e-signaturs retsvirkninger

Betænkning nr. 1456

København 2004

Publikationen kan bestilles hos

Danmark.dk's netboghandel
Telefon **1881**
www.danmark.dk/netboghandel

100 kr. inkl. moms

Publikationen kan hentes på www.jm.dk

ISBN 87- 601-9994-6
ISBN 87- 601-9995-4 (Internet)

Tryk: Herrmann & Fischer A/S

INDHOLDSFORTEGNELSE

Kapitel 1

Indledning

1.1. Udvalgets kommissorium

Udvalget er nedsat af Justitsministeriet den 3. november 1998 og har følgende kommissorium:

> ” **1.** Digital kommunikation mellem borgere, virksomheder, myndigheder m.v. foregår i stadigt stigende omfang, bl.a. som supplement til eller i stedet for kommunikation på papir. Hidtil har det været det mest almindelige, at digital kommunikation foregår i net med adgang for en begrænset kreds, hvor de involverede kender hinanden og på forhånd har aftalt, hvordan og med hvilken virkning kommunikationen skal foregå. Fremover forventes kommunikation via åbne net imidlertid at blive væsentlig mere udbredt.
>
> **2.** I december 1997 fremlagde regeringen en redegørelse for Folketinget om sikker digital kommunikation. I redegørelsen formuleres et af de overordnede mål på dette område således, at der skal være mulighed for, at man i praksis kan anvende denne kommunikationsform på alle områder, hvor digitale meddelelser kan opfylde de samme funktioner som papirdokumenter. Under redegørelsesdebatten i januar 1998 tilsluttede et bredt flertal i Folketinget sig denne målsætning.
>
> Ved digital kommunikation opstår der bl.a. spørgsmål om, hvordan der kan opnås tilstrækkelig sikkerhed for, at en meddelelse faktisk stammer fra den angivne udsteder, og at meddelelsens indhold ikke er ændret efter, at den er afsendt.
>
> I lyset heraf og på baggrund af den nævnte redegørelse har Forskningsministeriet udarbejdet et udkast til et lovforslag om digital signatur baseret på såkaldt public key-kryptering, dvs. anvendelsen af private og offentlige "nøgler", der består af hver sin algoritme, som bygger på to meget store primtal og har en indbyrdes matematisk sammenhæng. Med denne teknik kan digitale meddelelser kodes ved hjælp af et edb-program og afsenderens private signaturnøgle, således at den offentlige nøgle bruges til at afkode meddelelsen.

Ved public key-kryptering er der behov for, at nogen - en såkaldt troværdig tredjepart - står inde for, at den offentlige nøgle kommer fra den angivne nøgleindehaver. Et væsentligt element i Forskningsministeriets lovudkast var på denne baggrund nogle regler om offentlig autorisation af "nøglecentre", som skal kunne bekræfte, at en offentlig nøgle kommer fra en bestemt person. Lovudkastet indeholdt bl.a. tekniske og organisatoriske regler om nøglecentrenes virksomhed samt regler om "spærring" af signaturnøgler, tidsmæssig begrænsning af, hvor længe en privat signaturnøgle kan anses for sikker, og begrænsninger i, hvilke retshandler m.v. nøglerne må bruges til.

Lovudkastet indeholdt herudover visse generelle regler om retsvirkningerne af at anvende digitale meddelelser med digital signatur. Reglerne drejede sig bl.a. om mulighederne for at opfylde skriftlighedskrav m.v. i lovgivningen med digitale meddelelser, som er påført en digital signatur. Reglerne drejede sig endvidere bl.a. om retsstillingen mellem afsenderen og modtageren af en digital meddelelse i visse særlige tilfælde, dels hvor en signaturnøgle er "spærret", dels hvor tidsgrænsen for en signaturnøgle er udløbet, dels hvor signaturnøglen anvendes uden for et på forhånd fastlagt anvendelsesområde.

3. Forskningsministeriets lovudkast har i foråret 1998 været til høring hos berørte myndigheder og organisationer m.v.

I forbindelse med høringen over det nævnte lovudkast blev der peget på, at bl.a. spørgsmålet om retsvirkningerne af at anvende digitale meddelelser med digital signatur burde overvejes nærmere af et sagkyndigt udvalg, inden der eventuelt tages initiativ til lovgivning herom.

Justitsministeriet har på denne baggrund i samråd med Forskningsministeriet besluttet at nedsætte et udvalg, der skal vurdere spørgsmålet om lovregulering af digitalt signerede meddelelsers retsvirkning. Det bemærkes, at spørgsmålet om de strafferetlige aspekter ved digital kommunikation behandles i Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet.

Forskningsministeriet agter at fremsætte et lovforslag for Folketinget om de organisatoriske og tekniske rammer for offentlig autorisation af nøglecentre, der har til opgave at fungere som "troværdig tredjepart", jf. ovenfor. Lovforslaget vil endvidere indeholde regler om nøglecentrenes ansvar over for brugerne og i den forbindelse formentlig også regler om spærring af nøgler, begrænsning af det tidsrum, hvor en privat nøgle kan anses for at

være sikker, og begrænsninger i nøglernes anvendelsesområde. Lovforslaget vil blive fremsat, når der er fornøden afklaring af indholdet af et direktiv om elektroniske signaturer, som for tiden drøftes i EU, jf. nedenfor.

Denne lovgivning vil have til formål at skabe det fornødne tekniske og organisatoriske grundlag for udbredelsen af en mere sikker digital kommunikation i åbne net.

3.1. På den anførte baggrund og i lyset af den samfundsmæssige interesse i at fremme brugen af sikker digital kommunikation er det en hovedopgave for udvalget at vurdere behovet for, at der lovgives om anvendelsen af digitale meddelelser med digital signatur i forbindelse med formkrav og andre retsregler, som knytter retsvirkninger til, at en meddelelse er skriftlig og/eller underskrevet. En eventuel regulering kan enten udformes som generelle lovregler, dvs. lovregler, der omfatter hele eller større dele af lovgivningen, eller - som der allerede er eksempler på - som lovregler, der regulerer brugen af digital kommunikation på et eller nogle enkelte områder for sig. Findes der at være behov for lovgivning, bør udvalget vurdere fordele og ulemper ved de nævnte former for regulering. Finder udvalget det mest hensigtsmæssigt, at lovgivning gennemføres på hvert område for sig, bør udvalget søge at opstille nogle overordnede principper for udformningen af sådanne lovregler.

Lovgivningen indeholder flere tusind af de ovenfor nævnte formkrav m.v., og det må antages, at disse bestemmelser i en del tilfælde ikke kan fortolkes således, at der kan anvendes digitale meddelelser. Udvalget bør i sine overvejelser bl.a. tage udgangspunkt i, at krav om skriftlighed og/eller underskrift kan have en række forskellige formål, f.eks. hensynet til bevissikring, hensynet til at skabe klarhed (vished) eller hensynet til at lette administrative procedurer m.v. Formålet kan f.eks. også være at gøre de involverede parter særligt opmærksomme på visse forhold. Formkrav kan endvidere have betydning ved anvendelsen af andre retsregler som f.eks. registerretlige og arkivretlige regler og regler om aktindsigt. En række formkrav i lovgivningen følger i øvrigt af internationale forpligtelser.

Udvalget bør endvidere tage udgangspunkt i de forskelle, der er mellem digitale meddelelser og meddelelser på papir. Blandt disse forskelle kan nævnes, at oplysninger, der alene foreligger i digital form, ikke har fysisk eksistens i samme forstand som oplysninger på papir. Ved papirdokumenter foreligger der et originalt fysisk eksemplar, mens dette ikke er tilfældet ved digital kommunikation. Papirdokumenter er umiddelbart læsbare, mens digitale meddelelser dels skal transformeres fra "maskinsprog" til læsbar form, dels kun kan læses ved anvendelse af bestemte edb-programmer. Oplysninger på papir gives ved hjælp

af skrift på papiret, mens digitale oplysninger kan have flere forskellige repræsentationsformer, både med hensyn til lagringen (elektronisk, optisk m.v.) og med hensyn til fremtrædelsen (skærmbillede, stemmesimulering m.v.). Ændring af indholdet af et papirdokument forudsætter et fysisk indgreb, som kan spores (f.eks. ved grafologisk undersøgelse), mens ændring af indholdet af en digital meddelelse kan ske ved en ikke umiddelbart synlig ændring af bit-mønstret. I modsætning til digitale data kan papirdokumenter fysisk besiddes, og derfor kan papirdokumenter bl.a. være bærere af en rettighed og være umiddelbart anvendelige som bevis.

3.2. En anden hovedopgave for udvalget vil være at vurdere spørgsmålet om eventuel særlig lovgivning om de retlige konsekvenser i forholdet mellem afsenderen og modtageren, hvis en digital signatur anvendes, efter at signaturen er blevet "spærret", hvis signaturen anvendes uden for et på forhånd angivet anvendelsesområde, eller hvis en privat nøgles tidsgrænse er overskredet. Udvalgets eventuelle forslag til lovregler herom bør udformes i lyset af den lovgivning, som Forskningsministeriet vil fremsætte forslag om, jf. ovenfor.

3.3. De ovenfor under pkt. 3.1 nævnte forskelle mellem papirdokumenter og digitale meddelelser kan rejse en række andre spørgsmål af retlig karakter, som også har betydning for, hvilke retsvirkninger digitale meddelelser kan have. Udvalget bør navnlig overveje, om der ved digital kommunikation kan opstå særlige problemer med hensyn til anvendelsen af aftalelovens regler, bl.a. om virkningen af, at en meddelelse er kommet frem eller er kommet til modtagerens kundskab. Udvalget bør endvidere på baggrund af de aftaleretlige ugyldighedsregler overveje spørgsmålet om bevisbyrden for, at en digital meddelelse med digital signatur er falsk eller forfalsket.

3.4. I det omfang udvalget vil anbefale, at der gennemføres lovgivning, skal udvalget udarbejde forslag til lovregler eller eventuelt forslag til overordnede principper for udformningen af lovregler på de forskellige enkeltområder, jf. pkt. 3.1.

Udvalget anmodes om at fremme sit arbejde mest muligt, eventuelt ved afgivelse af delbetænkninger.

4. Det forudsættes, at udvalget i sine overvejelser inddrager de synspunkter, der er kommet til udtryk i høringssvarene vedrørende Forskningsministeriets lovudkast, jf. ovenfor.

Det forudsættes endvidere, at udvalget som grundlag for sine overvejelser indhenter oplysninger om retsstillingen og erfaringerne i andre lande, herunder de øvrige nordiske lan-

de samt bl.a. Tyskland og Italien, hvor man for nylig har gennemført lovgivning om digital signatur.

Udvalget bør endvidere være opmærksom på det arbejde vedrørende regulering af elektronisk signatur og af elektronisk handel, som foregår i FN (UNCITRAL), OECD og andre internationale fora.

Udvalget skal særligt følge det igangværende arbejde i EU med Kommissionens forslag til direktiv om en fælles ramme for elektroniske signaturer. Dette direktivforslag, der er fremsat i maj 1998, indeholder både regler om de tekniske og organisatoriske rammer for elektronisk signatur og visse regler om retsvirkningerne af anvendelsen af elektroniske signaturer. Justitsministeriet vil løbende orientere udvalget om arbejdet med direktivforslaget med henblik på, at udvalgets synspunkter kan indgå ved fastlæggelsen af den danske regerings holdning til forslaget. "

1.2. Udvalgets betænkning nr. 1400/2000 om e-signatur og formkrav i lovgivningen

Udvalget om retsvirkningerne af digital signatur mv. har haft tre hovedopgaver. For det første at vurdere behovet for at lovgive om anvendelsen af digital kommunikation og elektronisk signatur i forbindelse med formkrav i lovgivningen mv. For det andet at overveje en række spørgsmål om retsvirkningerne af anvendelse af digital kommunikation og elektronisk signatur, herunder om der er behov for at lovgive om retsforholdet mellem afgiveren og modtageren af en digital meddelelse med elektronisk signatur. Endelig skal udvalget som en tredje opgave vurdere, i hvilket omfang der bør laves særlige aftaleretlige regler, som tager sigte på aftaler indgået med brug af elektroniske signaturer.

Efter udvalgets undersøgelse af den første hovedopgave afgav udvalget den 5. december 2000 delbetænkning nr. 1400/2000 om e-signatur og formkrav i lovgivningen. På baggrund af udvalgets undersøgelser af en række formkrav i lovgivningen foreslog udvalget bl.a., at hvert ministerium skulle foretage en gennemgang af egen lovgivning med henblik på at fjerne formkrav, der unødigt hindrer digital kommunikation. Herudover foreslog udvalget, at der i forvaltningsloven[1] indførtes en bestemmelse, hvorefter vedkommende minister skal have adgang til at fastsætte regler om, at der kan anvendes digital kommunikation ved henvendelser til den offentlige forvaltning og om de nærmere vilkår herfor.

---

[1] Lov nr. 571 af 19. december 1985 med senere ændringer.

Baggrunden for udvalgets afgivelse af delbetænkningen var bl.a., at en delbetænkning om e-signatur og formkrav i lovgivningen efter udvalgets opfattelse kunne medvirke til at fremme arbejdet med at udbrede digital kommunikation, ligesom en delbetænkning ville gøre det muligt for de enkelte ministerier at påbegynde arbejdet med en revision af lovgivningen med henblik på at fjerne formkrav, der unødigt hindrer digital kommunikation.

Udvalgets forslag er blevet udmøntet i regeringens lovmoderniseringsarbejde, som blev iværksat i januar måned 2002, jf. nedenfor i nr. 2.2.

1.3. Udvalgets sammensætning

Udvalget har ved afgivelsen af denne betænkning haft følgende sammensætning:

Vicepræsident for Sø- og Handelsretten Michael B. Elmer (formand)
Advokat Stig Bigaard, Advokatrådet
Dommer Ove Dam, Den Danske Dommerforening
Kontorchef Christian Brandt, Finansrådet
Fuldmægtig Sara Gøtske, Ministeriet for Familie- og Forbrugeranliggender
Chefkonsulent Susanne Andersen, Dansk Industri
Professor Peter Møgelvang-Hansen, Handelshøjskolen i København
Vicedirektør Jane Eis Larsen, IT-Brancheforeningen
Cand.jur. Anette Høyrup, Forbrugerrådet
Cand.merc.jur. Kenneth Smith Petersen, Dansk IT
Fuldmægtig Vibeke Henriques, Forsikring og Pension
Kontorchef Yih-Jeou Wang, Videnskabsministeriet
Kontorchef Henrik S. Øe, Justitsministeriet

Sekretariat:

Specialkonsulent Anders Christian Boisen, Videnskabsministeriet
Fuldmægtig Jacob Nygaard Waage, Justitsministeriet

1.4. Baggrunden for afgivelsen af denne betænkning

Som skitseret ovenfor har udvalget fortsat til opgave dels at vurdere spørgsmålet om eventuel særlig lovgivning om retlige konsekvenser af anvendelsen af digital signatur, dels at overveje om der ved anvendelse af digital kommunikation kan opstå særlige problemer med hensyn til anvendelsen af aftalelovens regler.

Udvalget har efter aftale med Justitsministeriet valgt at fremskynde sit arbejde vedrørende spørgsmålet om retsvirkningerne af digital signatur, således at der nu afgives denne delbetænkning. Spørgsmålene om anvendelsen af aftalelovens regler udskydes til en senere delbetænkning, idet der pt. foretages drøftelser i FN-regi (UNCITRAL) om en konvention om elektronisk kontraktindgåelse, som vil have direkte betydning for udvalgets overvejelser om anvendelsen af aftalelovens regler på digitale signaturer.

UNCITRAL's udkast til en konvention om elektronisk kontraktsindgåelse (draft convention on use of data messages in the context of international contracts)[2] indeholder således en række bestemmelser om centrale aftaleretlige spørgsmål, herunder bl.a. vedrørende sondringen mellem tilbud og opfordring til at gøre tilbud i relation til f.eks. annoncering på Internettet, om tidspunktet for afsendelse og modtagelse af elektroniske meddelelser og om automatiserede transaktioner, f.eks. aftaler eller transaktioner baseret på EDI (Electronic Data Interchange).

Det kan ikke udelukkes, at en gennemførelse af konventionen i dansk ret vil kunne rejse spørgsmål om behov for ændring af aftalelovens regler. Udvalget har derfor fundet det mest hensigtsmæssigt at afvente forhandlingerne i UNCITRAL vedrørende konventionsudkastet, førend udvalget nærmere overvejer, hvilke konsekvenser digital kommunikation har for anvendelsen af aftalelovens regler. Arbejdet med konventionen er som nævnt i gang, og det må forventes, at et endeligt udkast er færdigforhandlet i løbet af 2005.

Udvalget har fundet, at spørgsmålet om retsvirkningerne af brugen af digital signatur ikke behøver at afvente disse aftaleretlige spørgsmål, og har på denne baggrund besluttet sig for at afgive denne delbetænkning om retsvirkningerne i forbindelse med henholdsvis certifikatindehaverens egen brug af en digital signatur og tredjemands uberettigede brug af en certifikatindehavers digitale signatur. Udvalget har navnlig søgt at afdække forskellige spørgsmål om hæftelse og erstatning, som kan opstå ved anvendelse af en digital signatur i sådanne situationer.

---

[2] Konventionsudkastet er tilgængelig på UNCITRAL´s hjemmeside: www.uncitral.org/en-index.htm.

1.5. Lidt om begreberne i betænkningen

1.5.1. Signaturer

Det vil oftest være en naturlig del af en skriftlig aftale, at parterne tilkendegiver deres identitet i form af en signatur, typisk ved at parterne underskriver dokumentet. Der er imidlertid ingen formkrav til signaturen – allerede fordi der efter dansk ret ikke er noget krav om skriftlighed til aftaler. Signaturen kan således ud over at være en traditionel håndskreven underskrift f.eks. være vedkommendes initialer, et fingeraftryk, et håndfladeaftryk eller et segl. Ved vigtige aftaler anvendes ofte den fremgangsmåde, at hver enkelt side af den skriftlige aftale godkendes af parterne med deres initialer (såkaldt parafering), mens aftalen afsluttes med parternes (fulde) underskrift.

En signatur kan ud over at anvendes som identifikationsmiddel også i en vis udstrækning anvendes som et middel til at sikre, at et dokument efter udstedelsen ikke er ændret af nogen af parterne (eller af tredjemand).

Begrebet "elektronisk signatur" betegner generelt den teknik, der benyttes til elektronisk at signere en (elektronisk) meddelelse. Den elektroniske signatur er data i elektronisk form, der er vedhæftet (eller logisk tilknyttet) andre elektroniske data, og som angiver, at disse data stammer fra den pågældende afsender. Begrebet er rummeligt, idet det dækker over alt fra et navn, der placeres nederst i en mail, til f.eks. en kvalificeret digital signatur. En "elektronisk signatur" kan kort defineres som "enhver form for elektronisk angivelse af identiteten af en afsender af en elektronisk meddelelse".

En elektronisk signatur er med andre ord en metode til elektronisk at tilkendegive dokumentudstederens (afsenderens) identitet. En elektronisk signatur adskiller sig således i retlig forstand principielt ikke fra andre typer af signaturer, idet der – medmindre lovgivningen specifikt anfører andet – ikke er direkte retsvirkninger knyttet til brugen af den. En elektronisk signatur kan ligesom en traditionel underskrift være et betydeligt element i bevisbedømmelsen af, om der foreligger en aftale mellem to parter, eller om der efter udstedelsen af et dokument er ændret i indholdet heraf.

Som nævnt kan en elektronisk signatur f.eks. være en såkaldt digital signatur. Begrebet "digital signatur" er betegnelsen for en særlig teknologisk metode til at give større sikkerhed for identiteten på afsenderen af et elektronisk dokument og til at sikre, at meddelelsen ikke kan ændres efter

afsendelsen, uden at det senere vil kunne konstateres. Ligesom ved andre elektroniske signaturer er der ikke – medmindre andet er bestemt i lovgivningen – særlige retsvirkninger knyttet til anvendelsen af den digitale signatur, men som der redegøres for i nr. 3.2, vil en digital signatur kunne give større sikkerhed for, at den angivne udsteder af et elektronisk dokument rent faktisk er den egentlige udsteder, og at der ikke efter udstedelsen er foretaget ændringer i dokumentet.

Da begrebet digitale signaturer således er en delmængde af de elektroniske signaturer, vil det ofte være af mindre væsentlig betydning, hvilken betegnelse der anvendes. I denne betænkning anvendes primært begrebet "digital signatur", idet den type af signaturer, som betænkningen omhandler, i praksis er digitale. De steder i betænkningen, hvor der henvises til hele overgruppen af elektroniske signaturer, vil betegnelsen "elektronisk signatur" dog være brugt, ligesom begrebet vil blive brugt, hvor det rent sprogligt vil være naturligt, f.eks. flere steder i forbindelse med beskrivelsen af lov om elektroniske signaturer.

1.5.2. Nøglecentre og certificeringscentre

I lov om elektroniske signaturer betegnes den virksomhed, der udsteder certifikater, som et nøglecenter. Efter loven har nøglecentret en række særlige pligter, der skal sikre tilliden til kvalificerede certifikater. Nøglecentret skal således f.eks. påtage sig et skærpet erstatningsansvar (culpaansvar med omvendt bevisbyrde).

Betegnelsen nøglecenter er imidlertid ikke slået igennem som almindelig betegnelse for virksomheder, der udsteder certifikater, hvilket bl.a. kan skyldes, at navnet til en vis grad er misvisende. I OCES certifikatpolitikkerne udarbejdet af Videnskabsministeriet benyttes i stedet betegnelsen certificeringscenter, der er afledt af den engelske betegnelse Certification Authority, hvilket er i overensstemmelse med fast praksis i branchen.

Hertil kommer, at Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer anvender betegnelsen "certificeringstjenesteudbyder".

Udvalget finder på denne baggrund, at det vil være mest hensigtsmæssigt at anvende betegnelsen "certificeringscenter" i hele betænkningen. Kun hvor der – f.eks. i forbindelse med citater – alligevel måtte være grundlag herfor, vil betegnelsen "nøglecenter" blive benyttet.

1.6. Sammenfatning

Betænkningen gennemgår de retsvirkninger, som anvendelsen af digital signatur har efter gældende dansk formueret og foretager på baggrund heraf en vurdering af, om der er behov for særlige lovregler herom.

Kapitel 1 beskriver udvalgets arbejde og arbejdsplan. Endvidere redegør udvalget for baggrunden for, at udvalget efter aftale med Justitsministeriet har valgt at afgive denne betænkning og at udskyde spørgsmål vedrørende digital aftaleindgåelse til en senere betænkning.

Kapitel 2 indeholder en gennemgang af udviklingen på området siden afgivelsen af udvalgets første betænkning nr. 1400/2000 om e-signatur og formkrav i lovgivningen.

Kapitel 3 giver en overordnet beskrivelse af formålet med digitale signaturer og gennemgår centrale begreber som f.eks. signering og kryptering af meddelelser samt certifikater og certificeringscentre.

I kapitel 4 gennemgås lovgivningen om kvalificerede signaturer, herunder direktivet om elektroniske signaturer og lov om elektroniske signaturer.

Kapitel 5 gennemgår den praktiske anvendelse af signaturløsninger.

Kapitel 6 indeholder en beskrivelse af de tilsvarende regler i de øvrige nordiske lande.

Kapitel 7 indeholder udvalgets vurdering af gældende ret og på den baggrund udvalgets vurdering af behovet for lovregler om retsvirkningerne af anvendelsen af digital signatur.

Kapitel 7, afsnit 1, indeholder almindelige bemærkninger om underskrifters retsvirkning. Udvalget henviser indledningsvis til udgangspunktet i dansk ret om, at der ikke gælder særlige formkrav til aftalers indgåelse, jf. bestemmelsen i 5-1-1 i Danske Lov fra 1683. Det er således afgørende for, om en løftegiver bliver bundet, at der er afgivet et løfte, mens det er ligegyldigt, på hvilken måde løftet er afgivet.

Det slås endvidere fast, at reglerne om retsvirkningen af underskrifter bygger på, at det afgørende er tilkendegivelsen gennem handling eller undladelse af en vilje til at blive forpligtet, og at formen for denne tilkendegivelse er uden betydning.

Dette princip er grundlæggende teknologineutralt og kan siges at være udtryk for et princip om ækvivalens (ligestilling) mellem forskellige former for underskrifter og forskellige former for dokumenter (papirbaserede, henholdsvis elektroniske). Reglerne har kunnet anvendes uden særlige problemer, efterhånden som nye teknologier er blevet taget i anvendelse.

Udvalget lægger på den baggrund til grund, at det på tilsvarende måde er muligt at tage den nye teknologi, som brugen af digitale meddelelser og brugen af digitale signaturer er, i brug, uden at det er nødvendigt at ændre reglerne om retsvirkninger af underskrifter.

I *kapitel 7, afsnit 2,* gennemgås hovedformålene med og retsvirkningerne af begrænsninger i gyldigheden af certifikater, som er tilknyttet en digital signatur.

Udvalget fastslår, at retsvirkningerne af en digital underskrift i princippet ikke adskiller sig fra retsvirkningerne af en håndskreven underskrift, idet det afgørende er, at begge typer af underskrifter tilkendegiver en vilje til at blive bundet.

Udvalget er dog opmærksomt på, at der kan rejses nogle særlige spørgsmål om retsvirkningerne af brugen af digitale signaturer, fordi de certifikater, som er knyttet til digitale signaturer, kan være spærret eller udløbet, og fordi certifikatet kan angive, at den digitale signatur er undergivet visse anvendelsesbegrænsninger, herunder formålsbegrænsninger eller beløbsbegrænsninger.

Udvalget finder i den forbindelse, at hovedformålet med at spærre et certifikat er at beskytte certifikatindehaveren mod, at en anden uberettiget anvender den digitale signatur. Den vigtigste baggrund for tidsbegrænsning af certifikater er risikoen for, at de krypteringsalgoritmer, som den digitale signatur består af, med tiden vil kunne brydes, således at der efter tidsbegrænsningens udløb vil kunne være risiko for, at uvedkommende eftergør signaturen. Hovedformålet med at angive anvendelsesbegrænsninger i et certifikat må derimod i første række antages at være at begrænse certificeringscentrets ansvar over for brugerne og modtagerne af den pågældende digitale signatur.

Under henvisning til dansk rets udgangspunkt, som er, at der ikke gælder formkrav for afgivelse af løfter mv., fastslår udvalget herefter, at det efter gældende ret må antages, at begrænsninger i et certifikats gyldighed ikke har den virkning, at certifikatindehaveren ikke bliver bundet af dispositioner, som certifikatindehaveren selv foretager på trods af begrænsningerne mv. Hvis man ikke antog dette, ville certifikatindehaveren kunne benytte begrænsningerne i certifikatet til efter forgodtbefindende at gøre sig fri af sine forpligtelser, hvilket ville være en form for selvbåndlæggelse, der ellers som udgangspunkt ikke anerkendes i dansk ret.

Udvalget finder derfor, at det aftaleretlige udgangspunkt er, at certifikatindehaveren bliver bundet af dispositioner, som certifikatindehaveren selv foretager ved brug af digital signatur, også selv om certifikatindehaveren har anvendt signaturen, efter at den er spærret eller udløbet, eller i strid med en anvendelsesbegrænsning.

Udvalget finder mere generelt, at der alene bør indføres særlige lovregler om anvendelsen af digitale signaturer, hvis almindelige aftaleretlige regler og principper ikke fører til en rimelig og hensigtsmæssig retstilstand, eller hvis retstilstanden er uklar. Der bør endvidere kun ske en fravigelse af almindelige aftaleretlige principper, hvis der foreligger helt særlige grunde hertil.

Man bør efter udvalgets opfattelse holde sig til det aftaleretlige udgangspunkt om, at certifikatindehaveren bliver bundet af erklæringer, som den pågældende afgiver ved udveksling af elektroniske meddelelser forsynet med digital signatur, idet dansk rets almindelige regler efter udvalgets opfattelse giver en tilfredsstillende regulering af forholdet. Dette bør efter udvalgets opfattelse gælde, uanset om certifikatindehaveren har gjort brug af et udløbet eller spærret certifikat, eller om certifikatindehaveren under brug af en digital signatur har indgået en aftale, som strider mod en anvendelsesbegrænsning i certifikatet.

Herved vil man efter udvalgets opfattelse opretholde en klar og enkel retstilstand, der er i overensstemmelse med almindelige aftaleretlige principper om, at der ikke gælder særlige formkrav for løfter mv., og at en løftegiver bliver forpligtet af sit løfte.

En signaturmodtager, som har modtaget en digital signatur med et certifikat, der indeholder anvendelsesbegrænsninger, vil endvidere i praksis ikke have nogen muligheder for at værge sig imod, at hans kontraktspart skaber sig selv en sådan ensidig fortrydelsesret. Det vil således ofte være umuligt for signaturmodtageren at vurdere, om en digital signatur er anvendt i strid med anvendelsesbegrænsninger i et certifikat.

Kapitel 7, afsnit 3, behandler spørgsmålet om, hvorvidt en digital signatur kan indebære en fuldmagt.

Problemet er, i hvilket omfang en certifikatindehaver, som overlader sin digitale signatur til en anden, må anses for at have givet den anden fuldmagt (legitimation) til at handle på sine vegne. Spørgsmålet har navnlig praktisk betydning for såkaldte medarbejdercertifikater og virksomhedscertifikater.

Spørgsmålet om, hvorvidt der er opstået et fuldmagtsforhold, må afgøres på grundlag af almindelige aftaleretlige regler og principper herom, og vurderingen må i første række afhænge af en konkret vurdering af den enkelte sags omstændigheder.

Udvalget finder således ikke, at der kan udledes noget generelt af, at et certifikat er et medarbejdercertifikat eller virksomhedscertifikat. Udvalget finder i stedet, at der efter omstændighederne vil kunne være etableret et fuldmagtsforhold, f.eks. hvis det pågældende certifikat angiver medarbejderens stilling (stillingsfuldmagt), eller hvis det er udtrykkeligt angivet i certifikatet, at medarbejderen har kompetence til at forpligte sin organisation i et nærmere bestemt omfang (fuldmagt med særlig tilværelse). Hertil kommer, at konkrete forhold i den enkelte virksomhed eller den pågældende branche kan have betydning for vurderingen af, om et virksomheds- eller medarbejdscertifikat skaber et fuldmagtsforhold.

Afgørelsen af, om et medarbejdercertifikat eller virksomhedscertifikat skaber et fuldmagtsforhold, afhænger således i første række af en konkret vurdering af omstændighederne i den enkelte sag.

Udvalget finder, at spørgsmålet om fuldmagtsforhold i forbindelse med virksomheds- og medarbejdercertifikater kan løses tilfredsstillende på grundlag af almindelige aftaleretlige regler og principper, navnlig reglerne i aftalelovens kapitel II om fuldmagt, og at der ikke bør indføres særlige lovregler herom. Det må således overlades til retspraksis efter en konkret vurdering på baggrund af dansk rets almindelige regler at tage stilling til, om et medarbejdercertifikat eller virksomhedscertifikat indebærer et fuldmagtsforhold.

I *kapitel 7, afsnit 4,* behandler udvalget spørgsmålet om retsvirkningerne af uberettiget brug af andres digitale signaturer, herunder falsk i forbindelse med anvendelse af andres signaturer og forfalskning af erklæringer forsynet med en digital signatur.

Det klare udgangspunkt i dansk ret er, at man ikke bliver aftaleretligt forpligtet af en erklæring, der uberettiget afgives i ens navn (falsk) eller ændres efter afgivelsen (forfalskning). Der kan dog

undtagelsesvis opstå situationer, hvor en person uanset falsk eller forfalskning bliver aftaleretligt forpligtet, nemlig hvor den pågældende har foretaget handlinger eller undladelser, som af løftemodtageren kan opfattes som en indforståelse med at være bundet.

Det er udvalgets opfattelse, at disse almindelige formueretlige principper også gælder, hvor en digital signatur har været benyttet i forbindelse med falsk eller forfalskning.

Hvis den private nøgle, der hører til den digitale signatur, er kompromitteret (f.eks. røbet for andre), og certifikatindehaveren ikke efterfølgende spærrer sin signatur, vil dette efter omstændighederne kunne indgå i den samlede vurdering af, om certifikatindehaveren bliver forpligtet aftaleretligt. Manglende spærring vil således efter omstændighederne kunne medføre, at certifikatindehaveren anses for at have givet besidderen af den private nøgle, der uhindret får mulighed for fortsat at anvende denne, fuldmagt hertil. Der skal dog formentlig temmelig meget til, og navnlig må det formentlig kræves, at certifikatindehaveren har viden om, at den private nøgle er kompromitteret.

Udvalget finder ikke grundlag for at foreslå særlige regler for anvendelsen af digitale signaturer med henblik på at regulere, hvilken adfærd der vil kunne føre til, at certifikatindehaveren i disse tilfælde bliver aftaleretligt forpligtet af tredjemands misbrug af den digitale signatur. Udvalget finder således, at sådanne spørgsmål på samme måde som andre spørgsmål om falsk og forfalskning mest hensigtsmæssigt afgøres af domstolene ud fra almindelige aftaleretlige regler og principper.

På tilsvarende måde finder udvalget heller ikke behov for særligt at regulere en certifikatindehavers erstatningsansvar i de tilfælde, hvor uagtsomhed fra certifikatindehaveren medfører, at der påføres en tredjemand tab, fordi denne stoler på, at en erklæring afgivet under anvendelse af en digital signatur stammer fra den pågældende certifikatindehaver.

Med hensyn til dette spørgsmål må der på samme måde som i den almindelige erstatningsret foretages en afvejning af de konkrete omstændigheder, hvor der især må ses på, hvor høj grad af uagtsomhed certifikatindehaveren har udvist, og i hvilket omfang modtageren af den falske meddelelse indså eller burde have indset, at aftalen, retshandlen eller meddelelsen var falsk.

Det er således udvalgets samlede vurdering, at spørgsmål vedrørende uberettiget brug af digitale signaturer mest hensigtsmæssigt bør løses ud fra dansk rets almindelige formueretlige regler og principper, der overlader det til domstolene at træffe afgørelse på grundlag af en konkret vurdering af samtlige den enkelte sags omstændigheder. I den forbindelse finder udvalget, at den almindelige regel i erstatningsansvarslovens § 24 giver tilfredsstillende muligheder for i særlige tilfælde at lempe certifikatindehaverens erstatningsansvar.

I *kapitel 7, afsnit 5*, slår udvalget fast, at bevisbyrden for, om en digital signatur er anvendt af den berettigede certifikatindehaver, generelt må følge de samme bevisbyrderegler som dem, der gælder for traditionelle underskrifter.

Udvalget fremhæver, at tilstedeværelsen af en håndskreven signatur i almindelighed vil skabe en formodning for, at dokumentet er udstedt af den, hvis signatur er anvendt.

På tilsvarende måde skaber brugen af en digital signatur i forbindelse med et elektronisk dokument efter omstændighederne en formodning for, at det elektroniske dokument er signeret af den person, som angives i det certifikat, der hører til den digitale signatur. Der er dog visse forskelle mellem den håndskrevne og den digitale signatur, og navnlig er den håndskrevne signatur i langt højere grad end den digitale knyttet til den pågældende person. Dette vil domstolene være opmærksomme på i forbindelse med de bevisspørgsmål, som måtte opstå på dette område.

Den bevismæssige betydning af brugen af en håndskreven eller digital signatur kan i øvrigt efter udvalgets opfattelse ikke anskues isoleret, men må vurderes i sammenhæng med parternes forhold og omstændighederne i øvrigt. En formodning kan afkræftes, hvis der føres modbevis over for den sandsynliggørelse af afsenderens identitet, som brugen af digitale signaturer kan skabe.

Kapitel 7, afsnit 6, indeholder udvalgets afsluttende bemærkninger.

Udvalget fremhæver, at domstolene endnu ikke har haft lejlighed til at tage stilling til sager om retsvirkningerne af brugen digital signatur, og at udvalget derfor har måttet basere sine overvejelser på en abstrakt og generel gennemgang af tænkelige problemstillinger uden støtte i retspraksis.

