokumentere sin kompetanse.

Nøglecenter (dansk), se CSP

Offentlig nøkkelinfrastruktur, se PKI

Policyforvalter, se sertifikatpolicy

PKI

Public Key Infrastucture/offentlig nøkkelinfrastruktur:

Datasystemer, distribusjonssystemer og rutiner som eksisterer med det formål å generere, tilbakekalle (se CRL), sende ut og på annen måte håndtere offentlige nøkkelsertifikater

Norsk språkråd gjør oppmerksom på at "nøkkelinfrastruktur" skrives i ett ord.

Merknad: "Glossary of terms" har en noe avvikende definisjon. I denne er kryssertifisering en del av PKI, og ikke noe som eventuelt skjer mellom PKIer, slik Digitale signaturer gir tillit til elektronisk kommunikasjon (Gul rapport, vedlegg 1) poengterer.

RA, se CSP

SA, se CA

Sertifisering

Sertifisering er en bekreftelse fra en uavhengig part om at et produkt eller en tjeneste tilfredsstiller kravene i et kravdokument. Denne definisjonen er i henhold til Norsk Akkreditering, jf *akkreditering*

Sertifiseringsautoritet, se CA

Sertifikatpolicy

En sertifikatpolicy er regler for hvordan utstedelse av digitale sertifikater utstedes og behandles og hvem som har ansvaret for sikkerheten ved dette. Sertifikatpolicyen fastsetter altså sikkerhetsnivået for tjenesten og derigjennom tillitsnivået.

"A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" (FSP-1:1.0).

"Sertifiseringspolicy" bør unngås fordi sertifisering (se dette) er noe annet enn utstedelse av sertifikater.

Norsk språkråd mener at "policy" ikke bør brukes på norsk, og antyder "regelverk for utstedelse av sertifikater", med "sertifikatregelverket" som mulig kortvariant.

Sertifikattjenesteleverandør

Sertifikattjenestetilbyder, se CSP

Sertifikatutstedelsespraksis,

En *sertifikatutstedelsespraksis* sier noe om den praksisen en CSP følger når den utsteder sertifikater. En CSP utsteder gjerne en beskrivelse av denne praksisen i en "Certification Practice Statement".

"Praksis" skal her ikke forstås som den faktiske gjennomføringen, men som en operasjonalisering av sertifikatspolicy (se denne).

"Sertifiseringsprakis" bør unngås fordi sertifisering (se dette) er noe annet enn utstedelse av sertifikater.

System med begrenset antall deltakere

I direktivet er "closed system" (fortalen pkt 16) endret til "specified number of participants"

Tilsyn

Verifisering av om en adressat for rettigheter og plikter overholder disse, og eventuelt sette inn korrigerende tiltak (H.P. Graver). Begrepet brukes både om aktiviteten og om organet som utfører aktiviteten.

TTP

Trusted Third Party/Tiltrodde tredjeparter

Generelt: En organisatorisk/teknisk enhet som av andre parter er betrodd å ivareta sikkerhetsrelaterte funksjoner og oppgaver på deres vegne.

Ifm digitale signaturer: Se CSP. I nyere engelsk terminologi har TTP fått en snevrere betydning enn i norsk terminologi.

Lagt inn 4. februar 2000 av Statens forvaltningstjeneste, ODIN-redaksjonen