På denne baggrund fremhæver udvalget behovet for, at man løbende overvejer, om der er behov for lovgivning om retsvirkningerne af brug af digital signatur i lyset af de erfaringer, som indvindes hermed, og den retspraksis, som dannes på dette område.

København, den 30. november 2004

Susanne Andersen Stig Bigaard Christian Brandt Ove Dam

Sara Gøtske Vibeke Henriques Anette Høyrup Jane Eis Larsen

Peter Møgelvang-Hansen Kenneth Smith Petersen

Yih-Jeou Wang Henrik S. Øe

Michael B. Elmer
(formand)

/Anders Christian Boisen
(sekretær)

Jacob N. Waage
(sekretær)

Kapitel 2

Udviklingen siden betænkning nr. 1400/2000

2.1. Indledning

Udvalgets delbetænkning 1400/2000 indeholder en række forslag med relation til digitale signaturer. I dette kapitel foretages en gennemgang af de konkrete tiltag, som forslagene har medført.

Herudover gives der en beskrivelse af en række andre væsentlige offentlige tiltag på IT-området med tilknytning til digitale signaturer.

Udviklingen er så vidt muligt beskrevet i kronologisk orden.

2.2. Regeringens handlingsplan for lovmodernisering

Under henvisning til betænkning nr. 1400/2000 fremlagde Justitsministeriet og Ministeriet for Videnskab, Teknologi og Udvikling den 11. januar 2002 en handlingsplan, som skulle bidrage til gennemførelsen af en lovmodernisering.

Handlingsplanen indeholdt blandt andet nedenstående beskrivelse af de opgaver, som de enkelte ministerier skulle udføre med henblik på at fjerne unødvendige hindringer for brug af digital kommunikation:

> "De enkelte ministerier skal med udgangspunkt i den af udvalget foreslåede model gennemgå egen lovgivning med henblik på at finde frem til de bestemmelser, der udgør eller kan udgøre en hindring for digital kommunikation, både for så vidt angår kommunikation mellem det offentlige og borgere og virksomheder mv. og kommunikation mellem borgere og virksomheder mv.
>
> Dernæst skal ministerierne overveje, om de konstaterede hindringer *bør* ændres, dvs. om der er særlige grunde til, at elektronisk kommunikation ikke bør finde anvendelse på et givet område. Herefter skal ministerierne på baggrund af lovgennemgangen udarbejde en *prioriteret handlingsplan* for arbejdet med at ændre de formkrav, som udgør en uhensigtsmæssig hindring for digital kommunikation.

Hvert ministerium skal i handlingsplanen redegøre for, hvordan de konkrete formkrav skal ændres, og hvornår ændringen kan forventes at være gennemført. Handlingsplanen skal desuden indeholde en oversigt over de hindringer, som ministerierne ikke har fundet anledning til at ændre samt en begrundelse herfor.

Rækkefølgen for moderniseringen af formkrav skal prioriteres i overensstemmelse med følgende retningslinjer:

- Formkrav, som udgør en hindring for en ønsket konkret anvendelse af digital kommunikation, ændres hurtigt. Det kan f.eks. dreje sig om, at gennemførelsen af konkrete digitaliseringsprojekter - eventuelt hos andre myndigheder - kræver, at bestemte formkrav ændres.

- En hurtig lovmodernisering er også generelt påkrævet for så vidt angår det kommunale og amtskommunale område, således at det sikres, at lovgivningen ikke lægger hindringer i vejen for kommuners og amters ønsker om at komme i gang med digital forvaltning mv.

- Formkrav, der er enkle at ændre, f.eks. fordi formkravet ikke længere tjener noget reelt praktisk eller juridisk formål, eller fordi den pågældende bestemmelse kan ændres ved bekendtgørelse, prioriteres ligeledes højt.

- Der tages hensyn til effektiviseringsgevinster for forvaltning, borgere og virksomheder.

Lovmoderniseringen kan ikke stå alene, men skal ses i sammenhæng med tilvejebringelse af de praktiske og tekniske løsninger til digital selvbetjening mv. Der er imidlertid ikke noget til hinder for, at lovgivningen moderniseres, selv om de praktiske løsninger endnu ikke er på plads. Det kan navnlig være relevant med en sådan "fremskudt" modernisering af lovgivningen på det kommunale og amtskommunale område, således at det sikres, at de kommuner eller amtskommuner, som ønsker at gå i gang med digital forvaltning på det pågældende område, ikke bliver hindret heri af lovgivningen.

Lovmoderniseringen skal desuden ses i sammenhæng med artikel 9 i EF-direktivet om visse retlige aspekter af informationssamfundstjenester, navnlig e-handel, i det indre marked (direktivet om elektronisk handel), hvoraf det følger, at medlemsstaterne skal sikre, at deres lovgivninger gør det muligt at indgå visse kontrakter elektronisk. Gennemførelsesfristen for direktivet er 17. januar 2002. Artikel 9 er omtalt i Justitsministeriets høringsskrivelse af 7. februar 2001 vedrørende delbetænkning nr. 1400 om e-signatur og formkrav i lovgivningen, der er fremsendt til samtlige ministerier."

Med henblik på koordinationen af lovmoderniseringsprogrammet blev der under Statens IT-råd og bestyrelsen for Projekt Digital Forvaltning[3] etableret et særligt sekretariat, Sekretariatet for lov-

[3] Statens IT-råd og Projekt Digital Forvaltning er beskrevet nedenfor i nr. 2.3 og nr. 2.4.

modernisering, bestående af medarbejdere fra Den Digitale Taskforce[4], Ministeriet for Videnskab, Teknologi og Udvikling og Justitsministeriet.

Sekretariatet offentliggjorde den 27. august 2002 et notat, som indeholder en gennemgang af de forskellige ministeriers arbejde med lovmoderniseringen. I notatets resumé og konklusion anføres følgende:

> "**Resumé**
>
> Resultatet af lovmoderniseringen er, at alle 18 ministerier har rapporteret deres handlingsplaner for modernisering af formkrav, der hindrer digital kommunikation. Gennemgangen betyder, at cirka:
>
> - 365 ændringer foretages administrativt
> - 88 lovændringer foretages i 21 forskellige love
> - 1085 formkrav, der hindrer digital kommunikation, ændres ikke.
>
> Antallet af indsendte skabeloner med lovændringer og administrative ændringer fordeler sig meget uligeartet på ministerierne. Enkelte ministerier har slet ikke indberettet nogen formkrav. Andre har indsendt hundredvis af skabeloner.
>
> Dette skal formentlig tages som udtryk for, at formkrav i lovgivningen, der hindrer digital kommunikation, er fordelt vidt forskelligt på de enkelte ressortområder.
>
> Langt de fleste ministerier har udelukkende indsendt skabeloner med bestemmelser, som indeholder formkrav, der hindrer digital kommunikation, men enkelte ministerier har også valgt at indsende skabeloner vedrørende formkrav, der er gennemgået, men som efter ministeriets vurdering ikke ses at hindre digital kommunikation.
>
> De ovenfor anførte 1085 formkrav er formkrav, der indeholder hindringer for digital kommunikation, men som efter ministeriernes vurdering ikke bør ændres under hensyntagen til de bagvedliggende hensyn. Mange af disse hensyn forekommer velbegrundede, f.eks. at der er knyttet retsvirkninger til besiddelsen af et bestemt dokument (pas, kørekort, særlige mærkningsordninger mv.), at formkravet har nødvendige bevisfunktioner, at andre tungtvejende hensyn gør sig gældende, eller at EU-regler eller internationale konventioner foreskriver det pågældende formkrav. F.eks. har Justitsministeriet ikke fundet anledning til at ændre § 20, stk. 2, i lov om ægteskabsindgåelse og opløsning, der kræver, at et vordende ægtepar møder personligt op ved deres egen vielse. Da ægteskab har vidtrækkende konsekvenser, bør parternes identitet og habilitet sikres ved personligt fremmøde.
>
> Sekretariatet har dog til visse ministerier fremsat specifikke bemærkninger til formkrav, der af det pågældende ministerium ønskes opretholdt, jf. nedenstående afsnit 5.

[4] Se nedenfor i nr. 2.4.

Man kan i øvrigt få indtryk af omfanget af ikke-hindrende formkrav ved at se på Økonomi- og Erhvervsministeriets handlingsplan, idet bl.a. dette ministerium har rapporteret såvel hindrende som ikke-hindrende formkrav. Af de i alt 1473 formkrav, som ministeriet har rapporteret, udgjorde 1022 (ca. 2/3) ingen hindring for digital kommunikation. Med de ændringer af hindrende formkrav, som ministeriet nu foreslår, vil omtrent 4/5 af ministeriets lovgivning fremover ikke udgøre en hindring for digital kommunikation. Et tilsvarende indtryk kan man få ved at se på dele af Undervisningsministeriets område.

Konklusion

Overordnet set er der i ministerierne gennemført et omfattende og et krævende arbejde i forbindelse med regeringens handlingsplan for lovmodernisering af formkrav.

Mange ministerier har udarbejdet gode og fremsynede handlingsplaner for lovmodernisering, der utvivlsomt vil skabe bedre muligheder for, at alle danskere kan kommunikere digitalt, med de fordele det indebærer. Ikke mindst den offentlige forvaltning kan nu i højere grad overgå til digital kommunikation på de områder, hvor de juridiske barrierer nu fjernes.

Sekretariatet må ud fra de indsendte handlingsplaner konstatere, at dansk lovgivning ikke ses at indeholde et væsentligt antal formkrav, der unødigt hindrer digital kommunikation. Der er i mange tilfælde blevet identificeret formkrav, som f.eks. skriftlighedskrav, hvor det er blevet fastslået, at disse ikke hindrer digital kommunikation.

Det kan anbefales ministerierne, hvor dette findes hensigtsmæssigt, at iværksætte oplysningsarbejde i forhold til dem, som reglerne retter sig til, så det bliver klart, hvor der nu kan benyttes digital kommunikation på det pågældende område.

Lovmoderniseringen vil kun medføre et moderat antal ændringer af love og administrative forskrifter.

Det kan i den forbindelse bemærkes, at der – som også forudsat forud for lovmoderniseringen – den 22. april 2002 er vedtaget en ændring af forvaltningsloven, der indfører en hjemmel for den enkelte ressortminister til at fastsætte regler om ret til at anvende digital kommunikation ved henvendelser til den offentlige forvaltning og om de nærmere vilkår herfor, herunder til at fravige formkrav i lovgivningen, der hindrer anvendelsen af digital kommunikation.

Endeligt kan det bemærkes, at flere ministerier har påpeget, at en mere udbredt anvendelse af digital kommunikation i forholdet mellem borgerne og det offentlige i højere grad end juridiske hindringer ses at bero på praktiske og tekniske forhold, herunder udvikling og udbredelse af digitale signaturer."

Størstedelen af formkravsændringerne angår Økonomi- og Erhvervsministeriets område, men også f.eks. lovgivningen på Beskæftigelsesministeriets område indeholder en række formkrav, der hindrer digital kommunikation.

Som det fremgår af citatet fra handlingsplanen, blev lovmoderniseringsarbejdet opdelt i flere faser. Handlingsplanen forudsatte således, at ændringer, der kunne ske administrativt, skete inden sommeren 2002, og at ændringer, der krævede fremsættelse af lovforslag, og som var af hastende karakter, skulle fremsættes efter Folketingets åbning i efteråret 2002 med ikrafttræden inden udgangen af 2002. Andre lovforslag skulle fremsættes hurtigst muligt med ikrafttræden i foråret 2003.

På baggrund af ministeriernes handlingsplaner og statusopgørelser konkluderede Sekretariatet for lovmodernisering, at stort set hele lovgivningen og den administrative regulering var blevet gennemgået med henblik på at finde formkrav, der unødigt forhindrer digital kommunikation, og at hovedparten af de tilbageblevne formkrav, der indeholder hindringer for digital kommunikation, skyldes sagligt velbegrundede hensyn, som f.eks. at der er knyttet retsvirkninger til besiddelse af et bestemt dokument (pas, kørekort, særlige mærkningsordninger mv.), at formkravet har nødvendige bevisfunktioner, eller at EU-regler eller internationale konventioner foreskriver det pågældende formkrav.

I forbindelse med tilbagemeldingen til sekretariatet påpegede flere ministerier, at en mere udbredt anvendelse af digital kommunikation mellem borgerne og de offentlige myndigheder beroede på praktiske og tekniske forhold, herunder udvikling og udbredelse af digitale signaturer, og kun i mindre omfang på juridiske hindringer.

Justitsministeriet har i øvrigt oplyst, at hensynet til digital kommunikation fremover vil indgå som et element i Justitsministeriets lovtekniske gennemgang af andre ministeriers lovforslag.[5]

2.3. Statens IT-råd

Statens IT-råd blev etableret i september 2000 med henblik på at udbrede anvendelsen af IT i den offentlige sektor.

Rådets to hovedopgaver er i samarbejde med de forskellige ministerier:

---

[5] Ovenstående bygger på oplysninger indhentet fra Sekretariatet for lovmodernisering.

- at bidrage med mulige initiativer til regeringens IT-politik, således at politikken opfylder regeringens overordnede målsætninger på området, og således at politikken bedst muligt støtter udviklingen i det danske samfund.
- at drøfte den statslige IT-politik, således at den statslige administration lettere kan udfylde sin del af regeringens IT-politik.

Alle ministerier er repræsenteret på ledelsesniveau med en direktør i Videnskabsministeriet som formand.

Aktiviteterne omfatter erfaringsudveksling, vejledninger og fælles løsninger. Andre samarbejdsområder vil være organisationsudvikling og kompetenceudvikling. Tekniske problemstillinger vil blive drøftet i et underudvalg, Statens IT-Forum, hvor ministeriernes IT-chefer mødes.

2.4. Projekt Digital Forvaltning og Den Digitale Taskforce

I sommeren 2001 besluttede regeringen, Kommunernes Landsforening og Amtsrådsforeningen, at iværksætte 'Projekt Digital Forvaltning' for at fremme omstillingen til digital forvaltning mellem myndighederne i den offentlige sektor.

Formålet med projektet er at afklare centrale juridiske, tekniske og organisatoriske problemstillinger vedrørende digital forvaltning og at sikre fremdrift i digitaliseringen af den offentlige sektor bl.a. ved at sikre, at der udarbejdes information og vejledning samt fælles rammebetingelser.

Projektet ledes af en bestyrelse, som er sammensat af departementscheferne i Finansministeriet, Justitsministeriet, Ministeriet for Videnskab, Teknologi og Udvikling, Økonomi- og Erhvervsministeriet, Indenrigs- og Sundhedsministeriet, de administrerende direktører i Kommunernes Landsforening og Amtsrådsforeningen, en repræsentant for København og Frederiksberg kommuner samt udviklingsdirektøren i Erhvervs- og Boligstyrelsen. Departementschefen i Finansministeriet er formand for bestyrelsen.

Projektets opgaver udføres af Den Digitale Taskforce og Ministeriet for Videnskab, Teknologi og Udvikling.

Den Digitale Taskforce, som beskæftiger cirka 20 medarbejdere – udstationeret fra forskellige ministerier, Kommunernes Landsforening og Amtsrådsforeningen – arbejder primært med organisatoriske og juridiske problemstillinger i forbindelse med indførelse af digital forvaltning og står

samtidig for udvikling af hjælpemidler samt et videncenter for offentligt ansatte, der er i gang med digitalisering på de enkelte institutioner.

Herudover medvirker taskforcen til at igangsætte tværgående samarbejder på centrale områder for omstillingsprocessen – de såkaldte servicefællesskaber. Den Digitale Taskforce har bl.a. arbejdet med etableringen af en fælles erhvervsportal (www.virk.dk), der samler digitale serviceydelser fra flere forskellige myndigheder i et fælles system, udbredelse af elektronisk sags- og dokumenthåndtering i offentlige myndigheder og en række konkrete digitaliseringsprojekter på områder som f.eks. sygedagpenge og boligstøtte.

I relation til digital forvaltning arbejder Videnskabsministeriet med tekniske problemstillinger i forbindelse med indførelse af digital forvaltning, herunder udbredelsen af digital signatur, standardiseringsarbejde og IT-sikkerhed.

Den Digitale Taskforce blev oprindelig oprettet for en periode på tre år. I forbindelse med økonomiaftalerne mellem regeringen og de kommunale parter i 2003 blev det imidlertid aftalt at videreføre Projekt Digital Forvaltning til udgangen af 2006 med sekretariatsbetjening af Den Digitale Taskforce.

2.5. OCES-signaturen

Ministeriet for Videnskab, Teknologi og Udvikling lancerede i foråret 2003 en digital signatur, baseret på den såkaldte OCES-standard. Det er hensigten, at OCES-signaturen skal være anvendelig for store dele af den digitale forvaltning.

OCES-signaturen er nærmere beskrevet nedenfor i nr. 5.2.

2.6. Lov om ændring af forvaltningsloven (digital kommunikation)

I betænkning 1400/2000 foreslog udvalget, at der gennem en ændring af forvaltningsloven blev indført en generel mulighed for den enkelte minister for at fravige gældende formkrav i lovgivningen om anvendelse af papirbaseret kommunikation ved henvendelse til forvaltningsmyndigheder.

Ved lov nr. 215 af 22. april 2002 blev udvalgets forslag gennemført ved indsættelse af følgende bestemmelse i forvaltningsloven:

> **§ 32 a.** Vedkommende minister kan fastsætte regler om ret til at anvende digital kommunikation ved henvendelser til den offentlige forvaltning og om de nærmere vilkår herfor, herunder fravige formkrav i lovgivningen, der hindrer anvendelsen af digital kommunikation.[6]

Ved lovændringen blev der således skabt hjemmel til at fravige regler i lovgivningen, som stiller krav om, at borgerne (eller myndigheder) i nogle sammenhænge skal anvende papirdokumenter ved henvendelser til en offentlig myndighed.

Efter bemærkningerne til lovforslaget er formålet med lovændringen at fremme og lette mulighederne for, at borgerne kan benytte den nye informationsteknik ved kommunikation med den offentlige forvaltning.

Lovbestemmelsen omfatter kun kommunikation med organer, der kan henregnes til den offentlige forvaltning, herunder såvel den statslige som den amtslige og kommunale forvaltning. Derimod gælder den ikke organer, der ikke er omfattet af forvaltningen, herunder domstolene og Folketinget. Lovbestemmelsen gælder al forvaltningsvirksomhed, altså både i henseende til afgørelsessager, til faktisk forvaltningsvirksomhed og ved det offentliges indgåelse af kontrakter.

Lovbestemmelsen omfatter heller ikke kommunikation mellem borgerne indbyrdes eller kommunikation fra offentlige myndigheder, men det anføres i bemærkningerne, at de nødvendige ændringer i formkrav, der indebærer en uhensigtsmæssig hindring for brug af digital kommunikation i overensstemmelse med udvalgets anbefalinger i delbetænkningen, forventes gennemført ved ændringslove på det enkelte område.

Det anføres endvidere i lovforslagets bemærkninger, at der ikke findes nogen generel lovgivning om formen for borgernes henvendelse til den offentlige forvaltning, og at det således som udgangspunkt må antages, at borgerne kan rette henvendelse til forvaltningen i den form, som de selv ønsker, forudsat at forvaltningen teknisk er i stand til at modtage henvendelser i denne form.

Lovbestemmelsen indeholder i øvrigt ikke en hjemmel for vedkommende minister til at udelukke specifikke former for kommunikation ved privates henvendelser til den offentlige forvaltning, f.eks. ved at fastsætte, at borgernes henvendelse til en offentlig myndighed alene kan ske ved brug af digital kommunikation.

---

[6] Se bemærkningerne til lovforslaget, Folketingstidende, 2001-2002, 2. saml., tillæg A, sp. 2062.

Obligatorisk eksamenstilmelding

Folketingets ombudsmand har i efteråret 2002 taget stilling til spørgsmålet om, hvorvidt en offentlig myndighed uden særlig lovhjemmel var berettiget til at pålægge en borger at benytte digital kommunikation ved henvendelse til myndigheden. I ombudsmandens referat af sagen anføres følgende:

"Af "Nyt fra Det juridiske Fakultet, Københavns Universitet", februar 2001, fremgik at tilmelding til sommereksamen 2001 kun kunne ske via Internettet.

Efter at have indhentet en udtalelse fra universitetet om sagen bad ombudsmanden Ministeriet for Teknologi, Videnskab og Udvikling om en udtalelse med henvisning til § 17, stk. 1, i ombudsmandsloven. Ombudsmanden bad ministeriet oplyse hvad det agtede at foretage sig i anledning af den ordning universitetet havde indført.

Ministeriet svarede at det havde meddelt universitetet at det efter ministeriets opfattelse krævede lovhjemmel at pålægge borgerne pligt til at benytte digital kommunikation ved henvendelse til offentlige myndigheder. Ministeriet havde derfor henstillet at Københavns Universitet ændrede det obligatoriske krav til en fakultativ ordning.

På denne baggrund meddelte ombudsmanden at han ikke foretog sig mere i sagen.[7]"

Ifølge lovforslagets bemærkninger kan det i alle tilfælde kræves, at borgeren i forbindelse med brug af digital kommunikation anvender et teknisk format, der indebærer, at borgerens henvendelse kan læses af myndigheden, ligesom forvaltningen også må være berettiget til at bestemme, at digitale henvendelser til myndigheden skal ske til en bestemt e-mail-adresse, der f.eks. kan være angivet på myndighedens hjemmeside.

Det fremgår således af ordlyden af forvaltningslovens § 32 a, at bestemmelsen ikke blot bemyndiger vedkommende minister til at fastsætte regler om ret til at anvende digital kommunikation ved henvendelser til den offentlige forvaltning, men også til at fastsætte regler om de nærmere vilkår herom.

Der vil herunder i visse tilfælde være anledning for vedkommende minister til at overveje, om der bør kræves en særlig sikkerhed for, at afsenderen af en henvendelse er den person, som vedkommende udgiver sig for. Det gælder f.eks., hvis der knytter sig særlige retsvirkninger til en henvendelse til den pågældende offentlige myndighed. I sådanne tilfælde må forvaltningen i fornødent omfang sikre sig afsenderens rette identitet f.eks. ved at anmode om, at henvendelsen signeres digitalt, eventuelt med en kvalificeret digital signatur.

---

[7] Folketingets Ombudsmands Beretning 2002, side 268.

Lovændringen giver altså mulighed for, at der i den enkelte bekendtgørelse fastsættes vilkår om, at digitale henvendelser på det pågældende område kræver brug af digital signatur. Vedkommende minister kan i den forbindelse også fastsætte vilkår om ret til brug af digital signatur på områder, hvor borgerne i dag efter den gældende lovgivning er berettiget til uden anvendelse af digital signatur at rette henvendelse til en offentlig myndighed ved hjælp af digital kommunikation, så længe det alene sker i tilfælde, hvor der foreligger særlige hensyn, som begrunder et sådant vilkår.[8]

I betænkning 1400/2000 opstillede udvalget en række retningslinjer, som udvalget fandt burde indgå i en vurdering af, på hvilke områder det kan være hensigtsmæssigt at fravige gældende formkrav, der vil kunne udgøre en hindring for digital kommunikation. Disse retningslinjer blev gentaget i bemærkningerne til lovforslaget, idet det her anførtes:

> "... at det i denne vurdering bl.a. må indgå, om der er et særligt behov for at kunne identificere afsenderen, og om formålet med et dokument kan opfyldes også ved brug af digitale medier. Desuden kan bl.a. administrative og økonomiske forhold samt behovet for bevissikring have betydning for, om det på det enkelte område vil være hensigtsmæssigt at fravige gældende formkrav om skriftlighed mv., herunder om der bør fastsættes vilkår for anvendelsen af digital kommunikation. Der henvises i øvrigt til betænkningen side 161 ff."[9]

Det forudsattes i bemærkningerne, at disse retningslinjer følges i forbindelse med anvendelsen af forvaltningslovens § 32 a.

Der henvises i øvrigt til gennemgangen af lov nr. 417 af 31. maj 2000 om elektroniske signaturer nedenfor i nr. 4.3, hvori det er omtalt, at bestemmelser i lovgivningen, hvorefter elektroniske meddelelser skal være forsynet med signatur, anses for opfyldt, hvis meddelelsen er forsynet med en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat, og som er fremstillet ved brug af et sikkert signaturgenereringssystem.

Forvaltningslovens § 32 a er f.eks. udnyttet i § 2 i bekendtgørelse nr. 33 af 20. januar 2003 om anmeldelse af arbejdsulykker mv. til Arbejdstilsynet:

---

[8] Folketingstidende 2001-02, 2. samling, tillæg A, sp. 2064.

[9] Folketingstidende 2001-02, 2. samling, tillæg A, sp. 2067.

"§ 2. Anmeldelse efter § 1 skal ske til Arbejdstilsynet i elektronisk form eller i papirform på særlige blanketter, der udleveres af Arbejdstilsynet og Arbejdsskadestyrelsen."[10]

2.7. Lovtiltag mod IT-kriminalitet

Ved lov nr. 352 af 19. maj 2004 om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven[11] er der gennemført en række regler med det hovedformål at skabe en forbedret strafferetlig beskyttelse mod IT-kriminalitet. Lovforslaget byggede på betænkning nr. 1417/2002 om IT-kriminalitet fra Justitsministeriets udvalg om økonomisk kriminalitet og datakriminalitet (Brydensholt-udvalget).[12]

Formålet med loven var endvidere ved ændringer af straffeloven og retsplejeloven at gøre det muligt for Danmark dels at ratificere Europarådets konvention om IT-kriminalitet (Convention on Cybercrime[13]) dels at deltage i vedtagelsen af en EU-rammeafgørelse om angreb på informationssystemer.

Lovændringen havde følgende hovedpunkter:

- Ny bestemmelse i straffeloven om uberettiget tilegnelse eller videregivelse af adgangskoder mv. til kommercielle og ikke-kommercielle informationssystemer.
- Forhøjelse af strafmaksimum for hacking fra 6 måneder til 1½ år og for hærværk fra 1 år til 1½ år.
- Forhøjelse af strafmaksimum fra 4 til 6 år for hacking af særlig grov karakter, groft hærværk og omfattende forstyrrelse i driften af almindelige samfærdselsmidler mv.
- Nye overbygningsbestemmelser i straffeloven om piratkopiering og industrispionage af særlig grov karakter med et strafmaksimum på 6 års fængsel.
- Ny bestemmelse i straffeloven om falske elektroniske penge.
- Ny bestemmelse i straffeloven om produktion, tilegnelse, besiddelse og videregivelse af falske betalingskort og betalingskortnumre.
- Udvidelse af dokumentfalskbestemmelsen til også at omfatte elektroniske dokumenter.

---

[10] Se også bekendtgørelse nr. 349 af 14. maj 2003 om administration af jordkøbslovens bestemmelser om statens forkøbsret mm. og bekendtgørelse nr. 950 af 26. november 2003 om lægers og tandlægers pligt til at anmelde arbejdsbetingede lidelser til Arbejdstilsynet og Arbejdsskadestyrelsen.

[11] Se bemærkningerne til lovforslaget, Folketingstidende 2003-2004, tillæg A, sp. 1761 ff.

[12] Betænkningen kan findes på: www.jm.dk/wimpdoc.asp?page=document&objno=64936#bund.

[13] Konventionen kan findes på: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

- Ændring af strafferammen for dokumentfalsk.
- Forhøjelse af strafmaksimum for rådighedshindring fra 6 måneder til 2 år.
- Ny bestemmelse i retsplejeloven om pligt for udbydere af telenet og teletjenester til at foretage "hastesikring" af elektroniske data på politiets begæring.

Lovændringen indeholdt regler, der tog sigte på i visse sammenhænge at sidestille den strafferetlige beskyttelse af elektroniske dokumenter med beskyttelse af fysiske dokumenter. Således blev bl.a. formuleringen af bestemmelsen om dokumentfalsk i straffeloven ændret, således at det af ordlyden klart fremgår, at den omfatter både skriftlige og elektroniske tilkendegivelser, der er bestemt til at tjene som bevis.

Hermed omfatter definitionen af begrebet dokument i straffelovens § 171, stk. 2, også eksempelvis falske e-mails. Samtidig blev strafferammen for dokumentfalsk i § 172 ændret, således at straffen nu er bøde eller fængsel indtil 2 år, der kan stige til fængsel i 6 år, hvis der foreligger skærpende omstændigheder, eller et større antal forhold er begået.

Straffelovens § 171

Den, der gør brug af et falsk dokument til at skuffe i retsforhold, straffes for dokumentfalsk.
Stk. 2. *Ved et dokument forstås en skriftlig eller elektronisk med betegnelse af udstederen forsynet tilkendegivelse, der fremtræder som bestemt til at tjene som bevis.*
Stk. 3. *Et dokument er falsk, når det ikke hidrører fra den angivne udsteder, eller der er givet det et indhold, som ikke hidrører fra denne.*

Straffelovens § 172

Straffen for dokumentfalsk er bøde eller fængsel indtil 2 år.
Stk. 2. *Er dokumentfalsk af særlig grov karakter, eller er et større antal forhold begået, kan straffen stige til fængsel i 6 år.*

2.8. eDag den 1. september 2003[14]

Efter anbefaling fra Projekt Digital Forvaltning aftalte regeringen og de kommunale parter, at alle offentlige myndigheder fra den 1. september 2003, den såkaldte eDag, fik ret til at sende og modtage dokumenter digitalt frem for på papir til og fra andre offentlige myndigheder.

[14] Se nærmere herom: www.e.gov.dk/sitemod/design/layouts/default/index.asp?pid=4490

Det er målet, at digital kommunikation bliver hovedreglen, når offentlige myndigheder kommunikerer med hinanden, og at papir kun benyttes undtagelsesvist, f.eks. ved dokumenter, der indeholder følsomme eller andre fortrolige oplysninger. Kommunikation med borgere og virksomheder var derimod ikke omfattet af eDag.

I henhold til aftalen om eDag skulle myndighederne fra den 1. september 2003 som minimum opfylde følgende krav:

1. Etablere en eller flere officielle e-post-adresser på myndigheds-, institutions-, afdelings- og/eller medarbejderniveau.
2. Implementere eDag baseret på nye arbejdsgange og rutiner omkring modtagelse og afsendelse af e-post, således at medarbejderne anvender, registrerer og håndterer e-post professionelt.
3. Sikre at IT-sikkerheden i myndigheden lever op til anbefalingerne fra Videnskabsministeriet.
4. Gennemgå dokumenttyper i organisationen og opstille nye retningslinjer for, hvilke dokumenttyper der skal sendes digitalt til andre myndigheder i fremtiden.
5. Tilrettelægge de nye kommunikationskanaler, herunder tage stilling til, hvordan massekommunikation skal foregå digitalt fremover, f.eks. via Internetservice.
6. Kommunikere eDag retningslinjerne til medarbejderne i organisationen.
7. Kommunikere institutionens nye retningslinjer for digital kommunikation til eksterne samarbejdspartnere.[15]

Dokumenter, der indeholder følsomme oplysninger om borgerne, f.eks. cpr-numre, eller andre fortrolige oplysninger, er ikke omfattet af aftalen.

Dokumenter, til hvis gyldighed der i lovgivningen er fastsat særlige krav, f.eks. om underskrift, og dokumenter, der ikke foreligger i digital form hos afsenderen, er heller ikke omfattet.

[15] De 7 punkter er citat fra aftalen om eDag udsendt den 19. februar 2003 fra formanden for bestyrelsen, Karsten Dybvad, til departementscheferne, direktørerne for styrelser og direktorater, amtsdirektører og kommunaldirektører.

2.9. eDag 2 den 1. februar 2005

Som opfølgning på eDag har Regeringen i samarbejde med de kommunale parter indgået en aftale om eDag 2, som skal iværksættes den 1. februar 2005. Med eDag 2 fokuseres på sikker digital kommunikation mellem private personer, virksomheder og myndigheder, således at også dokumenter med følsomt eller fortroligt indhold kan udveksles med anvendelse af den fælles-offentlige digitale signatur.[16]

Aftalen om eDag2 omfatter kommunale og amtskommunale centralforvaltninger, statslige departementer, styrelser og direktorater. Målet er, at 40 pct. af den brevpost, der i dag sendes som traditionel post, erstattes af elektronisk post.

I henhold til aftalen skal myndighederne senest den 1. februar 2005 som minimum opfylde følgende krav:

1. Etablere en eller flere officielle sikre e-post-adresser på myndigheds-, institutions-, afdelings- og/eller medarbejderniveau, hvortil der kan sendes sikker e-post.
2. Implementere eDag2 baseret på nye arbejdsgange og rutiner omkring modtagelse og afsendelse af e-post, således at medarbejderne anvender, registrerer og håndterer e-post professionelt.
3. Sikre at IT-sikkerheden i myndigheden lever op til anbefalingerne fra Videnskabsministeriet og gennemføre eventuelle forbedringer.
4. Gennemgå dokumenttyper i organisationen og opstille retningslinjer for, hvilke dokumenttyper der bør sendes ved hjælp af sikker e-post i fremtiden.
5. Tilrettelægge de nye kommunikationskanaler, herunder tage stilling til, hvordan kommunikation med borgere og virksomheder skal foregå digitalt fremover.
6. Kommunikere omstillingsprocessen til medarbejderne i organisationen.
7. Kommunikere institutionens ændrede retningslinjer for digital kommunikation til borgere, virksomheder og myndigheder.
8. Vælge og implementere en teknisk løsning til at håndtere sikker e-post.

[16] Se endvidere: www.e.gov.dk/edag

Kapitel 3

Digitale signaturer - begreber mv.

3.1. Indledning

En digital signatur er et redskab, som benyttes til – digitalt – at signere en meddelelse, således at en tredjemand, typisk modtageren af meddelelsen, kan konstatere meddelelsens autenticitet, dvs. identiteten af meddelelsens afsender, og integritet, dvs. at meddelelsens indhold ikke er blevet ændret efter afsendelsen.

En digital signatur har med andre ord til formål at forøge anvendelsesmulighederne for digital kommunikation ved at give modtageren af et digitalt dokument mulighed for at konstatere, om dokumentet og indholdet heraf stammer fra den angivne person. Er den digitale signatur sikker nok, vil den med andre ord kunne udgøre et væsentligt bevis i bedømmelsen af, om et digitalt dokument stammer fra udstederen.

En digital signatur kan således sammenlignes med en traditionel underskrift på den måde, at den knytter et bestemt dokument til en bestemt udsteder.

Signaturen kan som nævnt også tjene som bevis for, at et dokument ikke er ændret, efter at dokumentet er blevet sendt elektronisk. Ved afsendelsen af dokumentet kan afsenderen således vælge at signere den meddelelse, som dokumentet er vedhæftet, med den virkning, at dokumentets tekst låses og ikke kan ændres, uden at det vil kunne spores siden hen.

Med den udvikling i samhandel og andet samarbejde ved hjælp af elektroniske hjælpemidler, som Internettet og udbredelsen af e-mail har bevirket, er behovet for digitale signaturer stadigt stigende. Fjernsalg over Internettet bygger i vid udstrækning på aftaler mellem parter, hvoraf i hvert fald den ene af parterne ikke har kendskab til den anden. En digital signatur er et meget væsentligt bidrag for hver af parterne til at sikre sig den anden parts identitet.

3.2. Signering og kryptering af meddelelser[17]

En digital signaturs værdi afhænger af dens troværdighed. Den grad af sikkerhed, hvormed signaturen kan knyttes til en bestemt udsteder af en meddelelse, og hvormed det kan konstateres, at der ikke kan være foretaget ændringer i meddelelsen undervejs, er således af afgørende betydning.

Jo mere sikkert det er, at et dokument stammer fra en bestemt person, desto højere værdi har dokumentet som bevismiddel, hvis det senere skulle blive nødvendigt at bevise, at personen ved afgivelsen af meddelelsen vedstod sig dets indhold. Det er derfor vigtigt for udbredelsen af digitale signaturer, at man kan have tillid til, at signaturen virkelig stammer fra udstederen.

Den digitale signatur medfører en høj grad af sikkerhed og bygger på det såkaldte "offentlige nøgle-system" eller på engelsk "Public Key Infrastructure" (PKI). Systemet indebærer, at afsenderen er i besiddelse af to digitale nøgler, en privat og en offentlig. Disse udgør grundlaget for afgivelse og verificering af en digital signatur.

Denne private (signatur)nøgle er unik og skal holdes hemmelig af indehaveren. Det er således alene indehaveren, der har mulighed for at benytte den. Den offentlige nøgle er ligeledes unik, men er, som navnet angiver, principielt offentligt kendt og kan f.eks. være tilgængelig i et offentligt register på Internettet.

De to nøgler danner sammen et nøglepar, der er asymmetrisk forbundne, således at en meddelelse, der er låst (signeret) med den ene nøgle, kun kan åbnes med den anden nøgle. Det er den private nøgle, der benyttes til signering, og den offentlige nøgle, der benyttes til at verificere signaturen.

En lås – to koder

Man kan betragte sammenhængen mellem den private nøgle og den offentlige nøgle som sammenhængen mellem to koder til en elektronisk lås, hvor den ene kode skal bruges til at låse, og hvor den anden kode skal bruges til at låse op.

Teknikken bag den digitale signatur betyder, at en modtager af et signeret dokument kan opnå en meget høj grad af sikkerhed for identiteten på afsenderen og for, at der ikke er ændret i meddelelsen efter afsendelsen.

---

[17] Se endvidere side 24 ff i betænkning 1400/2000.

Sammenhængen mellem den offentlige og den private nøgle dokumenteres af et såkaldt certifikat, jf. nedenfor i nr. 3.3.

En vigtig forudsætning for sikkerheden ved en digital signatur er, at det ikke umiddelbart er muligt med kendskab til den ene nøgle at udlede den anden. Kendskabet til den offentlige nøgle kan derfor ikke benyttes til at udlede den private, således at uvedkommende kan afgive en falsk digital signatur i en andens navn. Dette udtrykkes ved, at nøglerne er asymmetriske.

Nøglernes styrke afhænger af deres matematiske kompleksitet i form af den datamængde, der danner grundlaget for nøglerne, udtrykt i antal bit. Men udviklingen i computerkraft betyder, at man til stadighed er nødsaget til at benytte stærkere nøgler for at forebygge, at de kan brydes. På grund af den teknologiske udvikling har en digital signatur således en begrænset levetid og skal med jævne mellemrum fornys.[18]

Ved digital signering sker der ikke nogen egentlig kryptering/hemmeligholdelse af meddelelsen. Digital signering giver således ikke i sig selv sikkerhed mod, at tredjemand skaffer sig adgang til og læser meddelelsen. Digital signering giver alene modtageren af et dokument sikkerhed for identiteten af afsenderen og for, at indholdet af dokumentet ikke er ændret efter afsendelsen.

En elektronisk underskrift

En elektronisk signatur kan sammenlignes med en traditionel underskrift. Underskriften har til formål at vise og bevise, hvem der er udsteder af et dokument. Tilsvarende har en elektronisk signatur til formål at vise og bevise, hvem der er afsender af en elektronisk meddelelse.

Kryptering af meddelelser

Kryptering kan benyttes, hvis en afsender af en elektronisk meddelelse ønsker sikkerhed for, at det alene er en bestemt modtager, f.eks. en bankrådgiver eller en offentlig myndighed, der kan læse indholdet af meddelelsen.

Teknikken bag digital signering – den asymmetriske sammenhæng mellem privat/offentlig nøgle – kan benyttes til en effektiv form for kryptering.

[18] En OCES-signatur skal f.eks. fornys hvert andet år.

Kryptering af en elektronisk meddelelse med henblik på, at indholdet kun skal kunne læses af modtageren, kan således ske ved, at afsenderen anvender modtagerens offentlige nøgle til at låse (kryptere) meddelelsen. Hermed sikrer afsenderen sig, at kun den, der har den private nøgle, kan åbne og læse meddelelsen.

F.eks. vil en bankkunde således kunne benytte sammenhængen mellem den offentlige nøgle og den private nøgle til at sende en fortrolig meddelelse til sin bankrådgiver med den virkning, at uvedkommende, der måtte opsnappe meddelelsen, ikke har mulighed for at læse dens indhold.

Ved at benytte bankrådgiverens offentlige nøgle (der f.eks. kan være tilgængelig via bankens hjemmeside) til kryptering af meddelelsen, før denne afsendes, sikrer bankkunden, at det alene er bankrådgiveren (indehaveren af den private nøgle), der kan dekryptere meddelelsen.

Ved at benytte denne teknik, er det – i modsætning til f.eks. de lukkede bankløsninger, hvor den offentlige nøgle opbevares i bankernes eget IT-system - muligt at sende krypteret post til en modtager, man ikke tidligere har haft kontakt til. Det eneste, som afsenderen behøver, er adgang til modtagerens offentlige nøgle.

3.3. Certifikater og certificeringscentre

Identiteten på den, som det pågældende nøglesæt tilhører, fremgår normalt af et såkaldt elektronisk certifikat, som er knyttet til nøglesættet. Det elektroniske certifikat udstedes af et certificeringscenter (certification authority, CA), som kan beskrives som en uafhængig tredjepart.

Certifikatet, som kan betragtes som certificeringscentrets tilkendegivelse til modtageren af en signeret meddelelse, vil typisk indeholde oplysninger om identiteten af den pågældende afsender (certifikatindehaver) og om, hvorvidt certificeringscentret har "tillid" til signaturen, dvs. f.eks. om den er tilbagekaldt af indehaveren, om meddelelsen kan være ændret undervejs, eller om certifikatet er udløbet.

Certificeringscentret er således en central aktør ved anvendelsen af digitale signaturer, idet det er certificeringscentret, der over for modtageren af et elektronisk signeret dokument tilkendegiver, at indehaveren af et certifikat er den, vedkommende udgiver sig for. Ud over at udstede certifikaterne er det desuden certificeringscentret, der fornyer og spærrer certifikater, hvis certifikatindehaveren anmoder herom, f.eks. hvis denne har mistanke om, at en uvedkommende har fået adgang til den private nøgle.

Certificeringscentrene har dermed som hovedopgave at knytte en bestemt person sammen med et nøglepar til afgivelse af digital signatur. Certificeringscentret kan selv udstede nøgleparret til en kunde og i den forbindelse udstede et certifikat til kunden. Et certifikat kan også udstedes til en kunde, der allerede er i besiddelse af et nøglepar til digital signatur, og som blot anmoder certificeringscentret om at udstede et certifikat til nøgleparret.

Når en person henvender sig til et certificeringscenter og anmoder om at få udstedt et certifikat til sin digitale signatur, må certificeringscentret kontrollere ansøgerens identitet.

Grundigheden af kontrollen af ansøgerens identitet afhænger af, hvad certifikatet og signaturen skal anvendes til. Der findes flere forskellige typer udstedelsesformer, der hver især giver et vist niveau af sikkerhed. En meget udbredt udstedelsesform er fremsendelse af registreringsoplysninger til ansøgerens postadresse kombineret med kontrol af cpr-oplysninger, men certificeringscentret kan også vælge at kræve, at ansøgeren giver personligt fremmøde, før et certifikat udstedes.

Et elektronisk certifikat er et elektronisk id-kort

Et elektronisk certifikat kan sammenlignes med et identifikationskort, mens et certificeringscenter kan sammenlignes med en myndighed eller virksomhed, som udsteder identifikationskort.

Sikkerheden bag digitale signaturer afhænger i høj grad af sikkerhedsniveauet hos certificeringscentret.

Som det fremgår nedenfor i nr. 4.3, stiller lov om elektroniske signaturer (lov nr. 417 af 31. maj 2000) krav om et højt sikkerhedsniveau ved kvalificerede certifikater, idet loven opstiller en lang række krav til certificeringscentre, der udsteder kvalificerede certifikater, herunder at centrene er undergivet tilsyn af IT- og Telestyrelsen.

Disse lovkrav gælder imidlertid udelukkende for de digitale signaturer, som er omfattet af loven. I princippet kan et certifikat udstedes af enhver. Modtagerens tillid til den digitale signatur vil derfor afhænge af tilliden til certificeringscentret og de procedurer, som certificeringscentret kræver for at sikre identiteten på certifikatindehaveren (angående de ikke-kvalificerede signaturer henvises til kapitel 5).

3.4. Hvilke faktorer har betydning for tilliden til et certifikat?

Brugernes tillid til certifikatet er som nævnt helt afgørende for, at certifikatet kan anvendes efter sit formål.

I motiverne til lovforslaget til lov om elektroniske signaturer[19] anføres en række forhold, som vil have betydning for signaturens sikkerhed, herunder

- Hvordan og hvor omhyggeligt certificeringscentret efterprøver underskriverens identitet forud for udstedelsen.
- Hvor sikre og omhyggelige certificeringscentrets procedurer er, når det gælder registrering af og information om, at et certifikat og en digital signatur er spærret eller udløbet, eller at certifikatet indeholder nogle anvendelsesbegrænsninger.
- At certifikatets oplysninger om ovennævnte er korrekte og fyldestgørende.
- Hvordan certificeringscentrets erstatningsansvar er i situationer, hvor der på et eller flere af de ovennævnte punkter er ukorrektheder i certifikatet eller på anden vis er sket fejl hos certificeringscentret, og dette har ført til tab hos enten afsender eller modtager.
- Kvaliteten af selve den elektroniske signatur, der anvendes i forbindelse med certifikatet, dvs. om det reelt er umuligt at bryde eller eftergøre signaturen, uden at det efterlader synlige spor.

Hertil kan f.eks. også føjes karakteren af den metode, som signaturindehaveren skal benytte ved anvendelse af den digitale signatur, herunder eksempelvis udformningen af passwords.

Hvor betydningsfulde ovennævnte forhold er, vil afhænge af, hvad signaturen ønskes brugt til. Man kan således sagtens forestille sig situationer, f.eks. når man skriver mindre forpligtende meddelelser, hvor der slet ikke vil være behov for at signere meddelelsen. Til gengæld kan man også forestille sig situationer, f.eks. hvor der er tale om meget fortrolige dokumenter, herunder dokumenter med følsomme personoplysninger, hvor et højt sikkerhedsniveau er af afgørende betydning.

---

[19] Se pkt. A 1 i de almindelige bemærkninger til forslag til lov om elektroniske signaturer, Folketingstidende 1999-2000, tillæg A, s 6346.

3.5. Nærmere om indholdet af et certifikat

Som nævnt ovenfor er et elektronisk certifikat en tilkendegivelse fra certificeringscentret, som indeholder en række oplysninger om certifikatindehaveren.

I lov om elektroniske signaturer angives der en række oplysninger, som et kvalificeret certifikat skal indeholde, herunder bl.a.:

- En angivelse af, at certifikatet er udstedt som et kvalificeret certifikat.
- Certificeringscentrets navn og hjemsted.
- Underskriverens navn eller pseudonym med angivelse af, at der er tale om et pseudonym.
- Eventuelle yderligere oplysninger om underskriveren, for så vidt det er nødvendigt for anvendelsen af certifikatet, herunder oplysninger, der sikrer en entydig identifikation af underskriveren.
- Certifikatets gyldighedsperiode.
- En tydelig angivelse af eventuelle begrænsninger i certifikatets anvendelsesområde (formålsbegrænsninger).
- En tydelig angivelse af eventuelle begrænsninger med hensyn til de transaktionsbeløb, certifikatet kan anvendes til (beløbsbegrænsninger).

Selv om lov om elektroniske signaturer kun retter sig mod kvalificerede certifikater, vil disse oplysninger også kunne fremgå af andre typer certifikater, da certifikaternes indhold i vidt omfang baseres på internationalt fastsatte standarder. F.eks. indeholder OCES-certifikaterne plads til oplysninger, der svarer til nogle af dem, der er nævnt ovenfor i punktopstillingen.

3.6. Begrænsninger i certifikatet

Et certifikat kan som nævnt indeholde oplysninger om, at certifikatet kun er beregnet til identifikation af afsenderen i forbindelse med et bestemt formål, f.eks. til kommunikation med skattemyndighederne eller til identifikation ved transaktioner op til et vist beløb. Oplysningerne om disse eventuelle begrænsninger vil være tilgængelige for den, der modtager et dokument signeret med en digital signatur.

Angivelse af begrænsninger har ikke været brugt i større omfang i praksis.

Et certifikats begrænsninger har til formål at begrænse certificeringscentrets ansvar i de tilfælde, hvor dette ellers ville kunne blive gjort ansvarlig for tab hos den, der forlader sig på certifikatet. Begrænsninger i certifikatet har derimod ingen betydning mellem parterne i et aftaleforhold, hvortil der ved indgåelsen har været anvendt en digital signatur.

Der er i de systemer til e-post og e-handel, som er almindelige i dag, ikke indlagt nogen automatisk kontrol af, om certifikater til modtagne signaturer er udløbet eller spærret, eller om de indeholder anvendelsesbegrænsninger. Modtageren af en signeret meddelelse må således foretage en nærmere undersøgelse af certifikatet for at få oplyst, om certifikatet er udløbet eller spærret eller indeholder en anvendelsesbegrænsning, således at modtageren kan tage de forholdsregler, som måtte være hensigtsmæssige i situationen, f.eks. kræve, at afsenderen anvender en digital signatur med et gyldigt certifikat.

Der er nedenfor i nr. 7.2 nærmere redegjort for, hvilke retsvirkninger sådanne begrænsninger må antages at have over for certificeringscentret, certifikatindehaveren og certifikatmodtageren.

Kapitel 4

Lovgivning om kvalificerede signaturer

4.1. Indledning

Den danske lovgivning om kvalificerede elektroniske signaturer bygger i det væsentligste på Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (herefter betegnet direktivet om elektroniske signaturer).

I dette kapitel foretages i nr. 4.2 en gennemgang af dette direktiv. Der er i en vis udstrækning tale om en ajourføring og udbygning af nr. 3.2. i betænkning nr. 1400/2000, men på grund af den nære sammenhæng med afsnittet om lov om elektroniske signaturer har udvalget fundet det mest hensigtsmæssigt at medtage en opdateret gennemgang.

Herudover foretages i nr. 4.3 en nærmere gennemgang af lov nr. 417 af 31. maj 2000 om elektroniske signaturer.

4.2. Direktivet om elektroniske signaturer[20]

Som nævnt i betænkning nr. 1400/2000 fremsatte Europa-Kommissionen i 1998 et forslag til et direktiv, hvilket resulterede i vedtagelsen af direktivet om elektroniske signaturer.[21]

Formålet med direktivet er – gennem fastsættelse af fælles retningslinjer for elektroniske signaturer og de tilknyttede certificeringstjenester mv. – at forbedre mulighederne for elektronisk samhandel i det indre marked. Dette søges opnået ved at gøre det muligt for en modtager af en elektronisk meddelelse at kunne opnå sikkerhed for afsenderens identitet og for, at indholdet ikke er blevet ændret efter afsendelsen. Hensigten hermed har bl.a. været at skabe rammer for en udvidet adgang til at foretage elektronisk handel ved at gøre det lettere at indgå juridisk bindende aftaler over Internettet (og andre åbne net).

---

[20] For en nærmere beskrivelse henvises til bemærkningerne til forslag til lov om elektroniske signaturer, Folketingstidende 1999-2000, tillæg A, sp. 6398 ff., og til betænkning 1400/2000 s. 41 ff.

[21] Direktivet og loven om elektroniske signaturer er optrykt som bilag 1 – 2 til betænkningen.

Direktivet opstiller bl.a. bestemmelser for markedsadgangen til at udbyde elektroniske signaturer og tilknyttede certifikattjenesteydelser (artikel 3), principper vedrørende det indre marked, herunder om forbud mod diskrimination mod certificeringstjenester fra andre medlemsstater og om fri bevægelighed inden for det indre marked for elektroniske signaturprodukter omfattet af direktivet (artikel 4), forskellige bestemmelser om retsvirkningerne af elektroniske signaturer og avancerede elektroniske signaturer (artikel 5), regler om erstatningsansvar for certificeringscentre (artikel 6), særlige regler om anerkendelse af kvalificerede certifikater fra lande uden for EU (artikel 7) og regler om databeskyttelse (artikel 8).

Ordforklaring til direktivets tekst[22]

Elektronisk signatur: Data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre elektroniske data, og som anvendes som en autentifikationsmetode.

Avanceret elektronisk signatur: Elektronisk signatur, som opfylder følgende krav:
- den er entydigt knyttet til underskriveren
- den kan identificere underskriveren
- den genereres med midler, som underskriveren kan bevare den fulde kontrol med, og
- den er knyttet til de data, som den vedrører, på en sådan måde, at en hvilken som helst senere ændring af disse data kan opdages.

Certificeringstjenesteudbyder (certificeringscentre): Et organ eller en fysisk eller juridisk person, der udsteder certifikater eller leverer andre tjenesteydelser i forbindelse med elektroniske signaturer.

Certifikat: En elektronisk attestation, som knytter signaturverificeringsdata til en person og bekræfter denne persons identitet.

Kvalificeret certifikat: Et certifikat, som opfylder kravene i direktivets bilag I og leveres af en certificeringstjenesteudbyder, som opfylder kravene i direktivets bilag II.

Signaturgenereringsdata: Unikke data, som f.eks. koder eller private krypteringsnøgler, som anvendes af underskriveren til generering af en elektronisk signatur. Bliver populært betegnet som "den private nøgle".

Signaturgenereringssystem: Konfigureret software eller hardware til behandling af signaturgenereringsdata (Edb-systemer mv., som gør det muligt at anvende den private nøgle, eller med andre ord det system, hvori den elektroniske signatur teknisk foretages).

Signaturverificeringsdata: Data, som f.eks. koder eller offentlige krypteringsnøgler, der anvendes til kontrol af den elektroniske signatur. Bliver populært betegnet som "den offentlige nøgle".

[22] Se endvidere direktivets artikel 2.

4.2.1. Direktivets bestemmelser om retsvirkningerne af elektroniske signaturer

Det fastslås i artikel 1, at direktivet ikke omfatter "*aspekter i forbindelse med kontrakters indgåelse og gyldighed eller andre retlige forpligtelser, som ifølge national ret eller fællesskabsret er undergivet formkrav, og heller ikke berører de regler og begrænsninger, der efter national ret eller fællesskabsret gælder for anvendelsen af dokumenter.*"

Bestemmelsen betyder, at det fortsat vil være op til medlemsstaterne at afgøre, på hvilke retsområder og i hvilke situationer man vil acceptere, at elektroniske signaturer skal opfylde formkrav om underskrift mv. Direktivet vil således ikke få betydning for spørgsmålet om, hvorvidt formkrav i lovgivningen om skriftlighed eller underskrift kan opfyldes ved brug af elektronisk kommunikation og elektronisk signatur.

I direktivets artikel 5, stk. 1, knyttes visse retsvirkninger til en såkaldt "avanceret elektronisk signatur". Reglerne i artikel 5, stk. 1, går ud på, at en "avanceret elektronisk signatur", som er frembragt på sikker vis – dvs. frembragt i overensstemmelse med de tekniske og proceduremæssige krav, som opstilles i direktivets bilag III – skal anses for at opfylde formkrav om underskrift på papirdokumenter og skal kunne benyttes som bevis i retssager, forudsat at anvendelsen af elektroniske signaturer i den pågældende sammenhæng er anerkendt af medlemsstaten, og uden at det påvirker princippet om fri bevisbedømmelse ved domstolene.[23]

Herudover følger det af bestemmelsen, at medlemsstaterne skal sikre, at elektroniske signaturer, der lever op til EU-reglerne, også opfylder krav i national ret om signatur på digitale meddelelser, hvilket indebærer, at hvis national lovgivning indeholder krav om, at en digital meddelelse skal være forsynet med signatur eller lignende, så skal dette krav anses for opfyldt, hvis der er brugt en "avanceret elektronisk signatur". Et sådant krav kan enten forekomme, hvor der er givet en udtrykkelig regel om, at digital kommunikation kan anvendes på et bestemt retsområde, eller fordi en regel med et generelt formuleret underskriftskrav, som måske oprindeligt var tiltænkt anvendt til brug for papirdokumenter, må forstås således, at dette krav også kan opfyldes ved brug af elektronisk signatur.

Ved kommunikation i den offentlige sektor giver direktivet dog i henhold til artikel 3, stk. 7, mulighed for, at medlemsstaterne kan stille strengere sikkerhedskrav til de elektroniske signaturer, hvis disse krav er objektive, gennemsigtige, rimelige og ikke-diskriminerende.

Direktivet indeholder i artikel 5, stk. 2, et forbud mod at "diskriminere" elektroniske signaturer i relation til retskraft og anerkendelse som bevis, alene fordi signaturen er elektronisk eller ikke lever op til visse sikkerhedskrav.

Dette "diskriminationsforbud" indebærer, at medlemsstaterne ikke må frakende elektroniske signaturer retsvirkning, alene fordi signaturerne er i elektronisk form, men forbuddet betyder derimod ikke, at medlemsstaterne ikke af andre årsager vil kunne behandle en elektronisk signatur anderledes end en håndskreven underskrift. Er en elektronisk signatur f.eks. udvirket ved en teknik, som kun yder en meget begrænset beskyttelse mod forfalskninger mv., vil det således ikke være i strid med "diskriminationsforbudet" at behandle en sådan signatur anderledes end håndskrevne underskrifter.

4.2.2. Kort om direktivets grundlæggende krav til certificeringscentrene

Med henblik på at skabe et marked for elektroniske signaturer af høj kvalitet og med samme sikkerhedsniveau i hele EU, er der i direktivet fastlagt en række krav til udbyderne af kvalificerede certifikater til elektroniske signaturer og tilknyttede tjenester.

Direktivet angiver i bilag II en række grundlæggende krav til certificeringscentrene, herunder bl.a. krav om:

- certificeringscentrets pålidelighed
- hurtig og sikker katalog- og tilbagekaldelsestjeneste
- muligheden for at fastslå dato og tidspunkt for udstedelse eller tilbagekaldelse af certifikater
- kontrollen af identiteten mv. til de personer, der udstedes kvalificerede certifikater til
- personalets kvalifikationer og sagkundskab mv.
- sikkerhedskrav og tekniske krav til systemer og produkter
- foranstaltninger imod forfalskning af certifikater mv.
- certificeringscentrets økonomiske ressourcer
- registrering af relevante oplysninger om de kvalificerede certifikater
- opbevaring eller kopiering af personers signaturgenereringsdata (den private nøgle) mv.
- at en person som indgår aftale med certificeringscentret om kvalificeret certifikat bliver oplyst om de nøjagtige vilkår for anvendelsen af certifikatet mv.

---

[23] Præamblens pkt. 21.

- opbevaringen af certifikater i verificerbar form.

Direktivet forudsætter, at alle certificeringscentre, som udsteder kvalificerede certifikater, opfylder alle de ovennævnte krav.

4.2.3. Certificeringscentrenes erstatningsansvar

Herudover fastlægger direktivet i artikel 6 retningslinjer for certificeringscentrenes erstatningsansvar over for "enhver person, som med rimelighed forlader sig på certifikatet".

Ansvarsreglerne omfatter alene de tilfælde, hvor et certificeringscenter har udstedt et kvalificeret certifikat, eller hvor udbyderen indestår for en anden udbyders kvalificerede certifikat.

Medlemsstaterne skal i henhold til bestemmelsen sørge for at certificeringscentret vil kunne gøres erstatningsansvarlig for tab, der påføres andre som med rimelighed forlader sig på ægtheden af certifikatet, for så vidt angår:

1) korrektheden af alle oplysningerne i certifikatet regnet fra udstedelsesdagen,
2) sikkerhed for, at den i det kvalificerede certifikat identificerede person på udstedelsesdagen var i besiddelse af de signaturgenereringsdata (den private nøgle), der passer til de i certifikatet indeholdte eller omhandlede signaturverificeringsdata (den offentlige nøgle), og
3) sikkerhed for, at signaturgenereringsdataene og signaturverificeringsdataene fungerer komplementært med hinanden i de tilfælde, hvor det er certificeringscentret, der genererer de to systemer.

Det fastsættes i bestemmelsen, at der er tale om et skærpet uagtsomhedsansvar (culpaansvar med omvendt bevisbyrde) for certificeringscentret. Det er således certificeringscentret, der har bevisbyrden for, at der ikke er handlet uagtsomt, men kan det på den anden side bevises, at der ikke fra certificeringscentrets side har været handlet uagtsomt, vil certificeringscentret ikke være erstatningsansvarligt.

Efter artikel 6, stk. 2, skal medlemsstaterne herudover sikre, at certificeringscentre, der udsteder kvalificerede certifikater, kan gøres erstatningsansvarlige for tab, der opstår som følge af manglende registrering af spærring af certifikatet, medmindre certificeringscentret kan bevise, at der ikke er handlet uagtsomt.

Certificeringscentrene kan imidlertid, jf. artikel 6, stk. 3, indsætte begrænsninger i de kvalificerede certifikaters anvendelsesområder, samt, jf. artikel 6, stk. 4, indsætte beløbsbegrænsninger i certifikaterne. Certificeringscentrene vil herved kunne frigøre sig for ansvar i de tilfælde, hvor certifikatet er anvendt i strid med begrænsningerne.

Bestemmelsen omhandler kun certificeringscentrenes ansvar over for en person, der med rimelighed forlader sig på certifikatet, hvilket som udgangspunkt vil sige certifikatindehaveren (underskriveren) og modtageren af den elektroniske signatur. Direktivet indeholder derimod ingen regulering af ansvarsforholdet i det indbyrdes forhold mellem underskriveren og modtageren af den elektroniske signatur.

Medlemsstaterne skal efter artikel 8, stk. 1, sikre, at certificeringstjenesteudbydere samt nationale akkrediterings- og tilsynsorganer opfylder det generelle EF-direktiv 97/46/EF om persondatabeskyttelse. I artikel 8, stk. 2, bestemmes det endvidere, at certificeringscentrene alene må indsamle personoplysninger direkte fra den pågældende person eller med denne persons udtrykkelige samtykke. Personoplysningerne må kun indsamles i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat.

4.2.4. Direktivets bestemmelser om markedsadgangen

Direktivet indeholder i artikel 3, stk. 1, et forbud mod forudgående autorisation af certificeringscentre som betingelse for at kunne udbyde certificeringstjenester til elektroniske signaturer.

Det anføres i bemærkningerne til forslaget til lov om elektroniske signaturer,[24] at der ved forudgående autorisation forstås "*enhver tilladelse, hvis udstedelse forudsætter, at de nationale myndigheder træffer en afgørelse, inden nøglecentret kan udbyde sine certificeringstjenester samt enhver anden foranstaltning med samme virkning*".

Forbudet mod forudgående autorisation skal sikre, at certificeringscentrene får mulighed for at udbyde deres produkter på tværs af grænserne i hele EU, således at den samlede konkurrence på dette specielle område styrkes.

Der indføres dog samtidig en pligt for medlemsstaterne til at etablere et passende tilsyn med certificeringscentre, der udsteder kvalificerede certifikater til elektroniske signaturer, dog således at

[24] Se det fremsatte forslag: Folketingstidende 1999-2000, tillæg A, s. 6398.

medlemsstaterne kan overlade etableringen af sådanne systemer til markedsaktørerne i form af selv-regulering.

4.2.5. Markedsadgangen for certificeringscentre uden for EU og EØS

Efter artikel 7 skal medlemsstaterne anerkende certifikater udstedt af certificeringstjenesteudbydere fra lande uden for EU og EØS på lige fod med certifikater udstedt af certificeringstjenesteudbydere fra EU og EØS, hvis

1) tredjelands-certificeringscentret opfylder direktivets krav og er akkrediteret i forbindelse med en frivillig akkrediteringsordning i et EU-land,
2) hvis et EU-certificeringscenter, der opfylder direktivets krav, indestår for tredjelandsudbyderens certifikater, eller
3) hvis tredjelands-certifikatet eller tredjelands-udbyderen er anerkendt i henhold til en international aftale.

4.2.6. Direktivets gennemførelse mv.

Direktivet om elektroniske signaturer skulle i henhold til direktivets artikel 13 være gennemført i national lovgivning senest den 19. juli 2001. Efter artikel 12 skulle Kommissionen inden 2 år efter denne implementeringsfrist skulle aflægge en rapport om, hvordan direktivet fungerede, herunder tage stilling til om direktivets anvendelsesområde burde ændres under hensyn til den teknologiske, markedsmæssige og retlige udvikling, og rapporten skulle på grundlag af de indhøstede erfaringer navnlig omfatte en bedømmelse af harmoniseringsaspekterne, samt om fornødent ledsages af forslag til retsforskrifter.

I oktober 2003 fremkom en rapport, "The Legal and Market Aspects of Electronic Signatures", som var bestilt af Kommissionen,[25] hvori implementeringen i de forskellige lande blev gennemgået artikel for artikel. Rapporten påpegede i denne forbindelse en række mangler i forbindelse med landenes implementering.

Det anførtes endvidere bl.a. i rapporten, at der ikke var behov for at foretage ændringer i direktivet, idet direktivets tekst – med visse opregnede uhensigtsmæssigheder – måtte anses for at opfyl-

[25] Rapporten er udarbejdet af en forskningsgruppe tilknyttet Katholieke Universiteit Leuven. Rapporten kan findes på http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf.

de sit formål. Herudover fremsattes der en række oplæg til nyfortolkning og afklaring af direktivteksten.

Rapporten indeholdt udover forskergruppens bemærkninger og rekommandationer et antal skemaer, som overordnet gennemgår forhold af relevans for direktivet for de 25 nuværende EU-lande samt for EØS-landene, Bulgarien, Rumænien og Schweiz.

4.3. Lov nr. 417 af 31. maj 2000 om elektroniske signaturer

4.3.1. Almindelige bemærkninger om loven

Lov nr. 417 af 31. maj 2000 om elektroniske signaturer indeholder bestemmelser, der gennemfører direktivet om elektroniske signaturer. Lovens formål er at fremme en sikker og effektiv anvendelse af elektronisk kommunikation gennem fastsættelse af krav til visse elektroniske signaturer og til certificeringscentre, der udsteder certifikater til elektroniske signaturer. [26]

Loven finder alene anvendelse på certificeringscentre etableret i Danmark, der udsteder kvalificerede certifikater som defineret i lovens kap. 3. En virksomhed, der udsteder certifikater, der ikke betegnes som kvalificerede, er ikke underlagt lovens bestemmelser.

Lovens primære sigte er at etablere en tilsyns- og kontrolordning for certificeringscentre, der ønsker at udbyde certifikater med betegnelsen kvalificerede certifikater og i tilknytning hertil at regulere de pågældende certificeringscentres drift og erstatningsansvar over for henholdsvis underskrivere og modtagere af kvalificerede certifikater.

Tilsynet varetages af IT- og Telestyrelsen, hvortil der skal foretages anmeldelse, når udstedelse af kvalificerede certifikater påbegyndes. Det er ikke hensigten med loven at regulere det samlede udbud af certificeringscentre, og certificeringscentrene har således fortsat frihed til at udbyde ikke-kvalificerede certifikater og elektroniske signaturer uden at skulle underlægge sig et omfattende tilsyn eller autorisationsordninger og uden at være tvunget til at benytte bestemte tekniske løsninger. Et eksempel på sådanne ikke-lovregulerede certifikater og elektroniske signaturer er nærmere beskrevet nedenfor i nr. 5.

---

[26] Jf. Folketingstidende 1999-2000, tillæg A, sp. 6346. Der henvises i øvrigt til betænkning 1400/2000.

Der opstilles i loven ligeledes en ramme med en række generelle minimumskrav til de systemer, der anvendes til at generere, opbevare og anvende de nøgler, der danner grundlaget for de elektroniske signaturer. Herved sikres det, at elektroniske signaturer baseret på kvalificerede certifikater har et vist kvalitetsniveau, der kan efterprøves.

4.3.2. Krav til certificeringscentret

Loven opstiller visse krav, som skal sikre, at der skabes et tilstrækkeligt sikkerhedsniveau i relation til udstedelse og administration af de kvalificerede certifikater. Loven opstiller både krav til indholdet af de kvalificerede certifikater og til de procedurer og forretningsgange, som certificeringscentrene skal anvende.

Det følger af lovens § 4, at betegnelsen kvalificerede certifikater eller betegnelser, der er egnede til at fremkalde det indtryk, at der er tale om kvalificerede certifikater, alene må anvendes om certifikater, der opfylder lovens krav. Udover en angivelse af, at certifikatet er udstedt som et kvalificeret certifikat, skal certifikatet bl.a. indeholde underskriverens navn, certifikatets gyldighedsperiode og tydelig angivelse af eventuelle begrænsninger med hensyn til de formål og/eller transaktionsbeløb, certifikatet kan anvendes til, samt opfylde en række mere tekniske krav, jf. lovens § 4, stk. 2 og 3.

Herudover skal certificeringscentret som et helt centralt element i reguleringen overholde visse minimumskrav om, hvordan underskriverens identitet kontrolleres forud for udstedelsen af et kvalificeret certifikat med henblik på at sikre en betryggende identitetskontrol.

Med hjemmel i lovens § 6, stk. 3, har ministeren for videnskab, teknologi og udvikling fastsat regler i en sikkerhedsbekendtgørelse (bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav mv. til certificeringscentre for procedurerne ved identifikationen af underskriveren). Det fremgår af bekendtgørelsens § 6, stk. 2 og 3, at underskriveren skal være fysisk til stede i forbindelse med, at identitetskontrollen foretages, medmindre certificeringscentret på forhånd har kendskab til underskriverens person.

Udover de nævnte krav i forbindelse med udstedelsen og administrationen af kvalificerede certifikater knytter der sig også andre krav til de certificeringscentre, der udsteder kvalificerede certifikater, jf. lovens kapitel 4. Bestemmelserne pålægger bl.a. udbyderne af kvalificerede certifikater løbende at træffe de juridiske, organisatoriske, tekniske, personale- og sikkerhedsmæssige foranstaltninger, som er nødvendige for, at der er tale om et sikkert og velfungerende udbud af elektroniske signaturer.

En af de vigtigste sikkerhedsmæssige foranstaltninger, som certificeringscentret skal opfylde, er etablering af en spærretjeneste (katalog og tilbagekaldstjeneste), der gør det muligt for indehaveren at spærre sit certifikat. Hertil kommer, at information om spærrede certifikater (spærrelister) skal være offentligt tilgængelig, f.eks. på Internettet, således at en modtager af et dokument med en elektronisk signatur kan gøre sig bekendt med status - altså hvorvidt certifikatet er spærret – for det tilhørende certifikat, jf. lovens § 9.

Endvidere skal certificeringscentrene til stadighed have tilstrækkelige økonomiske ressourcer til at kunne efterleve kravene i loven og herunder leve op til det økonomiske erstatningsansvar i medfør af lovens særlige ansvarsregulering, jf. § 11.

4.3.3. Begrænsninger i certifikatets anvendelsesområde

Et kvalificeret certifikat skal ifølge lovens § 4, stk. 2, nr. 5–7, indeholde oplysninger om eventuelle begrænsninger i certifikatets anvendelsesmuligheder. Begrænsningerne kan vedrøre certifikatets gyldighedsperiode, anvendelsesområde og transaktionens størrelse. Begrænsninger i anvendelsesområdet eller i beløbsstørrelsen kan indsættes af certificeringscentret eller på certifikatindehaverens begæring.

I praksis vil oplysningerne være anført i det elektroniske certifikat, som medsendes den pågældende meddelelse. Ved hjælp af kommandoer til det elektroniske postsystem vil modtageren af den signerede meddelelse kunne få adgang til certifikatet og herved kendskab til en række relevante oplysninger, herunder certifikatets gyldighedsperiode og evt. formåls- og beløbsbegrænsninger.

Tidsmæssig begrænsning (gyldighedsperiode)

Det følger af lovens § 4, stk. 2, nr. 5, at et kvalificeret certifikat skal indeholde oplysninger om certifikatets gyldighedsperiode. I lovforslagets bemærkninger til bestemmelsen er det anført, at bestemmelsen tager højde for det særlige forhold, at en elektronisk signatur frembragt på en meddelelse forældes, efterhånden som den teknik, der giver mulighed for at bryde de anvendte koder, bliver hurtigere og bedre.

Det er desuden anført i bemærkningerne til lovforslaget, at brugerne ved anvendelse af elektroniske signaturer nøje bør overveje, hvordan digitale dokumenter opbevares. Dokumenter, der kan få betydning ud over udløbsperioden for de involverede signaturer, bør ifølge bemærkningerne

opbevares med omtanke, og det bør overvejes, om en given type af meddelelser egner sig til at blive kommunikeret elektronisk.

Beløbsmæssig begrænsning og formålsbegrænsning i certifikatet

Ifølge lovens § 4, stk. 2, nr. 6, skal der i certifikatet være en tydelig angivelse af eventuelle begrænsninger i certifikatets anvendelsesområde (formålsbegrænsninger). Det vil således være muligt at angive, at certifikatet alene er beregnet til at anvendes til kommunikation med visse typer af virksomheder, eksempelvis pengeinstitutter eller forsikringsselskaber.

På tilsvarende måde er det også muligt i certifikatet at angive eventuelle begrænsninger for størrelsen af den transaktion eller betaling, som certifikatet er beregnet til at anvendes til (beløbsbegrænsninger), jf. lovens § 4, stk. 2, nr. 7. Beløbsbegrænsningen kan angives i danske kroner eller evt. i udenlandsk valuta.

Oplysningerne om eventuelle begrænsninger i certifikatet skal gives skriftligt af certificeringscentret ved indgåelse af aftale om udstedelse af et kvalificeret certifikat, jf. lovens § 8.

Indsættelse af anvendelsesbegrænsninger synes ikke at være udbredt på det danske certifikatmarked, hvilket kan hænge sammen med, at certificeringscentrene i øjeblikket teknologisk har vanskeligt ved at indsætte begrænsninger i mindre serier af certifikater og således ikke kan tilbyde kundespecifikke certifikater.

4.3.4. Erstatningsansvar for udbydere af kvalificerede certifikater

Udover de særlige krav, der stilles til kvalificerede certifikater i forbindelse med udstedelsen og den løbende administration, gælder der særlige erstatningsretlige regler for udbydere af kvalificerede certifikater, jf. lovens § 11. Reglerne er beskyttelsespræceptive og kan således ikke ved forudgående aftale fraviges til skade for skadelidte, jf. § 11, stk. 4.

Ansvarsgrundlaget

Det følger af lovens § 11, stk. 2, at i de tilfælde, hvor lovens § 11, stk. 1, er opfyldt, er certificeringscentret erstatningsansvarligt, medmindre certificeringscentret kan godtgøre, at certificeringscentret ikke har handlet forsætligt eller uagtsomt. Der påhviler således certificeringscentret et skærpet culpaansvar (culpaansvar med omvendt bevisbyrde). Ifølge lovforslagets bemærkninger til bestemmelsen er begrundelsen herfor områdets meget tekniske og komplicerede karakter. Det

vil for den almindelige bruger af elektroniske signaturer uden særlig kendskab til teknologien være vanskeligt at påvise, at certificeringscentret har begået fejl eller forsømmelser, der kan bedømmes som værende culpøse.

Certificeringscentrets erstatningsansvar forudsætter herudover, at de øvrige betingelser efter de almindelige regler om erstatningsansvar er opfyldt.

Ved siden af lovens skærpede erstatningsregel gælder fortsat dansk rets almindelige erstatningsregel om culpaansvar, og forhold uden for anvendelsesområdet for lovens særlige erstatningsregel skal således bedømmes efter dansk rets almindelige regler herom.

Hvilke tab er omfattet?

Det fremgår af lovens § 11, stk. 1, at certificeringscentre, der udsteder kvalificerede certifikater til offentligheden, eller som over for offentligheden indestår for sådanne certifikater udstedt af et andet certificeringscenter, er ansvarlige for tab hos den, der med rimelighed forlader sig på certifikatet.

Tabet skal skyldes en af de i § 11, stk. 1, nr. 1 – 5, opregnede årsager. Certificeringscentret vil således bl.a. kunne pådrage sig erstatningsansvar for tab, der skyldes, at oplysningerne i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet, at certifikatet ikke indeholder alle de oplysninger, som kræves efter lovens § 4, eller hvis tabet skyldes manglende eller fejlagtig information om, at certifikatet er spærret, om, hvilken udløbsdato certifikatet har, eller om, hvorvidt certifikatet indeholder formåls- eller beløbsbegrænsninger.

Ifølge bemærkningerne i lovforslaget til bestemmelsen kan certificeringscentret pådrage sig ansvaret over for både modtageren og underskriveren af en elektronisk signatur med et kvalificeret certifikat, ligesom certificeringscentret også vil kunne pådrage sig et erstatningsansvar for tab hos tredjemand, der skyldes certificeringscentrets uagtsomhed. Bestemmelsen vedrører derimod ikke forholdet mellem afsender og modtager af et kvalificeret certifikat, og et eventuelt erstatningsansvar i dette forhold skal bedømmes efter dansk rets almindelige bestemmelser om erstatningsansvar.

Fritagelse for ansvar

Lovens § 11, stk. 3, fritager certificeringscentret for ansvar for tab i visse situationer. Certificeringscentret er således som udgangspunkt ikke erstatningsansvarligt for et tab, der er opstået som

følge af, at certifikatet er anvendt uden for de formålsbegrænsninger, som gælder for certifikatet, eller for et tab, der er opstået som følge af en overskridelse af de beløbsbegrænsninger, der gælder for certifikatet. Fritagelsen for erstatningsansvar i de nævnte situationer forudsætter imidlertid, at begrænsningerne tydeligt fremgår af certifikatet, og at de på forespørgsel oplyses af certificeringscentret, jf. lovens § 11, stk. 3, sidste led.

Kapitel 5

Signaturløsninger i praksis

5.1. Indledning

Som nærmere omtalt i nr. 4.3 regulerer lov om elektroniske signaturer (alene) anvendelsen af elektroniske signaturer, som er baseret på kvalificerede certifikater. Hovedparten af de digitale identifikationstyper, som anvendes i dag, er imidlertid ikke omfattet af denne lov, og retsvirkningerne af brugen heraf må derfor i det hele udledes af de involverede parters aftale og af almindelige aftaleretlige og erstatningsretlige principper.

I dette kapitel foretages en gennemgang af en række digitale identifikationstyper, som bruges i Danmark. Det har ikke været muligt – eller for den sags skyld ønskeligt – at medtage alle digitale signaturlignende identifikationstyper, der findes på markedet, men med henblik på at give et generelt overblik over, hvilke forskellige muligheder der i dag findes for at kunne identificere sig digitalt, indeholder kapitlet en beskrivelse eller omtale af en række af de mest udbredte digitale identifikationstyper.

Indledningsvis foretages en gennemgang af den digitale signatur, som er baseret på "standard for offentlige certifikater til elektronisk service" (i det følgende: OCES-standarden), som er udarbejdet af Ministeriet for Videnskab, Teknologi og Udvikling.

OCES-signaturen er væsentligt mere indgående behandlet end de andre digitale identifikationstyper. Heri ligger imidlertid ikke nogen tilkendegivelse af, at OCES-signaturen er mere anvendelig eller for den sags skyld mere udbredt end de øvrige nævnte identifikationsløsninger. At beskrivelsen af OCES-signaturen er givet større vægt ved udvalgets beskrivelse skal ses i sammenhæng med, at udvalgets primære opgave efter kommissoriet er at behandle spørgsmål om digitale signaturer, som er baseret på public key-kryptering.

OCES-signaturen er et godt eksempel på en sådan digital signatur, som er baseret på public key-kryptering. De principper, som gælder for OCES-signaturer, gælder i vid udstrækning også for andre public key baserede identifikationstyper. Andre ulovregulerede digitale signaturer vil dog på flere måder være administreret anderledes, end hvad der her anføres om OCES-signaturer.

Ud over gennemgangen af OCES-signaturen omtales ID-løsninger som bankernes net-ID, Netbank og Pinkodeløsningen samt tjenester, som gør brug heraf, herunder ToldSkats tast-selv service og forskellige andre tjenester, som udbydes på Internettet.

5.2. OCES-signaturen

Som nævnt kan et eksempel på en digital identifikationstype, der ikke er reguleret af særlig lovgivning, findes i den digitale signatur, der er baseret på Ministeriet for Videnskab, Teknologi og Udviklings standard for offentlige certifikater til elektronisk service (OCES-standarden). Denne digitale signatur (OCES-signaturen) har siden foråret 2003 kunnet anvendes til signering af elektronisk post og til identifikation ved brug af offentlige og private elektroniske serviceydelser.

Den væsentligste forskel på OCES-certifikater og kvalificerede certifikater udstedt efter lov om elektroniske signaturer er, i hvilket omfang udstedelsesproceduren sikrer kendskab til ansøgerens identitet. Udstedelse af et kvalificeret certifikat kræver som hovedregel personligt fremmøde, hvilket betyder, at certifikatansøgeren skal møde personligt op hos certificeringscentret (eller en tilknyttet registreringsenhed) og her på passende vis dokumentere sin identitet. Udstedelsesproceduren for OCES-certifikater stiller ikke krav om personligt fremmøde, men verifikationen af ansøgerens identitet baseres derimod som udgangspunkt på fremsendelse af et PIN-kodebrev til certifikatansøgerens postadresse . Se nærmere om udstedelsesproceduren under nr. 5.2.2.

En anden væsentlig forskel er som tidligere nævnt, at certificeringscentre, der udsteder kvalificerede certifikater, er omfattet af lov om elektroniske signaturer, der bl.a. fastsætter certificeringscentrets erstatningsansvar over for brugerne af kvalificerede certifikater, mens et certificeringscenter, der udsteder OCES-certifikater, ikke er omfattet af loven, men derimod er forpligtet i medfør af OCES-certifikatpolitikkerne og certificeringscentrets aftale med IT- og Telestyrelsen.

5.2.1. Certifikatpolitikkerne og deres retlige status

For bl.a. at fastlægge et tilfredsstillende og ensartet sikkerhedsniveau for OCES-signaturen er de retningslinjer, der gælder for udstedelsen af et OCES-certifikat, nærmere beskrevet i en certifikatpolitik for OCES-certifikater.[27]

[27] Se nedenfor i nr. 5.2.6.

En certifikatpolitik kan betegnes som en offentlig meddelelse af de teknologiske og sikkerhedsmæssige rammer, som et certificeringscenter udbyder i forbindelse med udstedelsen af elektroniske certifikater.

En certifikatpolitik indeholder en overordnet beskrivelse af grundlaget for certifikaterne, ligesom beskrivelser af tekniske standarder og systemer, udstedelsesprocedurer og sikkerhedsforanstaltninger, herunder brugerens adgang til en spærreliste, typisk vil fremgå af certifikatpolitikken. Certifikatpolitikken vil herudover f.eks. kunne indeholde beskrivelser af det aftaleretlige grundlag for udstedelsen og anvendelsen af certifikaterne.

Formålet med OCES-certifikatpolitikkerne er således bl.a. at angive nogle minimumskrav til systemer og aftaler, som certificeringscentre skal opfylde i forhold til brugerne af certifikaterne, for herved at sikre, at anvendelse af certifikater kan ske på betryggende vis.

Ministeriet for Videnskab, Teknologi og Udvikling har offentliggjort tre OCES certifikatpolitikker, som beskriver rammerne for udstedelsen af OCES-certifikater.[28] De tre certifikatpolitikker, der omhandler henholdsvis certifikater til medarbejdere, virksomheder og personer, har samme opbygning og indeholder i vid udstrækning ensartede beskrivelser af de forskellige tekniske og sikkerhedsmæssige standarder, som de certificeringscentre, der ønsker at udbyde OCES-certifikater, skal opfylde.[29]

Grundlaget for certifikater efter OCES-standarden er på denne måde ensartet fastsat for alle certificeringscentre, der ønsker at udstede OCES-certifikater.

OCES-certifikatpolitikkerne er udarbejdet af IT- og Telestyrelsen under Ministeriet for Videnskab, Teknologi og Udvikling. For at opnå ret til at udstede OCES-certifikater skal de enkelte certificeringscentre indgå aftale med IT- og Telestyrelsen. I aftalen forpligter certificeringscentret sig til at overholde certifikatpolitikkerne.

Certifikatpolitikkerne har ikke status som lov, bekendtgørelse eller anden retsforskrift, men må anses som et sæt aftalevilkår mellem IT- og Telestyrelsen og det enkelte certifikatudstedende certificeringscenter. Som det er beskrevet ovenfor, vedrører de fleste bestemmelser de krav, som certificeringscentret skal opfylde for at have ret til at udstede OCES-certifikater. Certifikatpolitik-

---

[28] Certifikatpolitikkerne administreres af IT- og Telestyrelsen og er tilgængelige på: www.signatursekretariatet.dk. Som et eksempel på en certifikatpolitik er OCES-personcertifikatpolitik optrykt som bilag 3 til denne betænkning.

[29] Certifikaterne har dog af naturlige årsager bl.a. et forskelligt anvendelsesområde og forskellig registrering af certifikatholder.

kernes bestemmelser om forpligtelser og ansvar vil dog også have en afledet virkning for visse tredjemænd, idet bestemmelserne bl.a. angiver, hvilke vilkår certificeringscentret kan og skal medtage i sine aftaler med (kommende) brugere af certifikaterne.

F.eks. pålægges certifikatudstederen at give information til certifikatindehaveren om dennes forpligtelser i forbindelse med håndteringen af certifikater. Certifikatindehaveren skal herunder bl.a. informeres om pligten til at kontrollere et udstedt certifikat samt til at opbevare adgangskoder fortroligt.

5.2.2. Udstedelse af OCES-certifikater og installering af OCES-signaturer

For at opnå godkendelse til at udstede OCES-certifikater skal certificeringscentret indgå en aftale med IT- og Telestyrelsen, hvori centret forpligter sig til at overholde certifikatpolitikken. Herudover skal certificeringscentret udarbejde en erklæring i form af en såkaldt "certificeringspraksis" (CPS), der detaljeret beskriver, hvorledes certificeringscentret opfylder de enkelte krav i certifikatpolitikken. Certificeringspraksissen skal godkendes af IT- og Telestyrelsen, inden certificeringscentret må udstede OCES-certifikater.

OCES-certifikater kan udstedes som personcertifikater, medarbejdercertifikater eller virksomhedscertifikater.

Formålet med et personcertifikat er, at en afsender af en digital meddelelse over for en modtager skal kunne dokumentere sin identitet, mens formålet med et medarbejdercertifikat - ud over at kunne dokumentere afsenderens identitet - er, at den pågældende afsender skal kunne dokumentere et tilhørsforhold til en bestemt "arbejdsplads".

Endelig angiver et virksomhedscertifikat, at den digitale signatur stammer fra en bestemt virksomhed eller organisation, og har således til formål at kæde en afsender af en elektronisk meddelelse sammen med den pågældende virksomhed eller organisation, uden dog at angive hvem personen er, eller hvilken tilknytning vedkommende i øvrigt har til virksomheden eller organisationen.

Rent praktisk udstedes et OCES-certifikat ved, at ansøgeren – person, virksomhed eller organisation mv. – over Internettet anmoder et (godkendt) certificeringscenter om at udstede et certifikat

med et tilhørende nøglesæt.[30] I denne forbindelse skal ansøgeren oplyse postnummer og CPR-nummer/CVR-nummer.

Ansøgerens oplysninger "trækkes" herefter i CPR/CVR (Det Centrale Person Register/Det Centrale Virksomhedsregister), dvs. at det kontrolleres, om personens eller virksomhedens navn og adresse stemmer overens med det oplyste personnummer eller virksomhedsnummer. Efterfølgende fremsender certificeringscentret en engangskode i et PIN-brev til ansøgerens bopælsadresse eller virksomhedens postadresse som angivet i det pågældende register. Der sendes herudover en e-mail til den e-mailadresse, som brugeren oplyser, og aktiveringen af certifikatet kræver, at brugeren har adgang til både PIN-kodebrevet og e-mailen.

Certifikatet og nøglesættet installeres på brugerens computer og vil herefter fungere sammen med brugerens e-mailsystem og Internetbrowser. Adgangen til at afgive en digital signatur beskyttes af en aktiveringskode, som brugeren vælger i forbindelse med installationen.[31]

Forud for udstedelsen af certifikatet indgås en aftale mellem (den kommende) certifikatindehaver og certificeringscentret, der overordnet regulerer parternes indbyrdes forpligtelser og rettigheder. Det bemærkes i den forbindelse, at det er forudsat i OCES-certifikatpolitikkerne, at bl.a. de rettigheder, der tilskrives certifikatindehaveren i medfør af certifikatpolitikkerne, skal indgå i aftalen.

5.2.3. Oplysninger i OCES-certifikatet

Modtageren af et digitalt signeret dokument vil i det medfølgende tilknyttede certifikat kunne læse en række oplysninger om afsenderen samt evt. visse begrænsninger, der måtte gælde for certifikatet. Når dokumentet eller meddelelsen er modtaget, vil modtageren ved hjælp af nogle kommandoer have mulighed for at kalde certifikatet frem, således at oplysningerne kan læses.

---

[30] Sammenhængen mellem certifikatet og nøglesættet – samt en forklaring af disse begreber – er gennemgået i nr. 3.3.

[31] Systemet stiller en række kvalitetskrav til angivelse af aktiveringskoden, f.eks. i form af et minimum antal karakterer samt kombination af tal og bogstaver.

I certifikatpolitikkerne er det nærmere beskrevet, hvilke oplysninger der skal angives i et OCES-certifikat. For alle certifikattyper er det f.eks. obligatorisk, at certifikatet bl.a. skal indeholde oplysninger om det udstedende certificeringscenter, certifikatindehaverens eller – ved medarbejdercertifikater – certifikatholderens navn eller pseudonym, certifikatets ikrafttrædelses- og udløbsdato samt eventuelle begrænsninger.

5.2.4. Etablering af spærrelister

For at minimere risikoen for andres uberettigede brug af den digitale signatur, skal certificeringscentret dels etablere en spærretjeneste, som gør det muligt for bl.a. certifikatindehaveren eller – ved medarbejdercertifikater – certifikatholderen at spærre sit certifikat, dels offentliggøre en spærreliste på Internettet til brug for kontrol af gyldigheden af et modtaget certifikat.

Ifølge certifikatpolitikkerne skal certificeringscentret senest ét minut efter spærringen offentliggøre en ajourført spærreliste og fremsende kvitteringen for spærringen til den e-postadresse, der er angivet i certifikatet.

Oplysninger om og registrering af bl.a. spærringer skal ifølge certifikatpolitikkerne opbevares i mindst 6 år, og parterne vil således kunne fremskaffe dokumentation for et certifikats status på et givet tidspunkt inden for i hvert fald denne periode.

5.2.5. Fornyelse af OCES-certifikater

Et OCES-certifikat skal bl.a. indeholde oplysninger om certifikatets ikrafttrædelses- og udløbsdato (gyldighedsperiode).

Det fremgår af certifikatpolitikkerne, at certificeringscentret senest 14 dage før udløbsdatoen skal fremsende meddelelse herom til certifikatindehaveren ved e-mail eller traditionel brevpost.

Ved fornyelse udstedes et nyt certifikat med et nyt certifikatnummer og ny gyldighedsperiode. Fornyelse af certifikatet forudsætter, at certifikatet ikke er spærret.

5.2.6. Pligter og ansvar ifølge certifikatpolitikkerne

Certifikatpolitikkerne indeholder en nærmere beskrivelse af pligter og ansvar for certificeringscentre, certifikatindehavere og signaturmodtagere ved udstedelse og anvendelse af OCES-certifikater.

Certificeringscentret har en række forpligtelser, som skal overholdes ved udstedelsen og anvendelsen af OCES-certifikater. Certificeringscentret skal således bl.a. anvise, hvordan nøgler genereres og opbevares, foretage spærring af certifikaterne efter anmodning fra certifikatindehaveren eller certifikatholderen, offentliggøre spærrelister og underrette certifikatindehavere eller certifikatholderen om snarligt udløb af certifikatets gyldighedsperiode mv.

Herudover skal certificeringscentret sikre, at certifikatindehaveren eller certifikatholderen er opmærksom på retningslinjerne for opbevaring af nøgleparret og for afgivelse af fyldestgørende og korrekte svar på alle anmodninger fra certificeringscentret, samt om pligten til straks at spærre certifikatet ved mistanke om, at den private nøgle er blevet kompromitteret.

Disse pligter vil indgå som en del af den aftale, certificeringscentret indgår med den (kommende) certifikatindehaver, og den pågældende vil således kunne gøre sig bekendt med forpligtelserne. Certificeringscentrets manglende overholdelse af sine pligter, vil derimod ifølge aftalen med IT- og Telestyrelsen kunne medføre en ophævelse af aftalen og dermed en fratagelse af retten til at udstede OCES-certifikater.

I certifikatpolitikkerne er det endvidere anført, at certificeringscentret via sin hjemmeside skal gøre det muligt for modtagere af digitale signaturer (signaturmodtagere) at gøre sig bekendt med vilkår og betingelser for anvendelse af digital signatur.

5.2.7. Certificeringscentrets erstatningsansvar

Certifikatpolitikkerne indeholder desuden en nærmere beskrivelse af certificeringscentrets erstatningsansvar, særligt i forhold til certifikatindehavere og signaturmodtagere.

Certificeringscentret er erstatningsansvarligt efter dansk rets almindelige regler.

Herudover anføres det i certifikatpolitikkerne, at certificeringscentret er erstatningsansvarligt for tab hos certifikatindehavere og (direkte) signaturmodtagere, der med rimelighed forlader sig på certifikatet, hvis tabet skyldes et af følgende forhold:

- at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet,
- at certifikatet ikke indeholder alle oplysninger, som er krævet i henhold til certifikatpolitikken,
- certificeringscentrets manglende spærring af certifikatet i henhold til certifikatpolitikkens regler herom,
- manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger,
- tilsidesættelse af udstedelsesproceduren.

Ansvaret for certificeringscentret er et præsumptionsansvar, dvs. et culpaansvar med omvendt bevisbyrde. Certificeringscentret er således ikke ansvarligt for disse forhold, hvis centret kan godtgøre, at det ikke har handlet uagtsomt eller forsætligt. Certificeringscentrets ansvar svarer på den måde i visse henseender til det ansvar, der gælder for certificeringscentre, som udsteder kvalificerede certifikater efter lov om elektroniske signaturer, jf. lovens § 11. Dog kan certificeringscentret ikke begrænse sit ansvar over for private.

Certificeringscentret skal desuden tegne og opretholde en forsikring til dækning af eventuelle erstatningskrav fra såvel visse medkontrahenter (certifikatindehavere og signaturmodtagere) som IT- og Telestyrelsen. Forsikringen skal som minimum have en dækning på 2 millioner kr. årligt.

5.3. Andre identifikationstyper

Ved siden af OCES har andre typer af identifikationsteknologier opnået stor udbredelse, herunder netbank-signaturløsningerne, bankernes net-ID og pinkoder.

5.3.1. Netbank

De danske pengeinstitutter har opnået en stor udbredelse af de elektroniske netbankløsninger, kaldet homebanking. Det skønnes, at der i dag er knap 2 millioner netbankkunder i Danmark. Netbankløsningerne baseres i vidt omfang på en teknologi, der minder om digital signatur, og giver brugeren mulighed for at identificere sig over for banken mv. på et lige så højt sikkerhedsniveau som ved brug af en OCES-signatur.

5.3.2. Bankernes net-ID

Efter den 1. juni 2004 har mange pengeinstitutter med netbank tilbudt deres kunder at benytte net-ID. Net-ID bygger på det sikkerhedssystem, der ligger til grund for netbankerne, og er en måde, hvorpå netbankbrugere kan identificere sig elektronisk over for en virksomhed på Internettet.

For at blive tilmeldt net-ID skal netbankbrugeren indgå en aftale med sit pengeinstitut. Tilmeldingen foregår i netbanken, enten ved at brugeren tilmelder sig direkte i netbanken eller i forbindelse med, at netbankbrugeren logger sig på hos en virksomhed første gang. Virksomheden dirigerer automatisk brugeren til netbanken.

Virksomheder, som tilbyder services mv. på Internettet, skal indgå aftale med PBS om brug af net-ID.[32]

5.3.3. Pinkoder

En lang række offentlige myndigheder og private virksomheder benytter pinkoder til identifikation af borgere, der ønsker at kommunikere elektronisk via en hjemmeside. Pinkoden sendes typisk med almindelig post til brugerens postadresse, hvorefter brugeren kan identificere sig via Internettet.

En af de mest udbredte pinkodeløsninger er Den Fælles Pinkode, der er et resultat af et samarbejde mellem forskellige serviceudbydere på Internettet. Den Fælles Pinkode udstedes af KMD og kan benyttes både hos offentlige og private serviceudbydere, herunder størstedelen af de danske kommuner.

---

[32] Flere oplysninger om bankernes net-ID kan findes på: www.pbs.dk/it-services/net-id.

Pinkodeløsninger har dog – ligesom netbankløsninger – den anvendelsesmæssige begrænsning, at de alene kan bruges til identifikation på hjemmesider. Løsningerne er således begrænsede til såkaldt log-on og kan ikke benyttes til digital signatur og sikker e-mail kommunikation.

5.4. Digitale tjenester

De ovenfor i nr. 5.3 omtalte identifikationstyper kan betegnes som log-on løsninger, idet der er tale om midler til brug for identifikation af indehaveren på hjemmesider. Løsningerne kan derimod ikke benyttes til digital signatur eller sikker e-mailkommunikation.

Sideløbende med den stigende anvendelse af elektronisk kommunikation baseret på e-mail udbygges de offentlige elektroniske selvbetjeningsydelser, således at disse kan benyttes sammen med digital signatur eller andre identifikationstyper. F.eks. har KMD's Netborgerløsning, der udgør grundlaget for elektronisk selvbetjening i de fleste kommuner i Danmark, således fra efteråret 2003 tilbudt identifikation ved brug af digital signatur baseret på OCES-standarden.

En række andre offentlige myndigheder og private virksomheder og organisationer har siden efteråret 2003 tilbudt deres kunder elektronisk selvbetjening baseret på certifikater til digital signatur.

Størstedelen af de nuværende tjenester, der tilbyder digital signatur til identifikation, benytter digital signatur som et supplement til en traditionel identifikationsmetode, der typisk baseres på pinkoder (f.eks. KMD's NetBorger, der ligeledes benytter Den Fælles Pinkode). Da sikkerhedsniveauet for OCES-certifikater vurderes højere end de mest udbredte pinkodeløsninger, kan der med identifikation ved brug af denne type certifikater tilbydes flere former for avancerede selvbetjeningsløsninger. Denne type selvbetjeningsløsninger er dog endnu ikke udbredt, men der må forventes en øget udbredelse heraf inden for den nærmeste fremtid i takt med, at udbredelsen af certifikater hos borgere og virksomheder stiger.

Eksempler på tjenester, hvor identifikationsløsninger kan bruges

ATP
På ATP's portal er det muligt for private personer at få adgang til egne oplysninger. Identifikationen kan foretages med en digital signatur eller med en pinkode. For arbejdsgivere mv. er der herudover adgang til forskellige tjenester. Adgangen for arbejdsgiverne mv. bygger på pinkodeløsningen.

E-boks
E-boks er en gratis postboks, hvor en borger elektronisk kan modtage og opbevare kontoudtog, oversigter, lønsedler osv. E-boks kan også anvendes til opbevaring af personlige dokumenter, f.eks. en dåbsattest. E-Boks er tilknyttet CPR-nummeret.[33]

PensionsInfo
PensionsInfo er en forening af pensionskasser, livsforsikringsselskaber, pengeinstitutter og lovbaserede pensionsordninger, som siden 1999 har drevet hjemmesiden www.pensionsinfo.dk. Foreningens formål er via Internettet at formidle et overblik over pensionsordninger. PensionsInfo anvendte fra begyndelsen en pinkodeløsning, som forventes udfaset i løbet af 1 års tid. Siden foråret 2004 har der været adgang til PensionsInfo med OCES-signaturen. Det forventes endvidere, at der i begyndelsen af 2005 åbnes for adgang til PensionsInfo med Net-ID.

Sygeforsikringen "danmark"
Sygeforsikringen "danmark" tilbyder sine kunder at kunne servicere sig selv via "danmarks" hjemmeside. Her kan kunderne bl.a. få overblik over kontooplysninger, beregne støttebeløb og få udbetalt tilgodehavender. Identifikation kan ske såvel med en pinkode som med OCES-signatur og Net-ID.

ToldSkat
ToldSkat har fra foråret 2003 udvidet sin tast selv service på Internettet til også at omfatte identifikation med digital signatur. Fra hjemmesiden er det bl.a. muligt at foretage ændringer i selvangivelse og forskudsopgørelse samt at angive kontonummer til overskydende skat samt børnefamilieydelse/tilskud mv.

ToldSkat har igennem en årrække via egen pinkodebaserede identifikationsløsning tilbudt skatteborgerne at ændre og indberette selvangivelse via ToldSkat's hjemmeside. Ca. 800.000 danskere benyttede sig af denne mulighed i 2003.

Virk.dk
Via erhvervsportalen Virk.dk, der er et samarbejde mellem Staten og Krak, kan alle danske virksomheder elektronisk foretage administrativ kommunikation med det offentlige. Virk.dk tilbyder bl.a. adgang til ca. 1200 blanketter. Identifikationen af brugerne på Virk.dk baseres udelukkende på digital signatur.

WebReg
På Erhvervs- og Selskabsstyrelsens portal, WebReg, er det muligt med en digital signatur at registrere stiftelse af selskaber og ændring af virksomheder.

[33] Kilde: www.e-boks.dk.

Kapitel 6

Nordiske forhold

6.1. Indledning

I kapitel 3 i betænkning nr. 1400/2000 om e-signatur og formkrav i lovgivningen gennemgik udvalget den internationale udvikling i digital kommunikation. Kapitlet indeholdt bl.a. en beskrivelse af direktivet om elektroniske signaturer.

Siden betænkning 1400/2000 har alle nordiske lande gennemført direktivet om elektroniske signaturer, og den nordiske lovgivning vedrørende digitale signaturer, er således stort set ensartet.

Der er imidlertid en lang række tilknyttede emner, som også har relevans for digitale signaturer, og udvalget har på denne baggrund fundet, at der har været behov for at undersøge, hvordan de øvrige nordiske lande har tilpasset sig udviklingen på IT-området.

Der er med det følgende alene tilsigtet en generel oversigt over de IT-tiltag, som har været i Norden siden afgivelsen af udvalgets seneste betænkning, og som har relation til digital signatur. Udvalget har foretaget henvisninger til Internetadresser, hvor der vil kunne indhentes yderligere oplysninger om de andre nordiske landes forhold.

6.2. Finsk ret

På nationalt plan har det nyetablerede råd, Rådet för Informationssamhället, det overordnede ansvar for IT-udviklingen. Rådet, som ledes af statsministeren og består af repræsentanter fra den offentlige og den private sektor, blev nedsat ved Statsrådets beslutning den 4. september 2003 og virker i en tidsbegrænset periode indtil udgangen af statsminister Matti Vanhanens regeringsperiode.

Rådets opgaver er navnlig at følge informationsområdet på nationalt og internationalt plan og at støtte udviklingen af informationssamfundet til gavn for erhvervslivet og den offentlige sektor.[34]

---

[34] Rådets opgaver mv. kan ses på følgende Internet-adresse:
www.valtioneuvosto.fi/vn/liston/base.lsp?r=41389&k=sv.

6.2.1. Myndigheder mv.

I Finland er ansvaret for IT-området delt ud på de forskellige fagministerier. Der er dog også visse generelle opgaver, der specifikt hører ind under specifikke fagministerier.

Finansministeriet har således ansvaret for den offentlige forvaltnings udvikling generelt og kan i denne forbindelse udstikke retningslinjer på bl.a. IT-området. Det bemærkes dog, at der er en stor frihed for de øvrige fagministerier til at indføre egne løsninger, dersom Finansministeriets generelle direktiver findes uhensigtsmæssige for den pågældende myndighed.

Indenrigsministeriet, som er overmyndighed for Statens certificeringsmyndighed (Befolkningsregistercentralen (VRK)), administrerer området for elektroniske identiteter og signaturer mv.

Justitsministeriet er ansvarligt for udviklingen af retsvæsenet, herunder også spørgsmål om IT.

Kommunikationsministeriet har ansvaret for den fysiske infrastruktur. Kommunikationsministeriet er overmyndighed for Kommunikationsverket, der er tilsynsmyndighed inden for elektronisk kommunikation og informationssamfundets tjenester.

6.2.2. Lovgivningen

Finsk ret er – som den øvrige nordiske ret – baseret på princippet om aftalefrihed, herunder også fri bevisvurdering og formløshed ved aftaleindgåelse mv. Således vil enhver form for digital signatur kunne have en juridisk bevisværdi. I de tilfælde, hvor finsk lovgivning måtte opstille et formkrav om, at der kræves en egenhændig underskrift, kan en kvalificeret digital signatur anvendes i stedet for en underskrift.[35]

Finland gennemførte direktivet om elektroniske signaturer ved lag om elektroniska signaturer af 24. januar 2003 (14/2003).[36]

Loven indeholder – ud over implementeringen af direktivet – bestemmelser, som stiller krav til indehaveren af den digitale signatur, herunder § 13 som fastsætter krav om spærring (tilbagekal-

[35] Jf. Digitala Signaturer i Norden, Promemoria af 24. november 2003, Nordisk Ministerråd, side 16.
[36] Se loven (i svensk udgave): www.finlex.fi/linkit/fs/20030014.

delse) af certifikatet i tilfælde af, at indehaveren har grund til at antage, at signaturen anvendes uberettiget.

Desuden fastsætter loven i § 17 erstatningsansvar for en signaturindehaver, hvis signaturen anvendes uberettiget, og indehaveren ikke forinden har spærret certifikatet. Hvad angår tilfælde, hvor en forbruger er certifikatindehaver, gælder det dog, at ansvaret kun pålægges forbrugeren, hvis denne bevidst eller uagtsomt har overladt sin private nøgle til andre eller har undladt at tilbagekalde certifikatet, hvis der er mistanke om, at sikkerheden er blevet kompromitteret.

Af andre retsforskrifter på området kan nævnes, at Kommunikationsverket, som er den myndighed, der overvåger lovens overholdelse mv., med hjemmel i lovens § 9 har udstedt forskrift nr. 7/2003 M af 29. januar 2003 med tilhørende rekommandation om pligt for udstedere af kvalificerede certifikater til at anmelde sin virksomhed til Kommunikationsverket (föreskrift om skyldighet för certifikatudfärdere som tilkandahåller allmänheten kvalificerade certifikat att göra anmälan om sin verksamhet till kommunikationsverket).[37]

Herudover har Kommunikationsverket udstedt forskrift nr. 8 af 29. januar 2003 om krav om pålidelighed og informationssikkerhed for certifikatudstedere, som udsteder kvalificerede certifikater til offentligheden (föreskrift om krav på tillförlitlighet och informationssäkerhet i verksamhet av certifikatutfärdare som tillhandahåller allmänheten kvalificerade certifikat).[38]

Endelig kan der henvises til Lag nr. 13 af 24. januar 2003 om elektronisk kommunikation i myndigheternas verksamhet (se navnlig §§ 9, 16, 17 og 18 om elektroniske signaturer).[39]

6.2.3. Udvalgte links til finske Internet-sider

www.finlex.fi/svenska/index.html
www.ficora.fi/englanti/index.html
www.mintc.fi

---

[37] www.ficora.fi/ruotsi/document/Kommunikationsverket072003M.pdf (Rekommandationen: www.ficora.fi/ruotsi/document/SMS07.pdf).
[38] www.ficora.fi/ruotsi/document/Kommunikationsverket082003M.pdf (Rekommandationen: www.ficora.fi/ruotsi/document/SMS08.pdf).
[39] www.finlex.fi.

6.3. Islandsk ret

I 2001 nedsattes en arbejdsgruppe, som havde til opgave at behandle spørgsmål om opbygningen af en national islandsk struktur for elektroniske underskrifter og elektronisk identifikation. På baggrund af arbejdsgruppens forslag[40] opstillede den islandske regering en strategi, som bl.a. indebærer en fokusering på udbredelsen og standardiseringen af elektroniske certifikater.

Mens flere myndigheder, herunder toldmyndighederne, skattemyndighederne og Fiskeristyrelsen er påbegyndt anvendelsen af digitale signaturer, er udbredelsen af e-legitimation til private borgere stadig ganske begrænset. Der er således kun udstedt ca. 2000 certifikater – baseret på smart cards – med henblik på e-government og e-banking.

Der er i Island iværksat flere pilot-projekter, der sigter til at afdække behovet for e-identifikation.

6.3.1. Myndigheder mv.

Statsministerens kontor har ansvaret for IT-området på nationalt plan, herunder den almindelige koordinering af IT-området. Desuden har samtlige øvrige ministerier medvirket til at udvikle en generel national IT-strategi.

6.3.2. Lovgivningen

Island er gennem EØS-samarbejdet forpligtet til at gennemføre direktivet om elektroniske signaturer. Direktivet blev gennemført i islandsk ret ved lög nr. 28 af 7. maj 2001 um refrænar undirskriftir,[41] som er en stort set stringent implementering uden væsentlige ændringer i forhold til direktivteksten.

Udover arbejdsgruppen for opbygning af en national islandsk struktur for elektroniske underskrifter og elektronisk identifikation blev der i 2001 nedsat en arbejdsgruppe, som havde til hensigt at vurdere særlige juridiske spørgsmål. På baggrund af arbejdsgruppens anbefalinger fremsattes et

---

[40] Se: http://eng.fjarmalaraduneyti.is/media/Utgefin_rit/KPMG-report.pdf, hvor arbejdsgruppens rapport er tilgængelig i engelsk oversættelse (The Government of Iceland's Committee on PKI Preliminary PKI study on requirements and comparable initiatives in other countries, May 2001).
Se: http://eng.fjarmalaraduneyti.is/media/Utgefin_rit/KPMG-report.pdf.

[41] Se www.althingi.is/lagas/128a/2001028.html. Loven kan i engelsk oversættelse findes på følgende Internetadresse: http://eng.idnadarraduneyti.is/laws-and-regulations/nr/1179.

forslag om ændring af forvaltningsloven.[42] Lovforslaget blev vedtaget ved lov nr. 51 af 20. marts 2003,[43] som hjemler mulighed for, at myndighederne under visse opregnede betingelser kan anvende digital signatur som alternativ til traditionel underskrift.

6.3.3. Links til udvalgte islandske Internet-sider

www.althini.is
www.raduneyti.is/

6.4. Norsk ret

Lovmoderniseringen i Norge

I august 2001 fremlagde det norske Nærings- og Handelsdepartement forslag til ændringer i 39 love for at fjerne retlige hindringer for elektronisk kommunikation.[44] Lovforslaget er efterfølgende blev vedtaget som lov nr. 117 af 21. december 2001 om "endringer i diverse lover for å fjerne hindringer for elektronisk kommunikasjon".[45]

Inden for privatretten var der kun forholdsvis få absolutte hindringer for elektronisk kommunikation, og i mange tilfælde har en fortolkning af den enkelte bestemmelse ført til, at bestemmelsen som udgangspunkt er teknologineutral. Herudover blev det under lovarbejdet generelt forudsat, at begrebet "skriftlig" bør tolkes teknologineutralt, således at "skriftlig" skal ses i modsætning til "mundtlig", og at f.eks. en e-mail således dækkes af begrebet "skriftlig". Imidlertid tilkendegav det norske Justitsministerium i forbindelse med lovarbejdet, at det kan være hensigtsmæssigt, at det udtrykkeligt fremgår, at lovens eventuelle formkrav ikke hindrer elektronisk kommunikation, idet den blotte usikkerhed om et formkravs indhold kan hæmme den teknologiske og samfundsmæssige udvikling.

Også den norske aftalelov, der har store ligheder med den danske aftalelov, blev i denne forbindelse gennemgået. Det blev i denne forbindelse konstateret, at aftaleloven ikke indeholdt retlige hindringer for elektronisk aftaleindgåelse eller anden elektronisk kommunikation, selv om det samtidigt blev tilkendegivet, at udviklingen fremover skal følges.

I forslaget til loven blev der foretaget en mere generel drøftelse af, om der er behov for at fastsætte regler om, at elektronisk fremsendelse af visse meddelelser kræver modtagerens samtykke. Det anføres således, at de fleste mennesker er vant til, at vigtige meddelelser, der kan påvirke den pågældendes retsstilling, sendes med traditionel brevpost.

For at undgå situationer, hvor valget af kommunikationsmiddel helt er op til afsenderen, har man i flere norske love indsat bestemmelser, hvorefter elektronisk fremsendelse af de pågældende meddelelser kræver modtagerens samtykke.

---

[42] Stjórnsýslulög (lög nr. 37 af 30. apríl 1993).

[43] Lög um breytingu á stjórnsýslulögum, nr. 37/1993 (rafræn stjórnsýsla).

[44] Forslaget er tilgængelig på: www.odin.dep.no/odin/.

[45] Loven er tilgængelig på http: //www.lovdata.no/ltavd1/lt2001/t2001-1-16-19.html.

6.4.1. Særlige tiltag

I den norske regerings overordnede IT-politik for perioden 2002-2005[46] anføres det bl.a., at regeringen vil arbejde for, at der etableres og udvikles en infrastruktur for elektroniske signaturer i Norge. Det anføres endvidere, at infrastrukturen skal udvikles i et samarbejde mellem offentlige og private tjenesteleverandører samt brugere (af IT-samfundet).

Der findes to hovedinitiativer til fremme af anvendelsen af digitale signaturer i Norge, nemlig *PKI-Forum,*[47] som har til opgave at øge anvendelsen af elektronisk ID og elektronisk signatur, og *Koordineringsorganet for PKI i offentlig sektor*, som skal koordinere den offentlige sektors elektroniske identifikation.[48]

PKI-Forums hovedopgaver var oprindelig at etablere PKI-baserede løsninger samt at øge kendskabet og tilliden til elektroniske tjenester, som gør brug af PKI. PKI-forum havde i henhold til det oprindelige mandat følgende formålsbestemmelse:

> "PKI Forumet skal bidra til å utløse verdiskapningspotensialet i eNorge gjennom å være katalysator for etablering av hensiktsmessig(e) infrastruktur(er) i Norge som muliggjør, sikrer og forenkler elektroniska transaksjoner og - informasjonsutveksling knyttet til elektronisk handel, - forretningsdrift og elektroniske offentlige tjenester. Forumet skal etablere konkrete resultatmål med 6-12 måneders horisont og etterprøve disse."

PKI-forums mandat er efterfølgende ændret, således at hovedopgaverne nu er at udvikle strategier og handlingsplaner med henblik på udbredelsen af PKI-baserede løsninger og øge kundskaben om – og skabe tillid til – PKI-baserede løsninger i samfundet.[49]

Formålet med PKI Forum er således ikke i sig selv at fremme PKI løsninger, men derimod at fokusere på alle de tjenester som PKI muliggør. PKI Forum beskæftiger sig ligeledes med "totalløsninger", hvor PKI indgår som en komponent blandt flere.

---

[46] Angivet i planen eNorge fra maj 2002. http://odin.dep.no/archive/nhdvedlegg/01/03/eNorg022.pdf

[47] PKI: Public Key Infrastructure. Om PKI-forum: se www.handel.no/pkiforum/modules/module_109/publisher_view_product.asp?iEntityId=829.

[48] Organet er nedsat med hjemmel i § 28 i forskrift nr. 656 af 28. juni 2002 om elektronisk kommunikasjon med og i forvaltningen. Se www.dep.no/aad/modernisering/tverrgaendeprosjekter/pkiorgan/index-b-n-a.html.

[49] www.handel.no/pkiforum/modules/module_109/publisher_view_product.asp?iEntityId=829.

Koordineringsorganet for PKI i offentlig sektor har til opgave at sikre, at den offentlige sektors anvendelse af elektroniske signaturer standardiseres inden udgangen af 2005, således at brugerne får en så ensartet løsning som muligt at forholde sig til. Hovedopgaverne for organet er således at kortlægge, stimulere, samordne, standardisere, anbefale og informere på området for PKI i det offentlige.

Koordineringsorganet ledes af Arbeids- og administrasjonsdepartementet og har i øvrigt medlemmer fra Finansdepartementet, Helsedepartementet, Justisdepartementet, Kommunal- og regionaldepartementet, Nærings- og Handelsdepartementet, Samferdselsdepartementet og Sosialdepartementet.

6.4.2. Myndigheder mv.

Det er i dag det nyetablerede ministerium, Moderniseringsdepartementet, som har ansvaret for den overordnede nationale IT-politik i Norge.[50] Herudover er Nærings- og Handelsdepartementet ansvarlig for forskellige specifikke områder, herunder administrationen af lov om elektronisk signatur,[51] idet visse opgaver dog er uddelegeret til Samferdselsdepartementet (Post- og teletilsynet).[52]

Af andre væsentlige områder kan nævnes "personopplysningsforskriften", som er udstedt i medfør af personopplysningsloven. Mens det er Justisdepartementet, der administrerer loven, er varetagelsen af personopplysningsforskriften uddelegeret til Arbeids- og administrasjonsdepartementet.[53]

Det er ligeledes Arbeids- og administrasjonsdepartementet, som varetager tværgående spørgsmål angående IT i den offentlige sektor samt ministerierne (departementerne) imellem.

---

[50] http://odin.dep.no/mod/norsk/tema/ITpolitikk/bn.html og http://odin.dep.no/mod/norsk/bn.html.

[51] Lov nr. 81 af 15. juni 2001.

[52] Ved forskrift nr. 615 af 15. juni 2001.

[53] Ved forskrift nr. 1263 af 15. december 2000.

6.4.3. Lovgivningen[54]

Direktivet om elektroniske signaturer er EØS-relevant, og Norge er således forpligtet til at gennemføre direktivet på linje med EUs medlemsstater. Direktivet blev gennemført i norsk ret ved lov nr. 81 af 15. juni 2001 om elektronisk signatur.[55]

Udgangspunktet for den norske lovgivning har været en direktivtro gennemførelse, og der er således ikke indført særlige regler i forbindelse med implementeringen, som ikke også fremgår af direktivet.

Det bemærkes i øvrigt, at Nærings- og Handelsdepartementet (sammen med Finansdepartementet) den 9. marts 2004 har sendt et ændringsforslag til lov om elektronisk signatur i høring med henblik på at skabe en hjemmel til at etablere en frivillig certificerings- og godkendelsesordning for udstedere af digitale signaturer.[56] Ordningen ønskes etableret med henblik på at højne niveauet for de tjenester, som tilbydes af certifikatudstedere, både i forhold til krav, som stilles til kvalificerede certifikater efter lov om elektronisk signatur, og krav, som stilles til certifikater på et lavere niveau. Efter etableringen af Moderniseringsdepartementet den 1. oktober 2004 er arbejdet med lovforslaget imidlertid sat i bero, idet Moderniseringsdepartementet i stedet har påbegyndt arbejdet med en "kravspecifikation" for elektronisk signatur/elektronisk ID.[57]

Forslaget er en opfølgning på Stortingets vedtagelse af 16. juni 2003, om at regeringen skal fremme forslag med henblik på en sidestilling af skriftlig (visuel) og elektronisk legitimation efter hvidvaskningsloven.[58]

6.4.4. Formkrav mv. i lovgivningen

Som i den øvrige nordiske ret er aftalefriheden – og herunder formfriheden – også et centralt princip i norsk ret. Der gælder således som udgangspunkt ikke formkrav ved indgåelse af aftaler, og parterne kan vælge at indgå aftaler f.eks. mundtligt eller skriftligt, herunder elektronisk.[59]

---

[54] Om reguleringen af e-signaturer i Norge, se: Thomas Myhr, Elektroniske signaturer, Regulering og rettsvirkning. http://revreg.pdc.no/index.php?seks_id=8130&element=artikkel.

[55] www.lovdata.no/all/nl-20010615-081.html.

[56] www.dep.no/nhd/norsk/publ/hoeringsnotater/024081-990114/index-dok000-b-n-a.html.

[57] Se nærmere om kravsspecifikationsarbejdet på: http://odin.dep.no/jd/norsk/publ/hoeringsnotater/012001-080035/index-hov001-b-n-a.html.

[58] Lov nr. 41 af 20. juni 2003 om tiltak mot hvitvasking av utbytte fra straffbare handlinger mv. (hvitvaskingsloven).

[59] Princippet kan udledes af Norske Lov (1687) 5-1-1, som svarer til Danske Lov 5-1-1.

Tilsvarende gælder også princippet om fri bevisføring og fri bevisvurdering i norsk ret, hvilket indebærer, at parterne i en sag, som føres ved domstolene, som udgangspunkt kan føre ethvert bevis, der måtte findes hensigtsmæssigt, som så vil indgå ved rettens endelige bevisvurdering. Der er således ikke retsligt noget i vejen for at fremlægge elektroniske dokumenter i retten, ligesom en digital signatur kan anvendes som bevis for identiteten på den angivne udsteder af dokumentet.

I forhold til aftaleloven har Justitsdepartementet i overensstemmelse hermed udtalt, at "*avtaleloven ikke oppstiller rettslige hindringer for elektronisk avtaleinngåelse eller annen elektronisk kommunikasjon på avtalerettens område*."[60]

Som i dansk ret er der også i norsk lovgivning bestemmelser, som fastsætter krav om skriftlighed, og som således fraviger udgangspunktet om formfrihed. Krav om skriftlighed i lovteksten anses imidlertid ikke i sig selv at være til hinder for elektronisk kommunikation, og det skal således fremgå eksplicit af lovteksten, dersom en bestemmelse stiller krav om skriftlighed, og det ikke er hensigten, at dette krav skal kunne opfyldes ved elektronisk kommunikation.[61]

6.4.5. Lovmodernisering

Som nævnt i betænkning 1400/2000 iværksatte den norske regering i 1999 ved det såkaldte *"kartleggingsprosjekt"* en gennemgang af norsk ret med henblik på at finde ud af, hvor der fandtes formkrav, der hindrede anvendelsen af digital kommunikation. Resultaterne af *kartleggingsprosjektet* blev offentliggjort af Nærings- og Handelsdepartementet i en rapport.[62]

Konklusionen på kartleggingsprosjektet blev, at Norge ikke ønskede en generel bestemmelse (f.eks. svarende til den danske forvaltningslovs § 32 a), som skulle tage højde for anvendelsen af elektronisk kommunikation i det offentlige. Dette førte til, at kartleggingsrapporten i stedet blev brugt som en art manual i de forskellige ministeriers (departementers) arbejde med at fjerne unødige hindringer for elektronisk kommunikation.

---

[60] Se Ot.prp. nr. 108 (2000-2001) kapitel 3.7.1. http://odin.dep.no/jd/norsk/publ/hoeringsnotater/012001-080035/index-hov001-b-n-a.html.

[61] En sådan eksplicit lovtekst findes f.eks. § 10 i inkassoloven (lov nr. 26 af 13. maj 1988 med senere ændringer), som fastsætter følgende: "Når et krav er mottatt til inkasso og betalingsfristen i inkassovarsel etter § 9 er løpt ut, skal inkassatoren sende skyldneren en skriftlig oppfordring på papir…".

[62] http://odin.dep.no/filarkiv/112654/kartlegging.pdf. Om det tilsvarende danske lovmoderniseringsarbejde henvises til nr. 2.2.

Resultatet af dette arbejde blev et samlet lovforslag, som indeholdt ændringer til 39 forskellige love.[63] Ændringerne trådte i kraft 1. januar 2002. Herudover blev der med virkning fra 1. juli 2001 foretaget ændringer i 21 forskellige forskrifter.

I bemærkningerne til lovforslaget[64] peges der på, at der er en lang række tilfælde, hvor reglerne i forvejen ikke er til hinder for elektronisk kommunikation, og at der derfor her ikke var behov for regelændringer.

6.4.6. Links til udvalgte norske Internet-sider

www.npt.no
www.odin.dep.no
www.odin.dep.no/
www.statskonsult.no
www.pki.no/
www.zebsign.no
www.lovdata.no
www.enorge.org
www.handel.no

6.5. Svensk ret[65]

I forbindelse med fremsættelse af et lovforslag i 1997 (prop. 1997/98:136) opstillede den svenske regering retningslinjer for og krav til den fremtidige statslige forvaltning, herunder også regler om informationsteknikkens anvendelse. I forslaget gav regeringen bl.a. udtryk for, at statsforvaltningen – med respekt for integritet og sikkerhedsaspekter – burde udnytte informationsteknologiens muligheder til at forenkle og forbedre kontakterne mellem borgerne og myndighederne, til at øge offentlighedens indsigt og kontrol med myndighedernes virksomhed og til at effektivisere samarbejdet mellem myndigheder, den øvrige offentlige sektor og EU-institutionerne samt andre landes forvaltninger.

---

[63] Ot.prp. nr. 108 (2000-2001). Forslaget blev senere vedtaget som lov om endringer i diverse lover for å fjerne hindringer for elektronisk kommunikasjon: http://odin.dep.no/nhd/norsk/publ/otprp/024001-050007/inn-bu.html.

[64] http://odin.dep.no/nhd/norsk/publ/otprp/024001-050006/inn-bn.html.

[65] Gennemgangen bygger på oplysninger modtaget ved mails af 15. april og 8. november 2004 fra Sveriges Næringsdepartement samt redegørelsen "Digitala signaturer i Norden" af 24. november 2003, som er udarbejdet af det svenske *Statskontoret*.

Siden 1997 har Sverige gennemført en lang række tiltag på IT-området, herunder, som det vil fremgå nedenfor, også tiltag, som angår digitale signaturer.

6.5.1. Myndigheder mv.

Næringsdepartementet har det overordnede ansvar for koordineringen mv. af den samlede IT-politik, mens Finansdepartementets forvaltningspolitiske enhed er ansvarlig for IT-områderne af mere forvaltningsretlig karakter. Særlige spørgsmål vedrørende elektronisk identificering og elektroniske underskrifter (SAMSET-projektet) er henlagt til Skatteverket, mens regeringens "Statskontor" varetager opgaverne vedrørende "24-timmarsmyndigheden", jf. nedenfor. Spørgsmål i tilknytning til lag om kvalificerade elektroniska signaturer (2000:832) henhører under Post- och Telestyrelsen.

Af særlige organer på området kan herudover nævnes *Nämnden för elektronisk förvaltning*[66] og *Delegationen för utveckling av offentliga e-tjänster* (også kaldet 24-timmarsdelegationen).[67]

Nämnden för elektronisk förvaltning er nedsat med hjemmel i "förordning (2003:769) med instruktion för Nämnden för elektronisk förvaltning" med henblik på at støtte udviklingen af en sikker og effektiv elektronisk informationsudveksling mellem myndigheder indbyrdes samt mellem myndigheder og private, herunder at fastsætte standarder og lignende krav, som er nødvendige for den elektroniske informationsudvikling. Nævnet skal desuden bistå med information og udarbejde retningslinjer samt medvirke til, at der udbydes tjenester og produkter, som kan understøtte den elektroniske informationsudveksling.

Delegationen för utveckling av offentliga e-tjänster blev nedsat i juni 2003 med henblik på at drive udviklingen af "24-timmarsmyndigheden". En af delegationens vigtigste opgaver i den forbindelse er at igangsætte samarbejde om udviklingen af elektroniske tjenester mellem stat, kommune og amter (landsting) samt mellem den offentlige sektor og erhvervslivet.

Begrebet 24-timmarsmyndighed dækker over en myndighed, som er brugerorienteret, som arbejder åbent og effektivt med offentlig service, og som er tilgængelig for borgerne, når der er behov herfor. For at en myndighed kan kaldes en 24-timmarsmyndighed, skal visse krav være opfyldt, herunder skal myndigheden over Internettet informere klart og tydeligt om sin virksomhed og om

---

[66] Se herom www.statskontoret.se/organisation.

[67] Se herom www.24-timmarsmyndigheten.se og www.statskontoret.se/pdf/2003100.pdf.

borgernes rettigheder og pligter i relation til det offentlige og give adgang for alle til hurtige og kvalificerede svar, uanset hvem vedkommende er, og hvor i landet vedkommende bor. Når begrebet 24-timmarsmyndighed oprindeligt blev indført, var det med henblik på at skabe en mere positiv og serviceorienteret udviklingsspiral for myndighederne inden for elektronisk forvaltning. I dag anvendes begrebet også for kommuner og landsting (amtsforvaltning), som indfører principperne for 24-timmarsmyndigheder.

6.5.2. Lovgivningen

Sverige gennemførte direktivet om elektroniske signaturer ved lov nr. 832 af 2. november 2000 om kvalificerede elektroniske signaturer (lag om kvalificerade elektroniska signaturer (2000:832)). Ved loven er der udelukkende sket implementering af direktivet. Lovens § 22 indeholder dog en hjemmel for fastsættelse af regler for gebyrer (avgifter) for tilsynsmyndighedens virksomhed i medfør af loven.

Hidtil har ingen certifikatsudbydere foretaget den lovpligtige anmeldelse til tilsynsmyndigheden (Post- och Telestyrelsen) om, at udbyderen er påbegyndt udstedelsen af kvalificerede certifikater, og der findes således endnu ingen udbydere af kvalificerede elektroniske signaturer i Sverige.[68]

Som i dansk ret er den frie bevisvurdering en væsentlig del af den svenske retsanvendelse og gælder ligeledes for retshandlinger signeret elektronisk. Der er i Sverige derfor som udgangspunkt heller ingen særlige krav til e-certifikaters gyldighed, men som det fremgår nedenfor, skal e-certifikater, der skal anvendes inden for den offentlige sektor, opfylde kravene angivet i retningslinjerne udarbejdet i forbindelse med SAMSET-projektet.

En vigtig bestemmelse i denne sammenhæng findes i § 10 i förvaltningslagen (1986:223), som fastsætter følgende:

> Ett telegram eller annat meddelande som inte är underskrivet skall bekräftas av avsändaren genom en egenhändigt undertecknad handling, om myndigheten begär det.

Bestemmelsen indebærer f.eks., at en myndighed kan vælge at acceptere en digital signatur i stedet for f.eks. at kræve en traditionel underskrift.

---

[68] § 8 i lag (2000:832) af 2. november 2000 om kvalificerade elektroniska signaturer implementerer direktivets krav om anmeldelse til tilsynsmyndigheden. Oplysningen stammer fra redegørelsen Digitala Signature i Norden, som er udsendt den 24. november 2003.

Ved en regeringsbeslutning af 21. december 2000[69] pålagde Regeringen Riksskatteverket (nu Skatteverket) i forening med Rigsförsäkringsverket, Patent- och Registreringsverket og Statskontoret at etablere en sammenhængende administration af elektronisk identifikation inden for statsforvaltningen. Regeringen anmodede herunder om, at der blev udarbejdet retningslinjer og almindelige rutiner for certifikathåndteringen inden for statsforvaltningen samt at samordne de tjenester, som kræves for en velfungerende offentlig infrastruktur, der gør brug af digitale signaturer (SAMSET projektet). [70]

Skatteverket afgav den 27. februar 2003 rapporten "Administration av certifikat för elektronisk identifiering och elektroniska signaturer i statsförvaltningen",[71] hvori regeringens spørgsmål besvares, og hvori der anføres standarder, retningslinjer og forslag vedrørende anvendelsen af elektronisk identifikation.

Redegørelsen indeholder herunder en model for udbud af elektroniske identifikationsløsninger til offentligheden. Det anføres således, at Skatteverket, Rigsförsäkringsverket og Patent- och Registreringsverket alle har forskellige elektroniske tjenester i produktion, som borgerne ved hjælp af en "elektronisk ID-handling" kan anvende.

For at få en e-legitimation til brug over for det offentlige kan borgeren mod behørig legitimation henvende sig til en af de pågældende leverandører. Hidtil har bankerne, Posten og Telia udstedt ca. 100.000 digitale signaturer.[72]

Som nævnt er der ikke i svensk ret særlige krav til, hvad der kræves, for at en digital signatur er gyldig. Imidlertid har Skatteverket i forbindelse med SAMSET-projektet fastsat retningslinjer for myndighedernes anvendelse af digitale signaturer, herunder fastsat krav til udstedelsen af signaturer, hvis disse skal kunne anvendes over for det offentlige.[73] Udover at overholde disse retningslinjer, skal leverandørerne indgå en rammeaftale med Statskontoret, førend e-certifikaterne må udbydes med henblik på anvendelse til kommunikation med det offentlige.[74]

---

[69] http://finans.regeringen.se/fragor/forvaltningspolitik/pdf/uppdragrsv.pdf.

[70] SAMSET er en forkortelse for: Samhällets Elektroniska Tjänster.

[71] www.rsv.se/samset/pdf/d_rapport.pdf.

[72] Jf. The Legal and Market Aspect of Electronic Signatures, oktober 2003.

[73] Riksskatteverkests meddlanden, RSV M 2003:24. Se www.rsv.se/rattsinfo/meddelanden/03/rsvm_200324.html.

[74] Følgende leverandører har i dag (pr. 24. november 2003) en rammeaftale med Statskontoret: Föreningssparbanken och Handelsbanken, Nordea bank, Posten samt Telia.

6.5.3. Lovmodernisering

Ligesom Danmark[75] har Sverige foretaget en gennemgang af lovgivningen med henblik på at finde frem til regler, der kan udgøre en hindring for digital kommunikation.[76] I en redegørelse (DS 2003:29, Formel, Formkrav och Elektronisk kommunikation) udarbejdet af en arbejdsgruppe nedsat af Regeringskancelliet på baggrund af indberetninger fra de forskellige ressortministerier, er der således foretaget en gennemgang af gældende formkrav i love og forordninger. I redegørelsen har arbejdsgruppen desuden afgivet visse forslag til at fjerne unødige hindringer for elektronisk kommunikation.

Som et nyt eksempel på en lov, som gennemfører principperne i redegørelsen, kan nævnes lag om "självbetjäningstjänster via Internet inom socialförsäkringens administration (2004:115)".[77] Loven indeholder regler om selvbetjening via Internettet inden for socialforsikringsområdet, herunder bl.a. regler om adgangen til personoplysninger samt til at foretage visse retshandlinger. Af særlig interesse for denne betænkning fastsætter lovens § 3 følgende:

> "Enskild som lämnar uppgifter i samband med att han eller hon använder en självbetjäningstjänst skall använda en sådan elektronisk signatur som avses i 2 § lagen (2000:832) om kvalificerade elektroniska signaturer. Om det är fråga om att få tillgång till personuppgifter skall certifikat, till vilket en säker identifieringsfunktion är knuten, användas för kontroll av användarens identitet. Om det finns någon annan metod för identifiering eller skydd mot förvanskning av uppgifter som är tillräckligt säker med hänsyn till risken för integritetsintrång eller annan skada får dock den användas.
>
> Elektronisk signatur skall dock alltid användas när uppgifter skall lämnas på heder och samvete."

Det bemærkes, at denne lovgivning ud over at åbne op for anvendelsen af digitale signatur, stiller krav om anvendelse af kvalificeret digital signatur i tilfælde, hvor en erklæring eller andet skal afgives på ære og samvittighed (heder och samvete).

---

[75] Se om regeringens handlingsplan for lovmodernisering ovenfor i nr. 2.2.

[76] http://finans.regeringen.se/propositionermm/ds/pdf/ds2003_29.pdf.

[77] www.notisum.se/rnp/sls/lag/20040115.htm.

6.5.4. Links til udvalgte svenske Internet-sider

www.lagrummet.gov.se
www.naring.regeringen.se
www.prs.se
www.riksdagen.se
www.rsv.se
www.statskontoret.se
www.swedac.se
www.24-timmarsmyndigheten.se
www.skatteverket.se

Kapitel 7

Udvalgets overvejelser

7.1. Almindelige bemærkninger

Udgangspunktet i dansk aftaleret er, at der ikke gælder særlige formkrav til aftalers indgåelse. Dette udtrykkes i den fortsat gældende bestemmelse i 5-1-1 i Danske Lov fra 1683 således, at "Een hver er pligtig at holde hvad han med Mund, Hånd og Segl lovet og indgået haver".

Formueretligt er det afgørende for at blive bundet, at der er afgivet et løfte, mens det er ligegyldigt på hvilken måde løftet er afgivet. Der er i og for sig ingen grænse for, på hvilke måder løfter kan afgives. Eksemplifikationen i Danske Lov af "Mund, Hånd og Segl" angiver nogle indgåelsesmåder, som fortsat er af stor praktisk betydning. Mundtlige aftaler er således ganske udbredte og fuldt ud gyldige, hvis man i øvrigt kan bevise indholdet af dem. I visse brancher, f.eks. ved kreaturhandel, forekommer der stadig, i hvert fald i visse egne af landet og på visse markeder, handler, der indgås ved håndslag, som må betragtes som en underafdeling af de mundtlige løfter. Underskrift i form af laksegl bruges i praksis ikke mere, bortset fra ved indgåelse af visse særligt højtidelige aftaler, men udtrykket "segl" kan også ses som en henvisning til underskrift med blæk eller med maskinskrift og lignende.

Der er intet til hinder for at indgå aftale elektronisk, f.eks. ved at tilbudsgiver og tilbudsmodtager udveksler e-mails med tilbud og accept og angivelse af deres navne. En aftale indgået ved brug af e-mail er fuldt ud gyldig, og det er således ikke nødvendigt at bruge digital signatur, førend en aftale indgået elektronisk bliver gyldig. På de anden side er der heller intet til hinder for at indgå aftale ved udveksling af mails, som er forsynet med digital signatur, og den digitale signatur kan da bidrage til at skabe større sikkerhed for, at den angivne afsender virkelig også er den, som har sendt den pågældende elektroniske meddelelse. Den digitale signatur kan således knytte en større bevisværdi til de elektroniske meddelelser, hvorved en aftale er indgået.

Brugen af elektroniske aftaledokumenter er da også meget udbredt i forretningslivet, ikke mindst i brancher, hvor brugen af edb hertil kombineres med logistiksystemer, og hvor elektronisk udveksling af oplysninger giver store fordele.

Brugen af digitale underskrifter – være sig med eller uden anvendelse af digital signatur - adskiller sig kun i teknisk henseende fra brugen af håndskrevne underskrifter. Brugen af moderne teknik til at udføre selve underskriftshandlingen medfører således i almindelighed ikke nogen ændring i forhold til de regler, som angiver retsvirkningen af den pågældende underskrift.

Teknologiske landvindinger har da også igennem tiderne bevirket, at skrevne meddelelser eller aftaler fra at være skrevet med pen af gåsefjer og blæk er gået over til helt eller delvis at blive udfærdiget under anvendelse af nye teknologier, f.eks. fyldepennen, faksimilestemplet, skrivemaskinen, telegrafen, fjernskriveren, kopimaskinen, kuglepennen, fjernsynet, computeren og telefonen (sms). Disse teknologier har kunnet revolutionere den måde, vi kommunikerer og indgår aftaler med hinanden på, uden at det har været nødvendigt at ændre reglerne om retsvirkningerne af underskrifter.

Reglerne om retsvirkningen af underskrifter bygger på, at det afgørende er tilkendegivelsen gennem handling eller undladelse af en vilje til at blive forpligtet, og at formen for denne tilkendegivelse er uden betydning. Disse regler er grundlæggende teknologineutrale og kan siges at være udtryk for et princip om ækvivalens (ligestilling) mellem forskellige former for underskrifter og forskellige former for dokumenter (papirbaserede, henholdsvis elektroniske). Reglerne har kunnet anvendes uden særlige problemer, efterhånden som nye teknologier er blevet taget i anvendelse. Det er derfor på tilsvarende måde muligt at tage den nye teknologi, som brugen af digitale meddelelser og brugen af digitale signaturer er, i brug, uden at det er nødvendigt at ændre reglerne om retsvirkninger af underskrifter.

Ved vurderingen af, hvilke retsvirkninger der er forbundet med anvendelsen af digitale signaturer, må man, som det fremgår af det følgende, tage udgangspunkt i dansk rets almindelige regler og principper.

Det er udvalgets generelle opfattelse, at en digital signatur i almindelighed må sidestilles med en almindelig papirbaseret underskrift, og at der ikke er nogen grund til at knytte særlige retsvirkninger til aftaler, retshandler eller meddelelser, der afgives med digital signatur. Udvalget ser således ingen grund til at give afgiveren eller modtageren af en aftale, retshandel eller meddelelse nogen særlig retsstilling, blot fordi der er underskrevet med en digital signatur og ikke en håndskreven underskrift.

Udvalget finder endvidere, at der alene bør indføres særlige lovregler om digitale signaturer, hvis der ved anvendelsen af disse almindelige formueretlige regler og principper ikke opnås en rimelig eller hensigtsmæssig retstilstand, eller hvis der i øvrigt foreligger særlige grunde, der taler for en

lovregulering, f.eks. et væsentligt behov for afklaring af retstilstanden. Der bør i givet fald alene ske en fravigelse af almindelige formueretlige principper mv., hvis der foreligger helt særlige grunde hertil.

7.2. Digital signatur og begrænsninger i gyldigheden af det tilhørende certifikat

7.2.1. Præsentation af problemstillingen

Retsvirkningerne af en digital underskrift adskiller sig i princippet ikke fra retsvirkningerne af en håndskreven underskrift. Det afgørende er tilkendegivelsen af en vilje til at blive bundet, og denne vilje kan tilkendegives såvel ved en handling som ved en undladelse.

Der kan dog rejses nogle særlige spørgsmål vedrørende retsvirkningerne af brugen af digitale signaturer. Disse spørgsmål kan rejses, fordi de certifikater, som er knyttet til den digitale signatur, kan indeholde forskellige begrænsninger. Man kan derfor spørge, hvad der gælder, hvis man til at underskrive et elektronisk dokument anvender en digital signatur uden for det område, hvor den er gyldig, dvs. i strid med de begrænsninger, som i certifikatet angives for den digitale signaturs gyldighed.

Den første type af begrænsning har sammenhæng med, at indehaveren af en digital signatur har mulighed for at få sit certifikat spærret, hvis der opstår mistanke om, hvorvidt certifikatet er blevet kompromitteret, f.eks. hvis uvedkommende har haft adgang til den computer eller et chipkort, hvorpå den digitale signatur er lagret. Efter § 9, stk. 1, i lov om elektroniske signaturer skal certificeringscentret (ved kvalificerede certifikater) sørge for en hurtig og sikker katalog- og tilbagekaldelsestjeneste, som bl.a. giver mulighed for at undersøge, om et certifikat er spærret. Efter stk. 2 skal certificeringscentret spærre certifikatet straks efter at have modtaget anmodning herom, eller hvis forholdene i øvrigt tilsiger det.[78] Certificeringscentret vil sædvanligvis have en tilsvarende spærretjeneste for ikke-kvalificerede certifikater.[79]

Et af hovedformålene med en sådan spærretjeneste er som nævnt at beskytte certifikatindehaveren mod, at tredjemand uberettiget anvender den digitale signatur i tilfælde af, at den private nøgle er kompromitteret (dvs. at andre uberettiget har eller kan have fået kendskab til den private nøgle).

---

[78] Bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav mv. til nøglecentre indeholder i § 11 nærmere regler om katalog- og tilbagekaldelsestjenesten.

[79] Se f.eks. Certifikatpolitik for OCES-personcertifikater, version 2 (september 2004), pkt. 7.3.6. Se betænkningens bilag 3.

En spærring af certifikatet kan dog også skyldes andre forhold, f.eks. at certifikatindehaveren ikke længere ønsker at være i besiddelse af en digital signatur, at certifikatindehaveren har misligholdt kontrakten med certifikatudstederen, eller at den medarbejder, der er angivet i et medarbejdercertifikat, er fratrådt.

Den anden type af begrænsning har sammenhæng med, at teknologien på dette område udvikles med en sådan hast, at digitale signaturer kun har gyldighed i et begrænset åremål, som står i det certifikat, som er knyttet til den digitale signatur. Man tidsbegrænser gyldigheden af det certifikat, som er knyttet til den digitale signatur, fordi man ikke kan udelukke, at de krypteringsalgoritmer, som den digitale signatur består af, vil kunne brydes inden for en kortere tidshorisont. Løbende fornyelse af den digitale signatur sikrer således, at der kan ske overgang til en stærkere krypteringsalgoritme, inden den anvendte krypteringsalgoritme bliver sårbar over for angreb med deraf følgende risiko for, at uvedkommende kan kompromittere signaturen.

Det certifikat, der er knyttet til en digital signatur, vil således normalt indeholde en udløbsdato. Det fremgår således af § 4, stk. 1, nr. 5, i lov om elektroniske signaturer, at et kvalificeret certifikat skal indeholde dets gyldighedsperiode, ligesom OCES-certifikatpolitikkerne fastsætter, at et OCES-certifikat skal indeholde certifikatets ikrafttrædelses- og udløbsdato.[80] Udløbsdatoen kan dog også have andre funktioner, f.eks. at give mulighed for, at der i forbindelse med udstedelse af et nyt certifikat løbende kan ske opdatering af forskellige oplysninger i certifikatet.

Den tredje type af begrænsning i et certifikats gyldighed kan tænkes at bestå i, at signaturen kun skal kunne anvendes til bestemte typer af transaktioner mv. (formålsbegrænsninger) eller kun inden for visse beløbsgrænser (beløbsbegrænsninger).

Et kvalificeret certifikat skal indeholde en tydelig angivelse af eventuelle formåls- eller beløbsbegrænsninger, jf. lov om elektroniske signaturer § 4, stk. 2, nr. 6 - 7. Et OCES-certifikat skal tilsvarende indeholde eventuelle anvendelsesbegrænsninger.[81]

Formålet med at angive anvendelsesbegrænsninger for et certifikat må i første række antages at være at begrænse certificeringscentrets ansvar over for brugerne af en digital signatur. Efter § 11, stk. 3, i lov om elektroniske signaturer er certificeringscentret således ikke ansvarligt for tab, der er opstået som følge af, at et kvalificeret certifikat er anvendt uden for de formåls- eller beløbsbe-

---

[80] Se f.eks. Certifikatpolitik for OCES-personcertifikater, version 2.0 (september 2004), pkt. 7.3.3. Se betænkningens bilag 3.

[81] Se f.eks. Certifikatpolitik for OCES-personcertifikater, version 2.0 (september 2004), pkt. 7.3.3. Se betænkningens bilag 3.

grænsninger, som fremgår af certifikatet. Ved OCES-signaturer kan certifikatudstederen i disse tilfælde fraskrive sig ansvaret over for erhvervsdrivende og offentlige myndigheder, men ikke over for private borgere,[82] og man må gå ud fra, at certificeringscentre i praksis i videst muligt omfang vil fraskrive sig ansvaret for tab som følge af brugen af en digital signatur i strid med certifikatets anvendelsesbegrænsninger.

På nuværende tidspunkt er der teknisk ikke noget til hinder for, at certifikatindehaveren anvender den digitale signatur, selv om det tilhørende certifikat er spærret eller udløbet eller indeholder en anvendelsesbegrænsning, som overskrides i forbindelse med brugen.

7.2.2. Tidligere forslag til lovregler

Det daværende Forskningsministeriums udkast til lovforslag om digitale signaturer mv. fra 1998 indeholdt følgende bestemmelser med henblik på at regulere certifikatindehaverens retsstilling i tilfælde, hvor den digitale signatur blev anvendt efter, at certifikatet var spærret eller udløbet:

> "**§ 7.** ...
> *Stk. 2.* Der kan ikke støttes ret på en digital meddelelse med digital signatur, hvor det tilhørende nøglecertifikat er spærret, medmindre det godtgøres, at den digitale signatur blev afgivet før, nøglecertifikatet blev spærret.
>
> **§ 8.** ...
> *Stk. 3.* Der kan ikke støttes ret på en digital meddelelse med digital signatur, hvor det tilhørende nøglecertifikat er udløbet, medmindre det godtgøres, at den digitale signatur blev afgivet før, nøglecertifikatet udløb, og at den digitale meddelelse inden udløbet af nøglecertifikatet er suppleret med en digital signatur, hvor det tilhørende nøglecertifikat ikke er udløbet."
>
> **§ 9**. ...
> Stk. 3. Der kan ikke støttes ret på en digital meddelelse med digital signatur, hvor meddelelsen falder uden for anvendelsesområdet angivet i nøglecertifikatet."

Disse regler var efter lovudkastets bemærkninger navnlig begrundet i et ønske om at opstille klare og entydige regler, selv om det erkendtes, at certifikatindehaveren f.eks. senere ville kunne fragå et løfte f.eks. under henvisning til, at certifikatet var udløbet på anvendelsestidspunktet. Der pegedes i bemærkningerne på, at det som en anden mulighed kunne overvejes at udforme en bevisbyrderegel, hvorefter der ikke kunne støttes ret på signaturen, medmindre det blev godtgjort, at certifikatindehaveren havde vilje til at forpligte sig.

---

[82] Se f.eks. Certifikatpolitik for OCES-personcertifikater, version 2.0 (september 2004), pkt. 6.4. Se betænkningens bilag 3.

Lovudkastets regler blev kritiseret kraftigt under høringen over lovudkastet og blev derfor ikke medtaget i forslaget til lov om elektroniske signaturer mv. Man fandt, at udkastets regler indebar en fravigelse af grundlæggende aftaleretlige principper om, at en person bliver bundet af en viljeserklæring, uden at der opstilles særlige krav til formen herfor. Det blev samtidig anført, at en retstilstand, hvor certifikatindehaveren som udgangspunkt bliver bundet af erklæringer, som den pågældende har afgivet ved anvendelse af en digital signatur, selv om det tilhørende certifikat er spærret eller udløbet, eller dets anvendelsesbegrænsninger overskredet, må antages at indebære en lige så klar retstilstand som lovudkastets regel.

7.2.3. Udvalgets vurdering af gældende ret

Spørgsmålet om den retlige betydning af de ovennævnte tre former for begrænsninger i certifikater, der er knyttet til digitale signaturer, må i forhold til gældende ret tage sit udgangspunkt i, at der som udgangspunkt ikke gælder formkrav for afgivelse af løfter mv. Et certifikat kan være udløbet eller spærret af rent formelle grunde, uden at dette behøver at dække over nogen reel begrænsning i certifikatindehaverens evne til at disponere, på samme måde som en anvendelsesbegrænsning i realiteten ikke behøver at være og i praksis næppe heller er udtryk for andet end certificeringscentrets ønske om at begrænse sit eget ansvar.

I den forbindelse må man også være opmærksom på, at der efter dansk ret intet som helst er til hinder for at indgå retligt forpligtende aftaler og andre retshandler på formuerettens område ved udveksling af elektroniske meddelelser uden anvendelse af digital signatur. Den digitale signatur har bl.a. til formål at give en større sikkerhed, end der ellers ville være, for, at en elektronisk meddelelse er afsendt af den person, som meddelelsen angiver som afsender, men meddelelsen er fuldt ud gyldig og forpligtende også uden en digital signatur.

Spørgsmålet om den retlige virkning af, at certifikatindehaveren anvender en digital signatur i strid med en begrænsning i certifikatet, kan i realiteten omformuleres til et spørgsmål om, hvorvidt den, der anvender den digitale signatur, f.eks. efter udløbet af en tidsbegrænsning eller i strid med en af de andre begrænsninger, kan slippe for at være bundet af det løfte, som er afgivet under anvendelse af signaturen, blot ved at henvise til, at der er sket en overskridelse af en begrænsning i det certifikat, der er knyttet til den digitale signatur. Med andre ord er spørgsmålet, i hvilket omfang eventuelle anvendelsesbegrænsninger for certifikatet må forstås sådan, at de (også) har til formål at beskytte certifikatindehaveren mod uovervejede eller utilsigtede dispositioner ved anvendelse af en digital signatur.

Hvis der er tale om et mere formaliseret forhold mellem certifikatindehaveren og signaturmodtageren, f.eks. faste samhandelsparter eller parter i et lukket system, dvs. et system, hvor den digitale signatur alene anvendes til kommunikation mellem en nærmere afgrænset kreds af brugere (f.eks. mellem en bank og dens kunder), vil spørgsmålet om virkningen af, at certifikatets anvendelsesbegrænsninger overskrides, kunne være reguleret direkte i aftaleforholdet mellem parterne. Selv om dette ikke er tilfældet, vil parternes forudgående kontakter kunne få betydning, f.eks. hvis parterne tidligere har anvendt digitale signaturer i strid med anvendelsesbegrænsningerne, uden at dette er blevet anfægtet, eller omvendt, hvis overskridelse af anvendelsesbegrænsningerne tidligere (konsekvent) er blevet anfægtet.

I andre tilfælde, hvor den digitale signatur således anvendes i et åbent system, hvor kredsen af mulige kommunikationsparter ikke på forhånd er nærmere afgrænset, og hvor der ikke tidligere har været kontakter mellem parterne, er det derimod næppe generelt afklaret, hvilken betydning det har for forholdet mellem certifikatindehaveren og signaturmodtageren, at en digital signatur er anvendt i strid med certifikatets anvendelsesbegrænsninger.

Anvendelsen af digitale signaturer er endnu ikke særlig udbredt, og der kan næppe på nuværende tidspunkt fastlægges en almindelig forståelse i gældende ret af, om begrænsninger i certifikatet også har til formål at regulere forholdet mellem certifikatindehaveren og signaturmodtageren. Det forekommer imidlertid nærliggende at fortolke begrænsningerne således, at disse alene har til hensigt at begrænse certificeringscentrets ansvar.

Det kan således ikke antages, at begrænsninger i et certifikat efter gældende ret har den almindelige virkning, at certifikatindehaveren ikke bliver bundet af dispositioner, som certifikatindehaveren foretager på trods af begrænsningerne. Ellers ville certifikatindehaveren kunne benytte den pågældende anvendelsesbegrænsning til efter forgodtbefindende til at gøre sig fri af sine forpligtelser (en slags selvbåndlæggelse), og en sådan konstruktion kendes ikke i dansk ret.

Der findes således i dansk ret ikke almindelige regler, der giver en person mulighed for generelt at tilkendegive, at personen ikke vil være bundet af dispositioner, som foretages på en bestemt måde, eller at bestemte dispositioner kun skal være bindende, hvis de er foretaget på en nærmere angiven måde. Efter almindelige aftaleretlige fortolkningsregler måtte en efterfølgende disposition i strid med en generel tilkendegivelse herom således formentlig anses for en (stiltiende) ophævelse af de "selvpålagte formkrav", således at løftegiveren blev bundet af den efterfølgende disposition.

Det skal dog fremhæves, at sådanne selvpålagte formkrav ikke altid kan tilsidesættes ud fra denne betragtning, og at spørgsmålets besvarelse derfor må afhænge af en konkret vurdering bl.a. af formålet med den pågældende begrænsning.

Således antages det, at der kan ske tinglysning af rådighedsbegrænsninger, hvorved ejeren af en fast ejendom forpligter sig til alene at sælge eller pantsætte ejendommen med samtykke fra en bestemt anden person. Sådanne rådighedsbegrænsninger kan benyttes til med den pågældendes indforståelse at hjælpe f.eks. ældre til at undgå dispositioner, som den pågældende ikke kan overskue, uden at det er nødvendigt at skride til umyndiggørelse eller værgebeskikkelse.

I Pengeinstitutankenævnets praksis er det på linie hermed antaget, at en aftale mellem en myndig kontohaver og et pengeinstitut, hvorefter dispositioner over kontoen forudsætter samtykke fra tredjemand (f.eks. kontohaverens forældre), er bindende, således at pengeinstituttet handler ansvarspådragende, hvis det foretager udbetalinger i strid med det aftalte vilkår.[83] Også i denne situation har aftalen til formål at beskytte kontohaveren mod uoverlagte dispositioner over kontoen.

Hvis man antog, at certifikatindehaveren ikke blev bundet af dispositioner, som den pågældende foretager ved brug af digital signatur i strid med certifikatets anvendelsesbegrænsninger, ville certifikatindehaveren – i modsætning til, hvad der er det almindelige formueretlige udgangspunkt i dansk ret – i realiteten kunne skabe sig en generel fortrydelsesret med hensyn til dispositioner foretaget ved anvendelse af én bestemt kommunikationsteknologi. Certifikatindehaveren vil således på dette punkt generelt opnå en bedre retsstilling end ved anvendelse af mere "traditionelle" kommunikationsformer.

Udvalget finder på denne baggrund, at det aftaleretlige udgangspunkt i dag må være, at certifikatindehaveren bliver bundet af dispositioner foretaget ved anvendelse af en digital signatur, også selv om signaturen er anvendt i strid med certifikatets anvendelsesbegrænsninger.

7.2.4. Udvalgets overvejelser om behovet for lovregler

Udvalget finder, at der ved vurderingen af, om der er behov for lovregler vedrørende retsvirkningerne af certifikatindehaverens egen brug af en digital signatur i strid med begrænsninger i et certifikat, må tages udgangspunkt i dansk rets almindelige aftaleretlige regler og principper.

---

[83] Lennart Lynge Andersen og Peter Møgelvang-Hansen, Bankretlige emner (GadJura 1994), side 74 f.

Udvalget finder generelt, at der alene bør indføres særlige lovregler om anvendelsen af digitale signaturer, hvis almindelige aftaleretlige regler og principper ikke fører til en rimelig og hensigtsmæssig retstilstand, eller hvis retstilstanden er uklar, således at der er et væsentligt behov for at afklare den gennem lovregler. Der bør endvidere kun ske en fravigelse af almindelige aftaleretlige principper, hvis der foreligger helt særlige grunde hertil.

Med hensyn til *digitale signaturer, der anvendes efter, at de er udløbet eller spærret*, må det aftaleretlige udgangspunkt efter udvalgets opfattelse som nævnt ovenfor i nr. 7.2.3 være, at certifikatindehaveren bliver bundet af erklæringer, som den pågældende afgiver ved udveksling af elektroniske meddelelser forsynet med digital signatur, på samme måde som den pågældende bliver bundet af erklæringer, der afgives på anden måde, f.eks. ved anvendelse af elektroniske meddelelser uden anvendelse af digital signatur eller ved udveksling af papirdokumenter med håndskreven underskrift.

Dette udgangspunkt må efter udvalgets opfattelse i hvert fald fastholdes, hvor certifikatindehaveren anvender signaturen, selv om det tilhørende certifikat er udløbet eller spærret. Den pågældende må således antages at blive bundet af erklæringen, selv om certifikatet ikke længere er "gyldigt". Det er naturligvis en forudsætning, at det konkret kan lægges til grund, at den digitale signatur faktisk er anvendt af certifikatindehaveren selv og ikke uberettiget er anvendt af en tredjemand. Med hensyn til spørgsmålet om beviset for, hvem der har anvendt den digitale signatur, henvises til det, som anføres nedenfor i nr. 7.5.

Det ændrer efter udvalgets opfattelse ikke herved, at signaturmodtageren i praksis kan undersøge, om certifikatet er udløbet eller spærret, enten ved manuel kontrol af certifikatet eller af certificeringscentrets spærreliste eller ved modtagesystemets automatiske kontrol heraf. Det afgørende er, at certifikatindehaveren selv har ønsket at afgive et løfte og således forpligte sig ved anvendelse af den pågældende digitale signatur.

Efter udvalgets opfattelse er der her tale om en klar og enkel retstilstand, der er i overensstemmelse med almindelige aftaleretlige principper om, at der ikke gælder særlige formkrav for løfter mv., og at løftegiveren bliver forpligtet af sit løfte. Udvalget finder derfor ikke, at der er behov for særlige lovregler vedrørende tilfælde, hvor certifikatindehaveren anvender en digital signatur efter, at det tilhørende certifikat er udløbet eller spærret.

Med hensyn til *certifikatindehaverens brug af en elektronisk signatur i strid med anvendelsesbegrænsninger i certifikatet* må det først fremhæves, at sådanne anvendelsesbegrænsninger efter det, der er oplyst for udvalget, ikke har større praktisk betydning, og at de i givet fald må antages at

have til formål at begrænse certificeringscentrets ansvar, jf. ovenfor i nr. 7.2.3. Som ligeledes dér anført kan anvendelsesbegrænsninger ikke antages at have til formål at beskytte certifikatindehaveren mod utilsigtede eller uovervejede dispositioner og kan ikke have den virkning, at den pågældende efter forgodtbefindende kan erklære ikke at være bundet af erklæringer, som er afgivet ved anvendelse af en digital signatur i strid med anvendelsesbegrænsninger i certifikatet.

Certifikatindehaveren har endvidere i dag normalt kun begrænset indflydelse på udformningen af de anvendelsesbegrænsninger, der fastsættes for et certifikat, og kan normalt ikke få udstedt et certifikat med individuelle anvendelsesbegrænsninger, herunder individuelle formålsbegrænsninger.

Også ved vurderingen af betydningen af anvendelsesbegrænsninger i et certifikat må der efter udvalgets opfattelse tages udgangspunkt i, at spørgsmålet må anses for tilfredsstillende reguleret ved dansk rets almindelige regler, hvorefter der som udgangspunkt ikke gælder særlige formkrav for afgivelse af løfter mv. I dansk ret findes der ikke generelle regler, der giver personer mulighed for egenhændigt generelt at tilkendegive, at personen ikke vil være bundet af dispositioner, som foretages på en bestemt måde, eller at den pågældende kun vil være bundet af bestemte dispositioner, hvis de er foretages i en nærmere angiven form eller på en nærmere angiven måde. Efter almindelige aftaleretlige fortolkningsregler ville en efterfølgende disposition i strid med en sådan generel tilkendegivelse i øvrigt antagelig efter omstændighederne indebære en (stiltiende) ophævelse af sådanne selvpålagte formkrav, således at løftegiveren alligevel ville blive bundet af den efterfølgende disposition, jf. ovenfor i nr. 7.2.3.

Efter det, som er oplyst over for udvalget, er sådanne "selvbåndlæggelser" da i praksis også alene søgt anvendt i særlige tilfælde, jf. ovenfor i nr. 7.2.3 om tinglysning af rådighedsdeklarationer på fast ejendom og om Pengeinstitutankenævnets praksis. I disse tilfælde har der været tale om en konkret aftale mellem to aftaleparter vedrørende en helt specifik situation (disposition over en fast ejendom, henholdsvis en bankkonto) og ikke en generel tilkendegivelse med hensyn til anvendelse af en bestemt kommunikationsform eller lignende.

Udvalget finder som fremhævet ovenfor i nr. 7.2.3, at det aftaleretlige udgangspunkt efter gældende ret er, at certifikatindehaveren bliver bundet af dispositioner foretaget ved anvendelse af en digital signatur, også selv om signaturen er anvendt i strid med certifikatets anvendelsesbegrænsninger.

Denne retstilstand må efter udvalgets opfattelse anses for rigtig og hensigtsmæssig.

Hvis man gennemførte en ordning, hvorefter en certifikatindehaver ikke blev bundet af dispositioner, som den pågældende foretager ved brug af digital signatur i strid med anvendelsesbegrænsninger i det hertil hørende certifikat, ville certifikatindehaveren kunne misbruge denne retstilstand til efter forgodtbefindende at fragå aftaler eller andre formueretlige retshandler, som den pågældende har indgået under anvendelse af den digitale signatur.

Signaturmodtageren ville i praksis ikke have nogen muligheder for at værge sig imod, at hans kontraktspart skabte sig en sådan ensidig fortrydelsesret. Det er ikke altid let for en signaturmodtager at vurdere, om en digital signatur er anvendt i strid med anvendelsesbegrænsninger i et certifikat. En sådan vurdering kunne vel forholdsvist let foretages ved en beløbsmæssig begrænsning, men også her kunne der opstå tvivlsspørgsmål, f.eks. om hvordan en beløbsgrænse skal forstås ved lån eller køb på kredit, hvor det samlede beløb, der skal betales, overstiger lånets hovedstol eller købsprisen. Men der kunne også tænkes andre former for begrænsninger end beløbsmæssige, og problemet med at vurdere overholdelsen heraf ville blive yderligere forstærket, hvis certifikatindehaveren fik mulighed for at få indsat individuelle anvendelsesbegrænsninger i certifikatet, som f.eks. indebar, at den digitale signatur kun kunne anvendes til dispositioner, der lever op til visse miljømæssige eller etiske standarder.

Udvalget finder derfor, at dansk rets almindelige regler giver en tilfredsstillende regulering af forholdet, og at der ikke bør indføres særlige lovregler om retsvirkningerne af, at en digital signatur anvendes uden for anvendelsesbegrænsninger i certifikatet.

Udvalget har i tilknytning til dette spørgsmål overvejet, om hensynet til at søge at beskytte certifikatindehaveren mod uovervejede eller utilsigtede dispositioner ved anvendelse af en digital signatur kan begrunde, at der indføres generelle regler om fortrydelsesret, navnlig med henblik på tilfælde, hvor certifikatindehaveren er forbruger.

Efter lov om visse forbrugeraftaler mv. har forbrugere imidlertid allerede ved fjernsalg en generel fortrydelsesfrist på 14 dage. I det omfang en forbruger indgår elektroniske aftaler ved fjernsalg, f.eks. via Internettet eller ved anvendelse af e-mail, vil den pågældende således i vidt omfang have en almindelig fortrydelsesret i forhold til den erhvervsdrivende, således at forbrugeren herigennem beskyttes mod utilsigtede eller uovervejede dispositioner. Denne fortrydelsesret gælder, uanset om aftalen er indgået under anvendelse af digital signatur, eller dette ikke er tilfældet, og i givet fald også uden hensyn til, om den digitale signatur er anvendt inden for eller uden for anvendelsesbegrænsninger i certifikatet.

Hertil kommer, at aftaler og retshandler indgået elektronisk, herunder ved anvendelse af digital signatur, er omfattet af de almindelige beskyttelsesregler i aftaleloven, herunder aftalelovens § 36 om aftaler mv., som det vil være urimeligt eller i strid med redelig handlemåde at gøre gældende, og aftalelovens kapitel IV om urimelige kontraktvilkår i forbrugerforhold. Forbrugere, der indgår elektroniske aftaler eller andre retshandler med eller uden digital signatur, er således også i kraft af disse regler i et vist omfang beskyttet mod utilsigtede eller uovervejede dispositioner ved anvendelse af en digital signatur. Anvendes en digital signatur til betalingstransaktioner, sætter loven om visse betalingsmidler endvidere visse begrænsninger for, hvad kortindehaveren hæfter for.

Udvalget finder på denne baggrund ikke, at der er behov for at indføre lovregler specielt for aftaler, der indgås ved brug af digital signatur, som skal beskytte certifikatindehavere – navnlig forbrugere – mod utilsigtede eller uovervejede dispositioner.

7.3. Virksomheders brug af digital signatur

7.3.1. Præsentation af problemstillingen

Et af den digitale signaturs hovedformål er at skabe større sikkerhed for, at en elektronisk aftale, retshandel eller anden meddelelse, der er signeret med en digital signatur, rent faktisk er tiltrådt af den person, som signaturen angiver. Den private nøgle og den adgangskode, der hører til en digital signatur, skal derfor behandles som en meget personlig ting.

Hvis indehaveren af en digital signatur (certifikatindehaveren) overlader sin private nøgle til en anden, kan der opstå spørgsmål om, hvorvidt certifikatindehaveren må anses for at have legitimeret denne anden til at handle på sine vegne.

Spørgsmålet om, hvorvidt der skabes et fuldmagtsforhold ved, at en virksomhed giver en medarbejder adgang til at bruge en privat nøgle, opstår ved såkaldte medarbejdercertifikater og virksomhedscertifikater, for hvilke det karakteristiske er, at det umiddelbart kan udledes af certifikatet, at indehaveren af den private nøgle er forskellig fra certifikatindehaveren. Et *medarbejdercertifikat* indeholder en angivelse af en medarbejder og af den virksomhed eller organisation, som medarbejderen er knyttet til. Medarbejderen er indehaver af den private nøgle, og certifikatet er udstedt til virksomheden. Et *virksomhedscertifikat* angiver i modsætning til et medarbejdercertifikat ikke den fysiske person, der er indehaver af den private nøgle, men angiver alene, at den digitale signatur stammer fra en bestemt virksomhed eller organisation.

Om overladelse af en digital signatur i andre tilfælde kan skabe et fuldmagtsforhold, behandles nedenfor i nr. 7.4.

7.3.2. Udvalgets vurdering af gældende ret

Spørgsmålet om, hvorvidt der ved en virksomheds overladelse af et medarbejdercertifikat eller et virksomhedscertifikat til en medarbejder skabes et fuldmagtsforhold, må efter udvalgets opfattelse afgøres på grundlag af almindelige aftaleretlige regler og principper herom, og vurderingen heraf vil således i første række afhænge af en konkret vurdering af den enkelte sags omstændigheder mv.

Indeholder et *medarbejdercertifikat* ikke andre angivelser end identiteten på medarbejderen og virksomheden, kan det på den ene side anføres, at certifikatet ikke i sig selv udstyrer den pågældende medarbejder med fuldmagt, og at certifikatet alene viser, at medarbejderen er knyttet til virksomheden, således at medarbejderens adgang til at disponere på virksomhedens vegne må afgøres efter de almindelige regler herom, herunder den almindelige stillingsfuldmagt efter aftalelovens § 10, stk. 2.

Man må dog på den anden side også se på praksis i den pågældende virksomhed og eventuelt tillige branche samt løftemodtagerens tidligere forhold til og erfaringer med virksomheden og dennes sædvanlige fremgangsmåde, når man skal bedømme, om en løftemodtager har føje til at opfatte udstedelsen af medarbejdercertifikat til en medarbejder som en særskilt stillingsfuldmagt. Der vil således kunne tænkes tilfælde, hvor virksomheder netop ved at udstede medarbejdercertifikater til bestemte medarbejdere til brug for udførelsen af bestemte handlinger herved udstyrer de pågældende medarbejdere med stillingsfuldmagt eller anden særlig fuldmagt til at forpligte virksomheden.

Hvis et medarbejdercertifikat ikke indeholder anvendelsesbegrænsninger, må det efter udvalgets opfattelse i almindelighed antages, at certifikatet ikke i sig selv udstyrer den pågældende medarbejder med en særlig fuldmagt til at disponere på virksomhedens vegne. Ellers ville der være tale om en generel fuldmagt til den pågældende medarbejder til at disponere med retsvirkning for virksomheden, og det må i almindelighed have formodningen imod sig, at det har været hensigten at udstyre medarbejderen med en så vidtgående fuldmagt – navnlig set i lyset af, at certifikatet ikke udtrykkeligt indeholder en generel fuldmagt til den pågældende.

Er det i certifikatet udtrykkeligt angivet, at medarbejderen har kompetence til at forpligte organisationen i et nærmere bestemt omfang (f.eks. indkøb af varer inden for et vist maksimumsbeløb), må der formentlig antages at foreligge en fuldmagt med særlig tilværelse. Dette gælder, uanset at fuldmagtsdokumentet – her certifikatet - ikke er udstedt af fuldmagtsgiveren (virksomheden), idet det afgørende er, at det er udstedt efter anmodning fra virksomheden. Om en angivelse i medarbejdercertifikatet af en anvendelsesmæssig eller beløbsmæssig begrænsning i givet fald gælder frem for medarbejderens almindelige stillingsfuldmagt, eller om løftemodtageren kan påberåbe sig en videregående stillingsfuldmagt i forhold til virksomheden, må afhænge af de konkrete omstændigheder, herunder oplysninger om, hvad der må antages at have været fuldmagtsgiverens hensigt, og oplysninger om, hvordan denne hensigt har givet sig til kende i forhold til løftemodtageren.

Det kan anføres, at et certifikat, der f.eks. blot indeholder en beløbsangivelse uden nærmere at angive, hvilke dispositioner medarbejderen kan foretage, ikke uden videre kan tages som udtryk for, at medarbejderen er udstyret med en generel fuldmagt til at disponere inden for denne beløbsangivelse. Det kan også anføres, at der ligesom ovenfor i nr. 7.2 må anlægges en vurdering af, om en sådan begrænsning alene har til formål at begrænse certifikatudstederens eventuelle erstatningsansvar,[84] eller om den (også) har til formål at regulere forholdet mellem certifikatindehaveren og signaturmodtageren, dvs. at begrænse medarbejderens mulighed for at forpligte virksomheden i forhold til tredjemand.

Heroverfor kan det ved medarbejdercertifikater indgå i vurderingen, at det i fuldmagtsforhold er sædvanligt at fastsætte begrænsninger for, i hvilket omfang fuldmægtigen kan forpligte fuldmagtsgiveren, og at det derfor kan være mere nærliggende ved medarbejdercertifikater end ved almindelige personcertifikater at antage, at certifikatets anvendelsesbegrænsninger også har til formål at regulere dispositionsmulighederne for indehaveren af den private nøgle.

Ved medarbejdercertifikater, der indeholder en eller flere anvendelsesbegrænsninger, vil det på denne baggrund efter omstændighederne være nærliggende at antage, at en virksomheds overladelse af et sådant certifikat til en medarbejder, afhængigt af anvendelsesbegrænsningernes nærmere indhold og udformning, efter en konkret vurdering indebærer, at der gives en særlig fuldmagt til den pågældende medarbejder til at disponere med retsvirkning for virksomheden inden for de pågældende begrænsninger.

---

[84] Jf. herved f.eks. lov om elektroniske signaturer § 11, stk. 3, hvorefter certificeringscentret (ved kvalificerede certifikater) ikke er ansvarligt for tab opstået som følge af, at certifikatet er anvendt uden for formåls- og/eller beløbsbegrænsningerne.

Der foreligger kun få praktiske erfaringer med *virksomhedscertifikater* og ingen retspraksis herom, som nærmere kan belyse, hvilke virkninger der kan knyttes til et virksomhedscertifikat. Et virksomhedscertifikat kan på den ene side sammenlignes med, at en medarbejder har fået adgang til at anvende virksomhedens brevpapir, uden at medarbejderens navn eller tilknytning til virksomheden fremgår af brevpapiret. Men alt efter de konkrete omstændigheder kan virksomhedscertifikatet på den anden side også sammenlignes med, at en medarbejder, således som det er almindeligt i visse brancher, f.eks. vekselererbranchen og rederibranchen, får adgang til at underskrive med virksomhedens eller indehaverens navn og således får en meget vidtgående fuldmagt med særlig tilværelse. De konkrete forhold i vedkommende virksomhed og branche vil derfor være afgørende for vurderingen af, om en virksomheds overladelse af et virksomhedscertifikat til en medarbejder skaber et fuldmagtsforhold.

I det omfang der ved medarbejdercertifikater og virksomhedscertifikater antages at foreligge fuldmagtsforhold, vil retsvirkningerne af, at fuldmægtigen ved anvendelse af den digitale signatur handler uden for fuldmagtens grænser (legitimationen) eller uden for sin bemyndigelse, skulle vurderes i forhold til aftalelovens almindelige regler herom.

7.3.3. Udvalgets overvejelser om behovet for lovregler

Udvalget finder, at spørgsmålet om, hvorvidt en virksomheds overladelse af et medarbejdercertifikat eller virksomhedscertifikat til en medarbejder indebærer, at virksomheden herved giver den pågældende medarbejder fuldmagt til at handle på virksomhedens vegne, kan løses tilfredsstillende på grundlag af almindelige aftaleretlige regler og principper, navnlig reglerne i aftalelovens kapitel II om fuldmagt.

Disse spørgsmål er efter udvalgets opfattelse som udgangspunkt ikke egnede til lovregulering, og udvalget finder ikke, at der alene for digitale signaturer bør indføres særlige lovregler om, hvornår der er etableret et fuldmagtsforhold.

Det bør således som hidtil overlades til retspraksis efter en konkret vurdering at tage stilling til, om et medarbejdercertifikat eller virksomhedscertifikat udstyrer den pågældende medarbejder med en særlig fuldmagt til at disponere på virksomhedens eller organisationens vegne.

7.4. Uberettiget brug af andres digitale signatur

7.4.1. Præsentation af problemstillingen

En digital signatur er en meget personlig ting og skal opbevares og anvendes på en måde, der ikke kompromitterer sikkerheden.

Hvis andre uberettiget får adgang til den digitale signatur med tilhørende kode, kan det tænkes, at den digitale signatur vil kunne misbruges til at signere aftaler, retshandler eller elektroniske meddelelser i certifikatindehaverens navn. Der må sondres mellem tilfælde, hvor en person uberettiget afgiver erklæring i en andens navn (falsk), og tilfælde, hvor en afgiven erklæring uberettiget ændres (forfalskning).

Tilfælde med falsk i forbindelse med anvendelse af digital signatur kan f.eks. opstå, hvis det lykkes for en tredjemand at omgå sikkerhedsprocedurerne i forbindelse med udstedelse af certifikatet og få udstedt et certifikat i en andens navn. Som eksempel herpå kan nævnes, at det lykkes den pågældende at få udstedt et kvalificeret certifikat[85] i en andens navn ved at anvende et forfalsket pas, eller at en person bestiller en ikke-kvalificeret signatur (f.eks. en OCES-signatur) i en andens navn og derefter opsnapper brevet fra certificeringscentret med den PIN-kode, der skal anvendes for at aktivere signaturen.

Tilfælde af falsk ved anvendelse af en digital signatur vil også – og nok mere praktisk – kunne opstå, hvis det lykkes tredjemand at få adgang til den private nøgle til et allerede udstedt certifikat, f.eks. som følge af certifikatindehaverens uforsigtighed ved opbevaring eller anvendelse af den private nøgle.

Anvendelse af en digital signatur skal bl.a. sikre, at der ikke efterfølgende kan ændres i den meddelelse, der er forsynet med signaturen, uden at dette kan registreres af signaturmodtageren. Der vil derfor (så længe den pågældende digitale signatur teknologisk er "sikker") kun kunne blive tale om forfalskning af erklæringer, der er forsynet med en digital signatur, hvis det er lykkedes at "bryde" den kryptering, som er sket ved signeringen af meddelelsen med den digitale signatur.[86]

---

[85] Ved udstedelse af kvalificerede certifikater gælder der som udgangspunkt et krav om personligt fremmøde, jf. § 6 i bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav mv. til nøglecentre).

[86] Se herom nærmere betænkning 1400/2000, side 24 ff.

Der må derfor navnlig tages stilling til, om certifikatindehaveren bliver bundet ved aftaler mv., som en anden uberettiget indgår i certifikatindehaverens navn under anvendelse af den pågældendes digitale signatur.

Der kan også rejses spørgsmål om, hvorvidt certifikatindehaveren har pligt til at give certificeringscentret besked om at spærre certifikatet, og i hvilket omfang certifikatindehaveren ifalder erstatningsansvar for manglende spærring af certifikatet. I det omfang certifikatindehaveren ifalder erstatningsansvar, kan der rejses spørgsmål om, hvorvidt der er anledning til at begrænse dette.

7.4.2. Udvalgets vurdering af gældende ret

Det klare udgangspunkt i dansk ret er, at man ikke bliver aftaleretligt forpligtet af en erklæring, der uberettiget afgives i ens navn (falsk) eller ændres efter afgivelsen (forfalskning). Falsk og forfalskning kan gøres gældende som ugyldighedsgrund også over for en løftemodtager i god tro. Et løfte binder med andre ord kun den, der har afgivet det, eller som har givet en anden fuldmagt til at afgive det.

Der kan dog rent undtagelsesvist tænkes at opstå situationer, hvor den pågældende uanset falsk eller forfalskning bliver aftaleretligt forpligtet, nemlig i tilfælde, hvor den pågældende har foretaget en handling eller undladelse, som af løftemodtageren kan opfattes som indforståelse med at være bundet.[87] Den, der ikke i rimeligt omfang søger at modvirke, at andre afgiver falske eller forfalskede erklæringer i sit navn, kan endvidere efter omstændighederne herved tænkes at pådrage sig erstatningsansvar over for den, der i god tro modtager og stoler på sådanne erklæringer. I sammenhæng hermed er det omdiskuteret, i hvilket omfang der i relation til falske/forfalskede erklæringer gælder en reklamationspligt.[88]

---

[87] Se herved Lennart Lynge Andersen og Palle Bo Madsen, Aftaler og mellemmænd (4. udg. GadJura, 2001), side 133 ff., Henry Ussing, Aftaler paa Formuerettens Omraade (3. udg., Gad, 1950), side 41 f. og 398 f., og Henrik Udsen, Den digitale signatur - ansvarsspørgsmål (GadJura 2002, Ph.d.-afhandling fra Københavns Universitet, Retsvidenskabeligt Institut), side 93 ff.

[88] Lennart Lynge Andersen og Palle Bo Madsen, Aftaler og mellemmænd (4. udg. GadJura, 2001), side 134 f., hvor det anføres, at det i almindelighed forekommer rigtigst, at man har pligt til at underrette modtageren, når man bliver klar over, at ens navn er blevet misbrugt, og at dette i hvert fald må gælde, hvis det drejer sig om en forfalskning, hvor det er afgiverens egen oprindelige erklæring, der er blevet ændret. Se endvidere – mere forsigtigt – Henry Ussing, Aftaler paa Formuerettens Omraade (3. udg., Gad, 1950), side 41 f. og 398 f., Mads Bryde Andersen, Grundlæggende aftaleret (2. udg., Gjellerup, 2002), side 382 f., og Bernhard Gomard, Civilprocessen (5. udg. under medvirken af Michael Kistrup, GadJura, 2000), side 146. Se endvidere Ugeskrift for Retsvæsen 1945.723 H, 1996.568 V og 2002.1116 Ø.

Disse almindelige aftaleretlige regler gælder også for aftaler, retshandler eller meddelelser, som uberettiget underskrives med en andens digitale signatur. Certifikatindehaveren vil således som altovervejende hovedregel ikke være bundet af en erklæring, som er afgivet af en tredjemand, der uberettiget har fået adgang til den private nøgle. Det er principielt uden betydning for den aftaleretlige bundethed, om certifikatindehaveren reklamerer over for modtageren af erklæringen, altså giver denne meddelelse om, at der foreligger falsk.[89]

For så vidt angår spørgsmålet om, i hvilke tilfælde en certifikatindehaver bliver bundet ved efterfølgende at have godkendt en (uberettiget) disposition i certifikatindehaverens navn, ses der ikke at være særlige forhold, der gør sig gældende for dispositioner, der er foretaget ved brug af digital signatur. Der kan således f.eks. henvises til Østre Landsrets dom, refereret i Ugeskrift for Retsvæsen 2002, side 1116, hvorefter en person, der 1 år efter "aftaleindgåelsen" var blevet bekendt med, at "låneaftalen" uberettiget var blevet indgået i vedkommendes navn, men efterfølgende betalte ydelser på lånet, aftalte henstand og først 4 år senere gjorde gældende, at der var tale om falsk. Der er ingen grund til at tro, at dommens resultat ville være blevet anderledes, hvis den falske aftale var blevet indgået ved brug af en digital signatur.

Det er kun *uberettiget* brug af en andens underskrift eller digitale signatur, som bevirker, at dokumenter, herunder elektroniske dokumenter, er falske. Har certifikatindehaveren givet den anden person fuldmagt til at anvende sin digitale signatur til at indgå det pågældende retsforhold i certifikatindehaverens navn ved hjælp af dennes digitale signatur, og er modtageren af erklæringen i god tro, vil certifikatindehaveren i overensstemmelse med almindelige regler om fuldmagtsforhold kunne blive forpligtet. Det samme gælder, hvis certifikatindehaveren efterfølgende godkender dispositionen enten udtrykkeligt eller ved ord eller handlinger, som af løftemodtageren med rette må opfattes som en sådan godkendelse.

Det er mere uklart, hvornår en certifikatindehavers handlinger, der sætter tredjemand i stand til at identificere sig som certifikatindehaveren, vil kunne tages som udtryk for en tilkendegivelse fra certifikatindehaveren om, at den pågældende tredjemand udstyres med en bemyndigelse til at disponere på certifikatindehaverens vegne. Om der er tale om et fuldmagtsforhold, må således i første række bero på en nærmere fortolkning af aftaleforholdet mellem certifikatindehaveren og den person, som uberettiget benytter den digitale signatur. Den blotte overgivelse af den private nøgle med tilhørende adgangskode til en anden antages næppe i sig selv at indebære, at den pågældende

[89] Spørgsmålet om reklamation kan have betydning for certifikatindehaverens eventuelle erstatningsansvar over for personer, som lider tab ved at stole på signaturen, jf. nærmere nedenfor.

herved får fuldmagt eller i øvrigt kan anses som legitimeret til at indgå aftaler på certifikatindehaverens vegne.[90] Der skal formentlig mere til, f.eks. at den uberettigede bruger i forvejen er fuldmægtig for certifikatindehaveren, eller at certifikatindehaveren ved sin adfærd har givet tredjemand (modtageren) grund til at tro, at der foreligger et fuldmagtsforhold, f.eks. ved at hovedmanden accepterer, at en person optræder på en sådan måde, at tredjemand får indtryk af, at den pågældendes dispositioner binder hovedmanden. Der vil i praksis normalt være tale om tilfælde, hvor der består et vist interessefællesskab mellem hovedmanden og mellemmanden, f.eks. i form af ægteskab, forretningsforbindelse eller ansættelsesforhold.

Under alle omstændigheder kan spørgsmålet om, hvorvidt en certifikatindehavers adfærd vil bevirke en retlig forpligtelse over for godtroende løftemodtagere, ikke afgøres uden en samlet vurdering af det samlede hændelsesforløb, herunder kendskab til, hvilke oplysninger den enkelte løftemodtager måtte have været i besiddelse af om forholdet mellem certifikatindehaveren og den, der (uberettiget) har afgivet løftet ved brug af den digitale signatur.

Hvis den private nøgle er kompromitteret som følge af certifikatindehaverens egen uagtsomhed, og certifikatindehaveren ikke efterfølgende sørger for at få spærret sin signatur, vil dette efter omstændighederne kunne indgå i den samlede vurdering af, om certifikatindehaveren bliver aftaleretligt forpligtet. Manglende spærring vil således efter omstændighederne kunne medføre, at certifikatindehaveren anses for at have givet besidderen af den private nøgle, der uhindret får mulighed for fortsat at anvende denne, fuldmagt hertil. Der skal dog formentlig temmelig meget til, og navnlig må det formentlig kræves, at certifikatindehaveren har viden om, at den private nøgle er kompromitteret.

Spørgsmålet om, hvorvidt en certifikatindehaver pådrager sig *erstatningsansvar* ved at foretage handlinger eller undladelser, som bevirker, at en anden ved at benytte certifikatindehaverens private nøgle påfører andre tab, må afgøres efter almindelige erstatningsretlige principper.

Der må foretages en afvejning af de konkrete omstændigheder, hvor der især må ses på, hvor høj grad af uagtsomhed certifikatindehaveren har udvist, og i hvilket omfang modtageren af den falske meddelelse indså eller burde have indset, at aftalen, retshandlen eller meddelelsen var falsk.

En certifikatindehavers overladelse af sin private nøgle med tilhørende adgangskode til tredjemand vil således efter omstændighederne være erstatningspådragende, hvis overladelsen har gjort

---

[90] Se f.eks. Henrik Udsen, Den digitale signatur - ansvarsspørgsmål (GadJura 2002, Ph.d.-afhandling fra Københavns Universitet, Retsvidenskabeligt Institut), s. 81 ff.

det muligt for tredjemanden at misbruge nøglen, og misbruget i øvrigt medfører et (adækvat) tab for løftemodtageren.

Efter § 9, stk. 1, i lov om elektroniske signaturer skal certificeringscentret (ved kvalificerede certifikater) sørge for en hurtig og sikker katalog- og tilbagekaldelsestjeneste, som giver mulighed for bl.a. at undersøge, om et certifikat er spærret. Efter stk. 2 skal certificeringscentret spærre certifikatet straks efter at have modtaget anmodning herom, eller hvis forholdene i øvrigt tilsiger det.[91] Certificeringscentret/certifikatudstederen vil sædvanligvis have en tilsvarende spærretjeneste ved ikke-kvalificerede certifikater.[92] Spærrelisten har den betydning, at en signaturmodtager, som ved undersøgelse heraf bliver bekendt med, at certifikatet er spærret, men alligevel forlader sig på den digitale signatur, må antages selv helt eller delvist at skulle bære risikoen for, at det viser sig, at signaturen uberettiget er anvendt af tredjemand.

De nævnte regler fastsætter ikke nogen pligt for certifikatindehaveren til at spærre certifikatet, men en sådan pligt vil i almindelighed følge af aftalen mellem certificeringscentret og certifikatindehaveren – uanset om der er tale om et kvalificeret certifikat eller ej.[93] Denne pligt til at spærre certifikatet gælder i givet fald i forhold til certificeringscentret, men herudover opstår der spørgsmål om, hvorvidt certifikatindehaveren i forhold til modtagerne af den digitale signatur har "pligt" til at spærre certifikatet ved viden eller mistanke om kompromittering af den private nøgle, således at manglende spærring indebærer en (aftaleretlig eller erstatningsretlig) forpligtelse i forhold til modtageren.

Kompromittering af den private nøgle indebærer en markant forøgelse af risikoen for misbrug af den digitale signatur, og det må derfor antages, at certifikatindehaveren efter dansk rets almindelige erstatningsregler kan blive erstatningsansvarlig, hvis den pågældende undlader at spærre certifikatet, selv om certifikatindehaveren ved eller bør vide, at den private nøgle er kompromitteret. Dette gælder formentlig, uanset om det er nøglemediet, adgangskoden eller begge dele, der er kompromitteret. Omvendt må det antages, at certifikatindehaveren ikke bliver erstatningsansvarlig for tab, som påføres andre ved misbrug af en digital signatur, efter at der er givet meddelelse til nøglecentret om spærring af certifikatet.

---

[91] Bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav mv. til nøglecentre indeholder i § 11 nærmere regler om katalog- og tilbagekaldelsestjenesten.

[92] Se f.eks. Certifikatpolitik for OCES-personcertifikater, version 2.0 (september 2004), pkt. 6.2. og pkt. 7.3.6.

[93] Det fremgår f.eks. af Vilkår for OCES-certifikat fra TDC, punkt 2.4., at "certifikatindehaveren straks [skal] spærre sit certifikat i tilfælde af kompromittering af den private nøgle eller mistanke herom. … Certifikatindehaveren skal spærre certifikatet, hvis indholdet af certifikatet ikke længere er i overensstemmelse med de faktiske forhold.".

Certifikatindehaverens erstatningsansvar for handlinger eller undladelser, som bevirker, at en anden ved at benytte certifikatindehaverens private nøgle påfører andre tab, navnlig manglende spærring, omfatter i overensstemmelse med dansk rets almindelige erstatningsregler pligt til at erstatte det fulde tab ved skader, som har årsagsforbindelse med den pågældende handling eller undladelse, og som er adækvate, dvs. er typiske følger af den skadegørende handling eller undladelse.

Med hensyn til erstatningsansvarets omfang skal det i øvrigt fremhæves, at den almindelige lempelsesregel i erstatningsansvarslovens § 24 giver mulighed for i særlige tilfælde at lempe certifikatindehaverens erstatningsansvar.

7.4.3. Udvalgets overvejelser om behovet for lovregler

Udvalget finder, at dansk rets almindelige regler og principper, således som de er beskrevet i nr. 7.4.2, giver tilfredsstillende muligheder for at løse de problemer, der kan opstå ved andres uberettigede brug af digitale signaturer.

Ligesom ved papirbaserede underskrifter må det klare udgangspunkt på tilsvarende måde ved digitale signaturer antages at være, at man ikke bliver bundet af erklæringer, som andre uberettiget afgiver i ens navn.

Dansk rets almindelige regler giver efter udvalgets opfattelse også tilfredsstillende muligheder for, at domstolene i konkrete tilfælde kan modificere dette udgangspunkt, når der den enkelte sags omstændigheder giver grundlag herfor. Således må det i overensstemmelse med almindelige aftaleretlige principper antages, at en certifikatindehaver efter omstændighederne vil kunne blive bundet af tredjemands uberettigede dispositioner under anvendelse af den digitale signatur, hvis certifikatindehaveren ved sin adfærd uagtsomt har muliggjort eller lettet tredjemands misbrug af signaturen, og der som følge af certifikatindehaverens adfærd ud fra en konkret vurdering må antages at være etableret et fuldmagtsforhold mellem certifikatindehaveren og den, der uberettiget bruger den digitale signatur, eller hvis certifikatindehaveren efterfølgende godkender dispositionen.

Udvalget finder derfor ikke grundlag for at foreslå indførelse af særlige lovregler for anvendelsen af digitale signaturer med henblik på gennem lovbestemmelser at søge at regulere, hvilken adfærd der vil kunne føre til, at certifikatindehaveren bliver forpligtet i tilfælde af, at tredjemand misbruger en digital signatur. Efter udvalgets opfattelse afgøres sådanne spørgsmål både ved digitale

signaturer og ved andre kommunikationsformer som udgangspunkt mest hensigtsmæssigt af domstolene på grundlag af en konkret vurdering af den enkelte sags omstændigheder mv.

Udvalget har endvidere overvejet, om der bør indføres særlige lovregler om certifikatindehaverens pligt til at spærre certifikatet og virkningen af, at den pågældende undlader dette, selv om certifikatindehaveren ved eller bør vide, at den private nøgle er kompromitteret.

Som det fremgår af nr. 7.4.2, må det antages, at certifikatindehaveren efter dansk rets almindelige erstatningsregler efter omstændighederne kan pådrage sig erstatningsansvar ved at undlade at spærre certifikatet, selv om certifikatindehaveren ved eller bør vide, at den private nøgle er kompromitteret. Udvalget finder, at disse spørgsmål mest hensigtsmæssigt afgøres af domstolene ud fra en konkret vurdering af den enkelte sags omstændigheder mv. på grundlag af dansk rets almindelige formueretlige regler og principper, og at der ikke er behov for at foreslå lovregler herom.

I den forbindelse finder udvalget, at den almindelige regel i erstatningsansvarslovens § 24 giver tilfredsstillende muligheder for i særlige tilfælde at lempe certifikatindehaverens erstatningsansvar.

7.5. Digital signatur og beviset for, hvem der har anvendt den

Anvendelsen af en digital signatur kan i det store og hele betragtes som en digital underskrift. Der findes dog visse forskelle, som kan være relevante, når man skal analysere de problemer, som kan opstå i forhold til retsvirkningen af en digital, henholdsvis en håndskreven underskrift.

En håndskreven underskrift er uadskilleligt knyttet til én bestemt person, således at det ved grafologiske undersøgelser antages at kunne sandsynliggøres, at underskriften er afgivet (skrevet) af den pågældende person. En håndskreven underskrift antages derfor i vidt omfang at udgøre bevis for, hvem der har underskrevet og dermed udstedt det underskrevne dokument. Men det gælder ikke altid. Også den håndskrevne underskrift kan eftergøres eller efterlignes, og muligheden herfor er endog forøget ved moderne scanningsteknik.

En digital signatur er med den nuværende teknologi ikke uadskilleligt knyttet til en bestemt person, men er derimod elektroniske data, som ikke blot den retmæssige indehaver, men også andre, kan komme i besiddelse af, f.eks. hvis de får adgang til den computer eller det chipkort, hvor den digitale signatur er lagret, og til den adgangskode, som er knyttet til den digitale signatur. Den

teknologiske udvikling vil kunne ændre dette udgangspunkt, således at der opstår en tættere forbindelse mellem den digitale signatur og dens indehaver (certifikatindehaveren). Således vil man f.eks. kunne forestille sig, at man i løbet af nogle år vil gøre almindelig brug af fingeraftryksaflæsning i forbindelse med brug af digital signatur.

Brugen af en digital signatur i forbindelse med udstedelsen af et elektronisk dokument skaber en formodning for, at det elektroniske dokument er signeret af den person, som angives i det certifikat, der hører til den elektroniske signatur. Dette svarer til, at tilstedeværelsen af en håndskreven signatur skaber en formodning for, at dokumentet er udstedt af den, hvis signatur er anvendt.

Den bevismæssige betydning af brugen af en digital eller håndskreven signatur kan dog ikke anskues løsrevet fra parternes forhold og omstændighederne i øvrigt, herunder den praksis, som måtte udvikle sig i samfundet omkring opbevaringen af og benyttelsen af digitale signaturer.

Indholdet af det dokument, som signaturen er anvendt i forbindelse med, eller de omstændigheder, hvorunder dokumentet præsenteres for omverdenen, kan således medføre, at den, der modtager dokumentet, ikke med rimelighed kan tro, at det virkelig er den angivne person, der har underskrevet dokumentet. Der kan således næppe gælde nogen formodning for ægtheden af en digital eller håndskreven underskrift, hvis man f.eks. på et værtshus bliver præsenteret for et gældsbrev på 100 mio. kr. underskrevet af Anders Fogh Rasmussen.

I tilfælde, hvor der efter dokumentets indhold og omstændighederne i øvrigt består en formodning for ægtheden af den digitale eller håndskrevne underskrift, kan formodningen efter omstændighederne afkræftes, hvis der føres modbevis over for den sandsynliggørelse af afsenderens identitet, som brugen af digitale signatur kan skabe. Modbevis vil således kunne bestå i, at det bevises, at det er en anden end den, der er angivet som indehaver i certifikatet, som rent faktisk har anvendt den digitale signatur til at udstede dokumentet.

Dansk ret hylder princippet om bevisbedømmelsens frihed, jf. retsplejelovens § 344, stk. 2, og særlig for straffesager § 896, hvorefter bedømmelsen af bevisernes vægt ikke er bundet ved lovregler. Retten skal tillægge de enkelte beviser vægt efter den overbevisning (sandsynlighed), som beviset i den foreliggende situation skaber.[94]

---

[94] Bernhard Gomard, Civilprocessen (5. udg. under medvirken af Michael Kistrup, GadJura, 2000), s. 485 ff.

Udvalget har tiltro til, at domstolene på baggrund af dansk rets almindelige regler om bevisførelse og bevisbedømmelse vil være i stand til at løse de bevisproblemer, som måtte opstå i forbindelse med anvendelsen af digitale signaturer.

Udvalget finder derfor ikke grundlag for at foreslå særlige lovregler herom specielt med henblik på digitale signaturer.

7.6. Afsluttende bemærkninger

Som det fremgår af de ovenstående overvejelser, finder udvalget, at dansk rets almindelige regler giver en tilfredsstillende regulering af de formueretlige spørgsmål, som vil kunne tænkes at opstå i forbindelse med anvendelsen af digitale signaturer. En digital signatur må ved anvendelsen af dansk rets almindelige regler i det store og hele behandles fuldstændig som en traditionel papirbaseret underskrift, og anvendelsen af dansk rets almindelige regler herom fører efter udvalgets opfattelse til tilfredsstillende resultater i relation til digitale signaturer og de spørgsmål, som deres anvendelse kan give anledning til. Udvalget har derfor ikke fundet grundlag for at stille forslag om lovregler, der specielt tager sigte på at regulere de formueretlige spørgsmål, som kan opstå i forbindelse med anvendelsen af digitale signaturer.

Udvalget skal dog afslutningsvis fremhæve, at anvendelsen af digitale signaturer endnu er et så begrænset og nyt fænomen, at domstolene endnu ikke har haft lejlighed til at tage stilling til sager om retsvirkningerne af brug af digital signatur.

Udvalget har derfor måttet basere sine overvejelser på en abstrakt og generel gennemgang af tænkelige problemstillinger, men har ikke kunnet støtte sig til erfaringer med bedømmelsen af sager herom fra det praktiske retsliv.

Udvalget skal derfor anbefale, at man løbende overvejer, om der er behov for lovgivning om retsvirkningerne af brug af digital signatur i lyset af de erfaringer, som indvindes hermed, og den retspraksis, som dannes på dette område.

BILAG 1

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 1999/93/EF
af 13. december 1999
om en fællesskabsramme for elektroniske signaturer

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 47, stk. 2, artikel 55 og 95,

under henvisning til forslag fra Kommissionen ([1]),

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg ([2]),

under henvisning til udtalelse fra Regionsudvalget ([3]),

i henhold til fremgangsmåden i traktatens artikel 251 ([4]), og

ud fra følgende betragtninger:

(1) Kommissionen forelagde den 16. april 1997 Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget en meddelelse med titlen »Et europæisk initiativ inden for elektronisk handel«;

(2) Kommissionen forelagde den 8. oktober 1997 Europa-Parlamentet, Rådet, Det Økonomiske og Sociale Udvalg og Regionsudvalget en meddelelse med titlen »Sikkerhed og tillid i elektronisk kommunikation — Imod europæiske rammer for digitale signaturer og kryptering«;

(3) Rådet opfordrede den 1. december 1997 Kommissionen til snarest muligt at forelægge Europa-Parlamentet og Rådet et forslag til direktiv om digitale signaturer;

(4) elektronisk kommunikation og handel nødvendiggør elektroniske signaturer og dertil knyttede tjenesteydelser til autentifikation af data; forskellige regler for retlig anerkendelse af elektroniske signaturer og akkreditering af certificeringstjenesteudbydere i medlemsstaterne kan skabe betydelige hindringer for anvendelse af elektronisk kommunikation og elektronisk handel; en klar fællesskabsramme vedrørende betingelserne for elektroniske signaturer vil derimod styrke tilliden til og den generelle accept af de nye teknologier; medlemsstaternes lovgivning bør ikke udgøre en hindring for den frie bevægelighed for varer og tjenesteydelser i det indre marked;

(5) elektronisk signatur-produkters interoperabilitet bør fremmes; efter traktatens artikel 14 indebærer det indre marked et område med fri bevægelighed for varer; specifikke væsentlige krav til elektronisk signatur-produkter skal opfyldes for at sikre fri bevægelighed på det indre marked og opbygge tilliden til elektroniske signaturer, jf. dog Rådets forordning (EF) nr. 3381/94 af 19. december 1994 om en fællesskabsordning for kontrol med udførsel af varer med dobbelt anvendelse ([5]) og afgørelse 94/942/FUSP af 19. december 1994 om en fælles aktion vedtaget af Rådet vedrørende kontrol med udførslen af varer med dobbelt anvendelse ([6]);

(6) dette direktiv harmoniserer ikke levering af tjenesteydelser med hensyn til informationens fortrolige karakter, hvis disse ydelser er omfattet af nationale bestemmelser med »ordre public« eller offentlig sikkerhed;

(7) det indre marked sikrer den fri bevægelighed for personer, hvorfor unionsborgere og andre, der er bosat i EU, i stigende omfang har behov for kontakt med myndigheder i andre medlemsstater end den, hvori de er bosiddende; elektronisk kommunikation vil kunne blive til stor nytte i den forbindelse;

(8) den hastige teknologiske udvikling og Internettets globale karakter nødvendiggør, at den valgte metode er åben for forskellige teknologier og tjenester til elektronisk autentifikation af data;

(9) elektroniske signaturer vil blive anvendt i mange forskellige situationer og i forbindelse med meget forskellige applikationer, hvilket vil resultere i en lang række nye tjenesteydelser og produkter i relation til elektroniske signaturer; definitionen af sådanne produkter og tjenesteydelser bør ikke begrænses til udstedelse og forvaltning af certifikater, men bør også omfatte alle andre tjenesteydelser eller produkter, der anvender eller understøtter elektroniske signaturer, såsom registreringstjenester, tidsstempling, katalogtjenester, databehandlingstjenester eller konsulenttjenester i forbindelse med elektroniske signaturer;

(10) det indre marked giver certificeringstjenesteudbydere mulighed for at udvikle deres aktiviteter hen over grænserne med henblik på at øge deres konkurrenceevne og dermed tilbyde forbrugere og erhvervsliv nye muligheder for sikker elektronisk informationsudveksling og handel uden hensyn til grænser; certificeringstjenesteudbydere bør for at stimulere udbuddet af certificeringstjenesteydelser via åbne net i hele Fællesskabet frit kunne tilbyde deres tjenesteydelser uden forudgående autorisation; ved forudgående autorisation forstås ikke alene enhver

([1]) EFT C 325 af 23.10.1998, s. 5.
([2]) EFT C 40 af 15.2.1999, s. 29.
([3]) EFT C 93 af 6.4.1999, s. 33.
([4]) Europa-Parlamentets udtalelse af 13. januar 1999 (EFT C 104 af 14.4.1999, s. 49), Rådets fælles holdning af 28. juni 1999 (EFT C 243 af 27.8.1999, s. 33), Europa-Parlamentets afgørelse af 27. oktober 1999 (endnu ikke offentliggjort i EFT) og Rådets afgørelse af 30. november 1999 (endnu ikke offentliggjort i EFT).

([5]) EFT L 367 af 31.12.1994, s. 1. Forordningen er ændret ved forordning (EF) nr. 837/95 (EFT L 90 af 21.4.1995, s. 1).
([6]) EFT L 367 af 31.12.1994, s. 8. Afgørelsen er senest ændret ved afgørelse 1999/193/FUSP (EFT L 73 af 19.3.1999, s. 1).

tilladelse, hvis udstedelse forudsætter, at de nationale myndigheder træffer en afgørelse, inden certificeringstjenesteudbyderen kan udbyde sine certificeringstjenester, men også enhver anden foranstaltning med samme virkning;

(11) frivillige akkrediteringsordninger, hvis sigte er et tjenesteydelsesudbud på et mere avanceret niveau, kunne være den rette ramme for certificeringstjenesteudbyderne til at udvikle deres tjenester yderligere i retning af det tillids-, sikkerheds- og kvalitetsniveau, som et marked i hastig udvikling kræver; sådanne ordninger bør anspore udviklingen af optimal praksis blandt certificeringstjenesteudbydere; det bør stå certificeringstjenesteudbydere frit for, om de ønsker at tilslutte sig og nyde godt af sådanne ordninger;

(12) certificeringstjenesterne bør kunne udbydes enten af et offentligt organ eller en fysisk eller juridisk person oprettet i overensstemmelse med national ret; medlemsstaterne bør ikke forhindre certificeringstjenesteudbydere i at holde sig uden for sådanne akkrediteringsordninger; det bør sikres, at frivillige akkrediteringsordninger ikke svækker konkurrencen blandt certificeringstjenester;

(13) medlemsstaterne kan selv fastsætte, hvordan de vil sikre overvågningen af overholdelsen af direktivets bestemmelser; dette direktiv er ikke til hinder for indførelsen af overvågningssystemer, der baseres på den private sektor; direktivet forpligter ikke certificeringstjenesteudbyderne til at ansøge om at blive overvåget i henhold til en gældende akkrediteringsordning;

(14) det er vigtigt at finde den rigtige balance mellem forbrugernes og erhvervslivets behov;

(15) bilag III omfatter krav til sikre signaturgenereringssystemer med henblik på at sikre, at avancerede elektroniske signaturer fungerer hensigtsmæssigt; det omfatter ikke det samlede omgivende miljø, som systemerne opererer i; for at det indre marked kan fungere efter hensigten, er det påkrævet, at Kommissionen og medlemsstatene handler hurtigt med henblik på at muliggøre udpegelsen af de organer, der skal foretage overensstemmelsesvurderingen af sikre signatursystemer, jf. bilag III; for at imødekomme markedets behov bør overensstemmelsesvurderingen være rettidig og effektiv;

(16) dette direktiv bidrager til anvendelse og retlig anerkendelse af elektroniske signaturer i Fællesskabet; der er ikke behov for lovfæstede rammeforskrifter for elektroniske signaturer, der udelukkende anvendes inden for systemer, som er baseret på frivillige privatretlige aftaler mellem et afgrænset antal deltagere; parternes frihed til indbyrdes at aftale, på hvilke betingelser de vil acceptere elektronisk signerede data, bør respekteres i det omfang, national ret tillader det; elektroniske signaturer, der anvendes i sådanne systemer, bør ikke nægtes retlig gyldighed og anerkendelse som bevis under retssager;

(17) det er ikke dette direktivs mål at harmonisere national aftaleret, herunder især regler om kontraktindgåelse og -opfyldelse eller andre ikke-aftaleretlige formkrav vedrørende underskrifter: derfor bør bestemmelserne om elektroniske signaturers retsvirkninger ikke bevare formkrav til indgåelse af kontrakter eller regler til bestemmelse af, hvor en kontrakt er indgået, som er fastsat i national ret;

(18) opbevaring og kopiering af signaturgenereringsdata vil kunne udgøre en alvorlig trussel mod elektroniske signaturers juridiske gyldighed;

(19) elektroniske signaturer vil blive anvendt i den offentlige sektor inden for nationale forvaltninger og fællesskabsforvaltninger samt i kommunikationen mellem disse og med borgere og erhvervslivet, for eksempel i forbindelse med offentlige indkøb, beskatning, social sikkerhed, sundheds- og retsvæsenet;

(20) harmoniserede kriterier vedrørende retsvirkningen af elektroniske signaturer vil gøre det muligt at bevare en sammenhængende retlig ramme i hele Fællesskabet; der er i de nationale lovgivninger fastlagt forskellige krav for at anse håndskrevne underskrifter for juridisk gyldige; certifikater kan anvendes til at certificere identiteten af en person, der underskriver elektronisk; avancerede elektroniske signaturer, som er baseret på kvalificerede certifikater, tilsigter at skabe et højt sikkerhedsniveau; avancerede elektroniske signaturer, som er baseret på kvalificerede certifikater, og som er genereret af et sikkert signaturgenereringssystem, kan kun betragtes som retligt ligestillede med håndskrevne underskrifter, hvis kravene til håndskrevne underskifter er opfyldt;

(21) for at bidrage til at gøre elektroniske certificeringsmetoder almindeligt accepteret bør det sikres, at elektroniske signaturer kan anvendes som bevis ved retshandlinger i alle medlemsstater; den retlige anerkendelse af elektroniske signaturer bør hvile på objektive kriterier og ikke afhænge af den berørte certificeringstjenesteudbyders eventuelle akkreditering; fastlæggelsen af de retsområder, hvor der kan anvendes elektroniske dokumenter og elektroniske signaturer, reguleres i national lovgivning; dette direktiv indskrænker ikke nationale domstoles kompetence til at træffe afgørelse om, hvorvidt kravene i dette direktiv er overholdt, og berører ikke nationale bestemmelser om domstolenes fri bevisbedømmelse;

(22) certificeringstjenesteudbydere, der udbyder certificeringstjenester til offentligheden, er underkastet nationale erstatningsansvarsregler;

(23) udviklingen i international elektronisk handel kræver grænseoverskridende ordninger, der involverer tredjelande; for at sikre global interoperabilitet kan det være hensigtsmæssigt at indgå aftaler med tredjelande om multilaterale regler for gensidig anerkendelse af certificeringstjenester;

(24) med henblik på at øge brugernes tillid til elektronisk kommunikation og elektronisk handel skal certificeringstjenesteudbyderne overholde lovgivningen om databeskyttelse og privatlivets fred;

(25) bestemmelserne om brug af pseudonymer i certifikater bør ikke være til hinder for, at medlemsstaterne kan håndhæve krav om identifikation af personer i henhold til Fællesskabets lovgivning eller national lovgivning;

(26) de nødvendige gennemførelsesforanstaltninger til dette direktiv vedtages i overensstemmelse med Rådets afgørelse 1999/468/EF af 28. juni 1999 om fastsættelse af de nærmere vilkår for udøvelsen af de gennemførelsesbeføjelser, der tillægges Kommissionen [1];

(27) Kommissionen bør foretage en vurdering af dette direktiv to år efter dets gennemførelse bl.a. med henblik på at sikre, at hverken den teknologiske udvikling eller juridiske ændringer bliver til hinder for opfyldelsen af målene i dette direktiv; Kommissionen bør undersøge virkningerne af beslægtede tekniske områder og forelægge Europa-Parlamentet og Rådet en rapport herom;

(28) målsætningen om at skabe en harmoniseret retlig ramme for udbud af elektroniske signaturer og beslægtede tjenester kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne og kan derfor i overensstemmelse med subsidiaritets- og proportionalitetsprincipperne som omhandlet i traktatens artikel 5 bedre gennemføres af Fællesskabet; dette direktiv går ikke ud over, hvad der er nødvendigt for at nå dette mål —

UDSTEDT FØLGENDE DIREKTIV:

Artikel 1

Anvendelsesområde

Formålet med dette direktiv er at lette brugen af elektroniske signaturer og bidrage til disses retlige anerkendelse. Det fastlægger en retlig ramme for elektroniske signaturer og visse certificeringstjenester, for at det indre marked kan fungere efter hensigten.

Det omfatter ikke aspekter i forbindelse med kontrakters indgåelse og gyldighed eller andre retlige forpligtelser, som ifølge national ret eller fællesskabsret er undergivet formkrav, og det berører heller ikke de regler og begrænsninger, der efter national ret eller fællesskabsret gælder for anvendelsen af dokumenter.

Artikel 2

Definitioner

I dette direktiv forstås ved:

1) »elektronisk signatur«: data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre elektroniske data, og som anvendes som en autentifikationsmetode

2) »avanceret elektronisk signatur«: en elektronisk signatur, som opfylder følgende krav:

   a) den er entydigt knyttet til underskriveren

   b) den kan identificere underskriveren

   c) den genereres med midler, som underskriveren kan bevare den fulde kontrol med, og

   d) den er knyttet til de data, som den vedrører, på en sådan måde, at en hvilken som helst senere ændring af disse data kan opdages

3) »underskriver«: en person, der besidder et signaturgenereringssystem og handler på egne vegne eller på vegne af den fysiske eller juridiske person eller det organ, som vedkommende repræsenterer

4) »signaturgenereringsdata«: unikke data, som f.eks. koder eller private krypteringsnøgler, som anvendes af underskriveren til generering af en elektronisk signatur

5) »signaturgenereringssystem«: konfigureret software eller hardware til behandling af signaturgenereringsdata

6) »sikkert signaturgenereringssystem«: et signaturgenereringssystem, der opfylder kravene i bilag III

7) »signaturverificeringsdata«: data, som f.eks. koder eller offentlige krypteringsnøgler, der anvendes til kontrol af den elektroniske signatur

8) »signaturverificeringssystem«: konfigureret software eller hardware til behandling af signaturverificeringsdata

9) »certifikat«: en elektronisk attestering, som knytter signaturverificeringsdata til en person og bekræfter denne persons identitet

10) »kvalificeret certifikat«: et certifikat, som opfylder kravene i bilag I og leveres af en certificeringstjenesteudbyder, som opfylder kravene i bilag II

11) »certificeringstjenesteudbyder«: et organ eller en fysisk eller juridisk person, der udsteder certifikater eller leverer andre tjenesteydelser i forbindelse med elektroniske signaturer

12) »elektronisk signatur-produkt«: hardware eller software eller relevante komponenter heraf, som er beregnet til at blive brugt af en certificeringstjenesteudbyder til levering af tjenesteydelser i forbindelse med elektronisk signatur eller beregnet til at blive brugt i forbindelse med generering eller verificering af elektroniske signaturer

13) »frivillig akkreditering«: enhver tilladelse, der fastsætter rettigheder og forpligtelser, der er særlige for certificeringstjenester, og som efter anmodning fra den pågældende certificeringstjenesteudbyder tildeles denne af det offentlige eller private organ, der har til opgave at udarbejde og føre tilsyn med overholdelsen af sådanne rettigheder og forpligtelser, og hvor certificeringstjenesteudbyderen ikke er berettiget til at udøve de rettigheder, som tilladelsen giver, før denne har modtaget organets afgørelse.

[1] EFT L 184 af 17.7.1999, s. 23.

Artikel 3

Markedsadgang

1. Medlemsstaterne må ikke gøre udbud af certificeringstjenesteydelser afhængigt af forudgående autorisation.

2. Med forbehold af stk. 1 kan medlemsstaterne indføre eller opretholde frivillige akkrediteringsordninger med henblik på at højne niveauet for ydelse af certificeringstjenester. Alle vilkår i forbindelse med sådanne ordninger skal være objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende. Medlemsstaterne kan ikke af årsager, der falder ind under dette direktivs anvendelsesområde, begrænse antallet af akkrediterede certificeringstjenesteudbydere.

3. Medlemsstaterne sikrer, at der indføres et passende system til kontrol af certificeringstjenesteudbydere, der er etableret på deres område, og som udbyder kvalificerede certifikater til offentligheden.

4. Egnede offentlige eller private organer, som udpeges af medlemsstaterne, afgør, om sikre signaturgenereringssystemer opfylder kravene i bilag III. Kommissionen fastlægger efter proceduren i artikel 9 kriterier, ud fra hvilke medlemsstaterne afgør, om et organ er egnet til at blive udpeget.

Medlemsstaterne anerkender de afgørelser, som de organer, der er nævnt i første afsnit, træffer for så vidt angår opfyldelsen af kravene i bilag III.

5. Kommissionen kan efter proceduren i artikel 9 fastsætte og i *De Europæiske Fællesskabers Tidende* offentliggøre referencenumre på almindeligt anerkendte standarder for elektroniske signatur-produkter. Medlemsstaterne formoder, at et elektronisk signatur-produkt overholder kravene i bilag II, litra f), og bilag III, hvis det overholder sådanne standarder.

6. Medlemsstaterne og Kommissionen samarbejder med henblik på at fremme udviklingen og brugen af signaturverificeringssystemer på baggrund af anbefalingerne vedrørende signaturverificering i bilag IV og under hensyn til forbrugernes interesser.

7. Medlemsstaterne kan gøre anvendelse af elektroniske signaturer i den offentlige sektor afhængig af opfyldelsen af eventuelle supplerende krav. Sådanne krav skal være objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende, og må kun være affødt af den pågældende anvendelses særlige karakter. Kravene må ikke hindre grænseoverskridende tjenesteydelser til borgerne.

Artikel 4

Principper vedrørende det indre marked

1. Medlemsstaterne anvender de nationale bestemmelser, som de vedtager i henhold til dette direktiv, på certificeringstjenesteudbydere, der er etableret på deres område, og på disses tjenesteydelser. Medlemsstaterne kan ikke på områder, der er omfattet af dette direktiv, pålægge ydelse af certificeringstjenester med oprindelse i en anden medlemsstat begrænsninger.

2. Medlemsstaterne sikrer fri bevægelighed inden for det indre marked for elektroniske signatur-produkter, der overholder bestemmelserne i dette direktiv.

Artikel 5

Retsvirkninger af elektroniske signaturer

1. Medlemsstaterne sikrer, at avancerede elektroniske signaturer, der er baseret på et kvalificeret certifikat, og som er genereret af et sikkert signaturgenereringssystem,

a) opfylder retskravene til en signatur i forbindelse med data i elektronisk form, på samme måde som en håndskreven underskrift opfylder disse krav i forbindelse med papirbaserede data, og

b) kan godtages som bevismateriale under retssager.

2. Medlemsstaterne sikrer, at en elektronisk signatur ikke nægtes retlig gyldighed og anerkendelse som bevis under retssager alene af den grund, at den

— er i elektronisk form, eller

— ikke er baseret på et kvalificeret certifikat, eller

— ikke er baseret på et kvalificeret certifikat udstedt af en akkrediteret certificeringstjenesteudbyder, eller

— ikke er genereret af et sikkert signaturgenereringssystem.

Artikel 6

Erstatningsansvar

1. Medlemsstaterne sikrer som et minimum, at en certificeringstjenesteudbyder, der udsteder et certifikat som kvalificeret certifikat til offentligheden, eller som garanterer et sådant certifikat over for offentligheden, ifalder erstatningsansvar for tab, der påføres ethvert organ eller enhver fysisk eller juridisk person, som med rimelighed forlader sig på certifikatet for så vidt angår:

a) korrektheden af alle oplysningerne i det kvalificerede certifikat på udstedelsestidspunktet og certifikatets indhold af alle de for et kvalificeret certifikat foreskrevne angivelser

b) sikkerhed for, at den i det kvalificerede certifikat identificerede underskriver på udstedelsestidspunktet var i besiddelse af de signaturgenereringsdata, der svarer til de i certifikatet indeholdte eller omhandlede signaturverificeringsdata

c) sikkerhed for, at signaturgenererings- og signaturverificeringsdataene kan anvendes komplementært med hinanden i de tilfælde, hvor det er certificeringstjenesteudbyderen, der genererer begge datasæt,

medmindre certificeringstjenesteudbyderen kan bevise, at han ikke har handlet uagtsomt.

2. Medlemsstaterne sikrer som et minimum, at en certificeringstjenesteudbyder, der har udstedt et certifikat som et kvalificeret certifikat til offentligheden, er erstatningsansvarlig for tab, der påføres ethvert organ eller enhver fysisk eller juridisk person, som med rimelighed forlader sig på certifikatet, for så vidt angår manglende registrering af tilbagekaldelse af certifikatet, medmindre certificeringstjenesteudbyderen kan bevise, at han ikke har handlet uagtsomt.

3. Medlemsstaterne sikrer, at en certificeringstjenesteudbyder i et kvalificeret certifikat kan anføre begrænsninger i dette certifikats anvendelsesområde, idet disse begrænsninger skal være tydelige for tredjeparter. Certificeringstjenesteudbyderen hæfter ikke for tab, der skyldes brug af et kvalificeret certifikat, som overskrider begrænsningerne i dets anvendelsesområde.

4. Medlemsstaterne sikrer, at certificeringstjenesteudbyderen i et kvalificeret certifikat kan sætte en beløbsgrænse for de transaktioner, som certifikatet kan anvendes til, og at denne beløbsgrænse er tydelig for tredjeparter.

Certificeringstjenesteudbyderen hæfter ikke for tab, der skyldes en overskridelse af denne beløbsgrænse.

5. Stk. 1-4 berører ikke Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler [1].

Artikel 7

Internationale aspekter

1. Medlemsstaterne sikrer, at certifikater, der er udstedt som kvalificerede certifikater til offentligheden af en certificeringstjenesteudbyder, der er etableret i et tredjeland, anses for at være retligt ligestillede med certifikater, der er udstedt af en certificeringstjenesteudbyder, der er etableret inden for Fællesskabet:

a) hvis certificeringstjenesteudbyderen opfylder kravene i dette direktiv og er akkrediteret under en frivillig akkrediteringsordning i en medlemsstat, eller

b) hvis en certificeringstjenesteudbyder, der er etableret inden for Fællesskabet, og som opfylder kravene i dette direktiv, garanterer certifikatet, eller

c) hvis certifikatet eller certificeringstjenesteudbyderen er anerkendt i henhold til en bilateral eller multilateral aftale mellem Fællesskabet og tredjelande eller internationale organisationer.

2. For at lette grænseoverskridende certificeringstjenester med tredjelande og retlig anerkendelse af avancerede elektroniske signaturer med oprindelse i tredjelande fremsætter Kommissionen i givet fald forslag med henblik på den faktiske implementering af standarder og internationale aftaler om certificeringstjenester. Kommissionen forelægger, hvis det er nødvendigt, Rådet forslag til passende mandater til forhandling af bilaterale og multilaterale aftaler med tredjelande og internationale organisationer. Rådet træffer afgørelse med kvalificeret flertal.

3. Når Kommissionen underrettes om vanskeligheder, som EF-virksomheder støder på ved markedsføringen i tredjelande, kan den om nødvendigt forelægge forslag til Rådet til et passende mandat med henblik på forhandling af tilsvarende rettigheder for EF-virksomheder i disse tredjelande. Rådet træffer afgørelse med kvalificeret flertal.

Foranstaltninger, der træffes i henhold til dette stykke, berører ikke Fællesskabets og medlemsstaternes forpligtelser i henhold til relevante internationale aftaler.

Artikel 8

Databeskyttelse

1. Medlemsstaterne sikrer, at certificeringstjenesteudbyderne og de nationale akkrediterings- og tilsynsorganer opfylder kravene i Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger [2].

2. Medlemsstaterne sikrer, at den certificeringstjenesteudbyder, der udsteder certifikatet til offentligheden, kun har tilladelse til at opnå persondata direkte fra den registrerede eller med den registreredes udtrykkelige tilladelse og kun i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat. Data må ikke indsamles eller behandles til noget andet formål uden den registreredes udtrykkelige samtykke.

3. Uden at den retsvirkning, der tillægges pseudonymer i henhold til den nationale lovgivning dermed foregribes, må medlemsstaterne ikke forhindre, at certificeringstjenesteudbyderen på certifikatet anfører et pseudonym i stedet for underskriverens navn.

Artikel 9

Udvalg

1. Kommissionen bistås af et elektronisk signatur-udvalg, i det følgende benævnt »udvalget«.

2. Når der henvises til dette stykke, anvendes artikel 4 og 7 i afgørelse 1999/468/EF under overholdelse af bestemmelserne i afgørelsens artikel 8.

Den frist, der er omhandlet i artikel 4, stk. 3, i afgørelse 1999/468/EF, fastsættes til tre måneder.

3. Udvalget vedtager selv sin forretningsorden.

Artikel 10

Udvalgets hverv

Udvalget skal efter proceduren i artikel 9, stk. 2, præcisere de krav, der er fastlagt i bilagene, de kriterier, som er omhandlet i artikel 3, stk. 4, samt de alment anerkendte standarder for elektroniske signatur-produkter, der er indført og offentliggjort i henhold til artikel 3, stk. 5.

[1] EFT L 95 af 21.4.1993, s. 29.

[2] EFT L 281 af 23.11.1995, s. 31.

Artikel 11

Meddelelse

1. Medlemsstaterne meddeler Kommissionen og de øvrige medlemsstater følgende:

a) oplysninger om frivillige nationale akkrediteringsordninger, herunder alle supplerende krav i henhold til artikel 3, stk. 7

b) navn og adresse på nationale akkrediterings- og tilsynsorganer og på de organer, som er omhandlet i artikel 3, stk. 4

c) navn og adresse på alle akkrediterede nationale certificeringstjenesteudbydere.

2. Medlemsstaterne meddeler alle oplysninger i henhold til stk. 1 samt ændringer heraf så hurtigt som muligt.

Artikel 12

Revision

1. Kommissionen foretager en vurdering af, hvordan dette direktiv fungerer, og aflægger rapport herom til Europa-Parlamentet og Rådet senest den 19. juli 2003.

2. I vurderingen tages der bl.a. stilling til, om direktivets anvendelsesområde bør ændres under hensyn til den teknologiske, markedsmæssige og retlige udvikling. Rapporten skal på grundlag af de indhøstede erfaringer navnlig omfatte en bedømmelse af harmoniseringsaspekterne. Rapporten ledsages om fornødent af forslag til retsforskrifter.

Artikel 13

Gennemførelse

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv inden den 19. juli 2001. De underretter straks Kommissionen herom.

Disse love og administrative bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastlægges af medlemsstaterne.

2. Medlemsstaterne meddeler Kommissionen de væsentligste nationale retsforskrifter, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 14

Ikrafttræden

Dette direktiv træder i kraft på dagen for offentliggørelsen i *De Europæiske Fællesskabers Tidende*.

Artikel 15

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 13. december 1999.

På Europa-Parlamentets vegne	*På Rådets vegne*
N. FONTAINE	S. HASSI
Formand	*Formand*

BILAG I

Krav til kvalificerede certifikater

Kvalificerede certifikater skal indeholde:

a) angivelse af, at certifikatet er udstedt som et kvalificeret certifikat

b) den udstedende certificeringstjenesteudbyders identifikation og den stat som vedkommende er etableret i

c) underskriverens navn eller pseudonym; i sidstnævnte tilfælde skal det fremgå, at der er tale om et pseudonym

d) særlige oplysninger om underskriveren, der tilføjes, hvis det er relevant, afhængigt af formålet med certifikatet

e) de signaturverificeringsdata, som svarer til de signaturgenereringsdata, som er under underskriverens kontrol

f) certifikatets ikrafttrædelses- og udløbsdato

g) certifikatets identifikationskode

h) den udstedende certificeringstjenesteudbyders avancerede elektroniske signatur

i) eventuelle begrænsninger i certifikatets anvendelsesområde, og

j) eventuelle beløbsmæssige begrænsninger med hensyn til de transaktioner, for hvilke certifikatet kan anvendes.

BILAG II

Krav til certificeringstjenesteudbydere, der udsteder kvalificerede certifikater

Certificeringstjenesteudbydere

a) skal udvise den fornødne pålidelighed til at kunne udbyde certificeringstjenester

b) skal sørge for en hurtig og sikker katalog- og tilbagekaldelsestjeneste

c) skal sikre, at det er muligt at fastslå datoen og tidspunktet for udstedelsen eller tilbagekaldelsen af et certifikat

d) skal med hensigtsmæssige midler og i overensstemmelse med national ret kontrollere identiteten og eventuelt særlige forhold i forbindelse med de personer, til hvem der udstedes kvalificerede certifikater

e) skal beskæftige personale med den ekspertviden og de erfaringer og kvalifikationer, som de tilbudte tjenesteydelser kræver, navnlig ledelseskompetence, sagkundskab inden for elektronisk signaturteknologi og indgående kendskab til korrekte sikkerhedsprocedurer; de skal også anvende adækvate administrative og ledelsesmæssige procedurer, som overholder anerkendte standarder

f) skal anvende pålidelige systemer og produkter, som er beskyttet mod ændringer, og som garanterer de af disse systemer og produkter understøttede processers tekniske og kryptografiske sikkerhed

g) skal træffe foranstaltninger imod forfalskning af certifikater, og, hvis certificeringstjenesteyderen genererer signaturgenereringsdata, garantere disse datas fortrolighed under genereringsprocessen

h) skal til stadighed have tilstrækkelige økonomiske ressourcer til at drive virksomheden i overensstemmelse med dette direktivs krav, navnlig til at bære erstatningsansvaret, f.eks. ved at tegne en passende forsikring

i) skal registrere alle relevante oplysninger om kvalificerede certifikater i en rimelig periode, navnlig for at kunne fremlægge bevis for certificering, når det er påkrævet i retssager. Denne registrering kan ske elektronisk

j) må ikke opbevare eller kopiere de personers signaturgenereringsdata, som certificeringstjenesteyderen har tilbudt nøglehåndteringstjenester

k) skal, inden de indgår i et kontraktforhold med en person, der søger at opnå et certifikat fra dem til støtte for sin elektroniske signatur, gennem et bestandigt kommunikationsmedium underrette denne person om de nøjagtige vilkår for anvendelsen af certifikatet, herunder eventuelle begrænsninger i brugen heraf, eksistensen af en eventuel frivillig akkrediteringsordning og procedurer for klager og bilæggelse af tvister. Sådanne oplysninger, som kan sendes elektronisk, skal gives skriftligt og i et umiddelbart forståeligt sprog. De relevante dele af disse oplysninger skal efter anmodning også stilles til rådighed for tredjemand, der forlader sig på certifikatet

l) skal benytte pålidelige systemer til opbevaring af certifikater i verificerbar form, således at

— kun bemyndigede personer kan foretage tilføjelser og ændringer

— oplysningernes ægthed kan kontrolleres

— certifikaterne kun er offentligt tilgængelige i de tilfælde, hvor indehaveren har givet sit samtykke, og

— eventuelle tekniske ændringer, som bringer disse sikkerhedskrav i fare, er synlige for operatøren.

BILAG III

Krav til sikre elektroniske signaturgenereringssystemer

1. Sikre signaturgenereringssystemer skal ved hjælp af passende og tekniske og proceduremæssige midler i det mindste sikre, at:

   a) signaturgenereringsdata, der anvendes til signaturgenerering, i praksis kun kan fremtræde én gang, og at de med rimelig sikkerhed forbliver hemmelige

   b) signaturgenereringsdata, der anvendes til signaturgenerering, med rimelig sikkerhed ikke kan udledes, og at signaturen er beskyttet mod forfalskning under anvendelse af eksisterende teknologi

   c) signaturgenereringsdata, der anvendes til signaturgenerering, på pålidelig vis kan beskyttes af den retmæssige underskriver mod andres brug.

2. Sikre signaturgenereringssystemer må ikke ændre de data, som skal underskrives, eller hindre, at disse data vises for underskriveren forud for signaturprocessen.

BILAG IV

Anbefalinger vedrørende signaturverificering

I løbet af signaturverificeringsprocessen bør der skabes rimelig sikkerhed for, at:

a) de data, der anvendes til verificering af signaturen, svarer til de data, som vises kontrolløren

b) signaturen verificeres på pålidelig vis, og at resultatet af denne verificering vises korrekt

c) kontrolløren om nødvendigt på pålidelig vis kan fastslå indholdet af de underskrevne data

d) certifikatets ægthed og gyldighed, som kræves på tidspunktet for signaturverificeringen, verificeres på pålidelig vis

e) resultatet af verificeringen og underskriverens identitet vises på korrekt vis

f) anvendelsen af pseudonym klart fremgår

g) eventuelle sikkerhedsrelevante ændringer kan spores.

BILAG 2

Lov om elektroniske signaturer[1)]

VI MARGRETHE DEN ANDEN, af Guds Nåde Danmarks Dronning, gør vitterligt:

Folketinget har vedtaget og Vi ved Vort samtykke stadfæstet følgende lov:

Kapitel 1

Formål og anvendelsesområde

§ 1. Lovens formål er at fremme en sikker og effektiv anvendelse af elektronisk kommunikation gennem fastsættelse af krav til visse elektroniske signaturer og til nøglecentre, der udsteder certifikater til elektroniske signaturer.

§ 2. Loven finder anvendelse på nøglecentre etableret i Danmark, der udsteder kvalificerede certifikater til offentligheden, jf. dog § 12.

Stk. 2. Loven finder desuden anvendelse på efterprøvelse af, at signaturgenereringssystemer overholder de opstillede krav til sikre signaturgenereringssystemer.

Kapitel 2

Definitioner

§ 3. I denne lov forstås ved:

1) Elektronisk signatur: Data i elektronisk form, der knyttes til andre elektroniske data ved hjælp af et signaturgenereringssystem, og som anvendes til at kontrollere, at disse data stammer fra den person, der er angivet som underskriver, og at de ikke er blevet ændret.
2) Avanceret elektronisk signatur: En elektronisk signatur, der
   a) entydigt er knyttet til underskriveren,
   b) gør det muligt at identificere underskriveren,
   c) skabes med midler, som kun underskriveren har kontrol over, og som
   d) er knyttet til de data, den vedrører på en sådan måde, at enhver efterfølgende ændring af disse data kan opdages.
3) Underskriver: En fysisk person, der besidder et signaturgenereringssystem og handler på egne vegne eller på vegne af en anden fysisk eller juridisk person.
4) Signaturgenereringsdata: Unikke data, som for eksempel en kode eller en privat krypteringsnøgle, som anvendes til at fremstille en elektronisk signatur.
5) Signaturgenereringssystem: Et software- eller hardwarebaseret system til behandling og opbevaring af signaturgenereringsdata.
6) Signaturverificeringsdata: Unikke data, som for eksempel en kode eller en offentlig krypteringsnøgle, som anvendes til at verificere en elektronisk signatur.
7) Signaturverificeringssystem: Et software- eller hardwarebaseret system til behandling af signaturverificeringsdata.
8) Certifikat: En elektronisk attest, som knytter bestemte signaturverificeringsdata til underskriveren og bekræfter dennes identitet.
9) Nøglecenter: En fysisk eller juridisk person, der udsteder certifikater.

[1)] Loven indeholder bestemmelser, der gennemfører Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EF-Tidende 2000 nr. L 13, s. 12).

Forskningsmin., j.nr. ITR 4843

AF000162

J. H. Schultz Grafisk A/S

Kapitel 3

Kvalificerede certifikater

§ 4. Betegnelsen kvalificerede certifikater eller betegnelser, der er egnede til at fremkalde det indtryk, at der er tale om kvalificerede certifikater, må kun anvendes om certifikater, der opfylder de i stk. 2 og 3 nævnte krav, og som udstedes af et nøglecenter, der opfylder bestemmelserne i kapitel 4 samt regler fastsat i medfør heraf.

Stk. 2. Et kvalificeret certifikat skal indeholde:

1) En angivelse af, at certifikatet er udstedt som et kvalificeret certifikat.
2) Nøglecentrets navn og hjemsted.
3) Underskriverens navn eller pseudonym med angivelse af, at der er tale om et pseudonym.
4) Eventuelle yderligere oplysninger om underskriveren, for så vidt det er nødvendigt for anvendelsen af certifikatet, herunder oplysninger, der sikrer en entydig identifikation af underskriveren.
5) Certifikatets gyldighedsperiode.
6) En tydelig angivelse af eventuelle begrænsninger i certifikatets anvendelsesområde (formålsbegrænsninger).
7) En tydelig angivelse af eventuelle begrænsninger med hensyn til de transaktionsbeløb, certifikatet kan anvendes til (beløbsbegrænsninger).
8) Certifikatets identifikationskode.
9) De signaturverificeringsdata, der svarer til de signaturgenereringsdata, som var under underskriverens kontrol på udstedelsestidspunktet.

Stk. 3. Et kvalificeret certifikat skal være underskrevet med nøglecentrets avancerede elektroniske signatur.

Kapitel 4

Krav til nøglecentres virksomhed

§ 5. Et nøglecenter skal træffe de foranstaltninger, som er nødvendige for et sikkert, pålideligt og velfungerende udbud af kvalificerede certifikater. Nøglecentret skal herunder

1) anvende betryggende administrative og ledelsesmæssige procedurer, som overholder anerkendte standarder,
2) beskæftige personale med den fornødne ekspertise, erfaring og kvalifikationer, herunder personale med sagkundskab inden for elektronisk signaturteknologi og indgående kendskab til korrekte sikkerhedsprocedurer i forbindelse hermed,
3) anvende pålidelige systemer og produkter, som er beskyttet imod uautoriserede ændringer, og som sikrer den tekniske og kryptografiske sikkerhed af de processer, som disse systemer og produkter understøtter,
4) træffe foranstaltninger mod eventuelle muligheder for forfalskning af certifikaterne og
5) til stadighed have tilstrækkelige økonomiske ressourcer til at drive virksomhed i overensstemmelse med bestemmelserne i denne lov, herunder til at opfylde erstatningsmæssige forpligtelser i henhold til loven.

Stk. 2. Nøglecentre, der udsteder kvalificerede certifikater, skal vælge en ekstern statsautoriseret revisor til varetagelse af systemrevisionen i nøglecentret. Telestyrelsen kan i særlige tilfælde dispensere fra kravet om, at systemrevisor skal være statsautoriseret revisor.

Stk. 3. Forskningsministeren fastsætter nærmere regler om kravene i stk. 1.

§ 6. Nøglecentre skal fastsætte og anvende betryggende procedurer til at kontrollere identiteten og andre forhold vedrørende underskriveren forud for udstedelsen af certifikatet.

Stk. 2. Oplysninger om procedurerne som nævnt i stk. 1 skal være offentligt tilgængelige.

Stk. 3. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1 og 2.

§ 7. Et nøglecenter skal ved udstedelse af et kvalificeret certifikat sikre, at underskriveren på tidspunktet for udstedelsen er i besiddelse af de signaturgenereringsdata, som korresponderer med de signaturverificeringsdata, der er indeholdt i certifikatet.

Stk. 2. Ved udstedelse af kvalificerede certifikater, hvor det er nøglecentret, der leverer signaturgenereringsdata og signaturverificeringsdata, må der kun anvendes signaturgenereringsdata og signaturverificeringsdata, som hører sammen på en unik måde. Nøglecentret skal sikre signaturgenereringsdataenes fortrolighed under genereringsprocessen.

Stk. 3. Et nøglecenter skal fastlægge procedurer for udstedelse af certifikater, der gør det muligt at fastslå dato og tidspunkt for udstedelsen.

§ 8. Ved indgåelse af en aftale om udstedelse af et kvalificeret certifikat skal nøglecentret skriftligt oplyse underskriveren om:

1) Vilkårene for anvendelsen af certifikatet, herunder eventuelle formåls- eller beløbsbegrænsninger.
2) Eventuelle krav til underskriverens opbevaring og beskyttelse af signaturgenereringsdataene.
3) Underskriverens omkostninger ved erhvervelse og anvendelse af certifikatet og brug af nøglecentrets øvrige tjenester.
4) Hvorvidt nøglecentret er tilknyttet en frivillig akkrediteringsordning.
5) Procedurer for behandling af klager og bilæggelse af tvister.

Stk. 2. Kontraktsvilkårene kan afgives elektronisk, forudsat at det sker i en for modtageren umiddelbart læsbar form.

Stk. 3. De relevante dele af de i stk. 1 nævnte oplysninger skal på anmodning stilles til rådighed for tredjemand, der forlader sig på et kvalificeret certifikat.

Stk. 4. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1-3.

§ 9. Nøglecentre skal sørge for en hurtig og sikker katalog- og tilbagekaldelsestjeneste, som giver mulighed for, at det kan undersøges, om et kvalificeret certifikat er spærret, hvilken gyldighedsperiode certifikatet har, og om certifikatet indeholder formåls- eller beløbsbegrænsninger.

Stk. 2. Et nøglecenter skal spærre et certifikat straks efter at have modtaget anmodning fra underskriveren herom, eller hvis forholdene i øvrigt tilsiger dette.

Stk. 3. Oplysninger efter stk. 1 skal være umiddelbart tilgængelige.

Stk. 4. Et kvalificeret certifikat må kun gøres offentligt tilgængeligt, hvis underskriveren har givet samtykke hertil.

Stk. 5. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1-3.

§ 10. Et nøglecenter skal registrere og opbevare alle relevante oplysninger om certifikaterne i en rimelig periode, dog mindst seks år.

Stk. 2. Et nøglecenter skal benytte pålidelige systemer til opbevaring af certifikater i verificerbar form.

Stk. 3. Nøglecentre må ikke opbevare eller kopiere de personers signaturgenereringsdata, som nøglecentret gennem udstedelsen af certifikater måtte have fået kendskab til.

Stk. 4. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1 og 2.

Kapitel 5

Erstatningsansvar

§ 11. Nøglecentre, der udsteder kvalificerede certifikater til offentligheden, eller som over for offentligheden indestår for sådanne certifikater udstedt af et andet nøglecenter, er ansvarlig for tab hos den, der med rimelighed forlader sig på certifikatet, såfremt tabet skyldes,

1) at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet,
2) at certifikatet ikke indeholder alle oplysninger som krævet i henhold til § 4,
3) manglende spærring af certifikatet, jf. § 9, stk. 2,
4) manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. § 9, stk. 1 og 3, eller
5) tilsidesættelse af § 7.

Stk. 2. Et nøglecenter pådrager sig erstatningsansvar efter stk. 1, medmindre nøglecentret kan godtgøre, at nøglecentret ikke har handlet uagtsomt eller forsætligt.

Stk. 3. Et nøglecenter er ikke ansvarlig for

1) tab opstået som følge af anvendelse af et kvalificeret certifikat uden for de formålsbegrænsninger, som gælder for certifikatet, eller for
2) tab opstået som følge af en overskridelse af de beløbsbegrænsninger, som gælder for certifikatet,

forudsat at de pågældende begrænsninger tydeligt fremgår af certifikatet, jf. § 4, og på forespørgsel oplyses, jf. 9, stk. 1 og 3.

Stk. 4. Stk. 1-3 kan ikke ved forudgående aftale fraviges til skade for skadelidte.

Stk. 5. Stk. 1-3 finder ikke anvendelse, i det omfang tabet dækkes efter lov om visse betalingsmidler.

Kapitel 6

Supplerende krav til behandling af personoplysninger

§ 12. Et nøglecenter må kun indsamle personoplysninger i forbindelse med nøglecentervirksomheden direkte fra den registrerede eller med den registreredes udtrykkelige samtykke og kun i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat.

Stk. 2. Personoplysninger indsamlet i medfør af stk. 1 må ikke behandles eller videregives til andet formål end nævnt i stk. 1 uden den registreredes udtrykkelige samtykke hertil.

Kapitel 7

Elektronisk signatur og formkrav

§ 13. Bestemmelser i lovgivningen, hvorefter elektroniske meddelelser skal være forsynet med signatur, skal anses for opfyldt, hvis meddelelsen er forsynet med en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat, og som er fremstillet ved brug af et sikkert signaturgenereringssystem. Ved elektroniske meddelelser til og fra en offentlig myndighed gælder dette dog kun, såfremt andet ikke følger af lov eller bestemmelser fastsat i medfør af lov.

Kapitel 8

Sikre signaturgenereringssystemer

§ 14. Ved et sikkert signaturgenereringssystem forstås et signaturgenereringssystem, der ved hjælp af procedurer og tekniske midler sikrer, at signaturgenereringsdata, der anvendes til at skabe en elektronisk signatur,

1) i praksis kun kan fremtræde en gang,
2) med rimelig sikkerhed forbliver hemmelige og ikke kan udledes,
3) er beskyttet mod forfalskning og
4) på pålidelig vis kan beskyttes af underskriveren mod andres uretmæssige brug.

Stk. 2. Et sikkert signaturgenereringssystem må ikke indrettes således, at det ændrer de data, som en elektronisk signatur knyttes til, eller hindrer, at disse data forevises for underskriveren forud for signeringen.

Stk. 3. De i stk. 1 og 2 nævnte krav skal anses for opfyldt, såfremt et signaturgenereringssystem overholder almindeligt anerkendte standarder for sådanne systemer, som Kommissionen har fastsat og offentliggjort i EF-Tidende i overensstemmelse med proceduren i artikel 9 i Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer.

§ 15. Forskningsministeren udpeger et eller flere egnede organer eller myndigheder, som kan medvirke til at efterprøve, om signaturgenereringssystemer opfylder kravene til sikre signaturgenereringssystemer, jf. § 14, stk. 1 og 2, og fastsætter nærmere regler om procedurerne for denne efterprøvelse samt om betaling af gebyr for efterprøvelsen.

Stk. 2. Et signaturgenereringssystem, der betegnes som et sikkert signaturgenereringssystem, må først markedsføres eller anvendes til at fremstille avancerede elektroniske signaturer, der er baseret på et kvalificeret certifikat, når det er blevet efterprøvet, jf. stk. 1.

Stk. 3. Med en efterprøvelse efter stk. 1 ligestilles en efterprøvelse af et sikkert signaturgenereringssystem foretaget af et organ eller en myndighed i et andet land inden for Det Europæiske Økonomiske Samarbejde (EØS).

Kapitel 9

Tilsyn

§ 16. Nøglecentre skal senest samtidig med, at udstedelse af kvalificerede certifikater påbegyndes, foretage anmeldelse til Telestyrelsen.

Stk. 2. Anmeldelsen skal indeholde oplysning om

1) nøglecentrets navn og hjemsted,
2) selskabsform, såfremt nøglecentret drives som selskab,
3) nøglecentrets ledelse og systemrevisor.

Stk. 3. Ændringer i forhold, der er anmeldt i henhold til stk. 2, skal anmeldes inden 8 dage efter, at ændringen er sket.

Stk. 4. Telestyrelsen kan fastsætte nærmere regler om, hvilke yderligere oplysninger anmeldelsen skal indeholde.

§ 17. Nøglecentret skal samtidig med anmeldelse efter § 16 indsende en rapport til Telestyrelsen.

Stk. 2. Rapporten skal indeholde

1) en beskrivelse af nøglecentrets virksomhed og systemer,
2) en erklæring fra nøglecentrets ledelse om, hvorvidt nøglecentrets samlede data-, system- og driftssikkerhed må anses for betryggende og i overensstemmelse med denne lovs regler samt regler fastsat i medfør heraf, og
3) en erklæring fra systemrevisor, jf. § 5, stk. 2, om, hvorvidt nøglecentrets samlede data-, system- og driftssikkerhed efter systemrevisors opfattelse må anses for betryggende og i overensstemmelse med denne lovs regler samt regler fastsat i medfør heraf.

Stk. 3. Nøglecentret skal årligt udarbejde en opdateret rapport. Telestyrelsen fastsætter en

frist for, hvornår rapporten senest skal indsendes til Telestyrelsen.

Stk. 4. Telestyrelsen kan fastsætte nærmere regler vedrørende indholdet af nøglecentrets rapporter samt om systemrevisionens gennemførelse i nøglecentre.

§ 18. Telestyrelsen påser overholdelsen af denne lov og bestemmelser udstedt i medfør af loven.

Stk. 2. Telestyrelsen kan påbyde et nøglecenter at

1) foretage anmeldelse til Telestyrelsen, jf. § 16,
2) indsende rapporter til Telestyrelsen, jf. § 17,
3) bringe forhold vedrørende nøglecentrets virksomhed i overensstemmelse med loven eller bestemmelser udstedt i medfør af loven.

Stk. 3. Telestyrelsen fastsætter en tidsfrist for opfyldelse af påbud efter stk. 2.

Stk. 4. Telestyrelsen kan pålægge et nøglecenter tvangsbøder med henblik på at gennemtvinge påbud efter stk. 2, § 19, stk. 1, eller § 20.

Stk. 5. Telestyrelsen kan kræve, at der gennemføres en ekstraordinær systemrevision af et nøglecenter. Telestyrelsen udpeger den systemrevisor, som skal udføre den ekstraordinære systemrevision. Nøglecentret kan pålægges at betale for den ekstraordinære systemrevisions udførelse.

Stk. 6. Telestyrelsen kan fratage et nøglecenter retten til at anvende betegnelsen kvalificerede certifikater, jf. § 4, hvis nøglecentret

1) trods pålæg af tvangsbøder undlader at efterkomme Telestyrelsens påbud efter stk. 2, § 19, stk. 1, eller § 20,
2) groft eller i gentagne tilfælde har overtrådt lovens regler eller regler fastsat i medfør heraf eller
3) anmelder betalingsstandsning eller kommer under konkurs.

Stk. 7. Telestyrelsens afgørelse efter stk. 6 kan af nøglecentret forlanges indbragt for domstolene. Anmodning herom skal være modtaget i Telestyrelsen senest 4 uger efter, at afgørelsen er blevet meddelt nøglecentret. Telestyrelsen anlægger sag mod nøglecentret efter reglerne i den borgerlige retsplejes former.

Stk. 8. Anmodning om sagsanlæg har ikke opsættende virkning, men retten kan ved kendelse bestemme, at det pågældende nøglecenter under sagens behandling skal have adgang til at udstede kvalificerede certifikater. Ankes en dom, hvorved fratagelsen af adgangen til at udstede kvalificerede certifikater ikke findes lovlig, kan den ret, der har afsagt dommen, eller den ret, hvortil sagen er indbragt, bestemme, at nøglecentret ikke må udstede kvalificerede certifikater under ankesagens behandling.

§ 19. Telestyrelsen kan af nøglecentre kræve meddelt alle oplysninger, som findes nødvendige for tilsynet efter § 18, herunder til afgørelse af, om en fysisk eller juridisk person er omfattet af dette tilsyn.

Stk. 2. Nøglecentret og systemrevisor skal straks meddele Telestyrelsen oplysning om forhold, der er af afgørende betydning for nøglecentrets fortsatte virksomhed.

§ 20. Telestyrelsen kan pålægge nøglecentret inden for en fastsat frist at vælge en ny systemrevisor, jf. § 5, stk. 2, såfremt den fungerende systemrevisor findes åbenbart uegnet til sit hverv.

Stk. 2. Telestyrelsen kan pålægge systemrevisor at give oplysninger om nøglecentrets forhold uden accept fra nøglecentret.

Stk. 3. Ved revisorskifte skal nøglecentret og den eller de fratrådte systemrevisorer hver især give Telestyrelsen en redegørelse. Telestyrelsen kan give påbud om at efterkomme 1. pkt.

§ 21. Telestyrelsens afgørelser efter denne lov eller bestemmelser, der er fastsat i medfør heraf, kan ikke indbringes for anden administrativ myndighed.

§ 22. Forskningsministeren kan fastsætte regler om, at udgifterne ved Telestyrelsens tilsyn afholdes af de nøglecentre, der udsteder kvalificerede certifikater.

Kapitel 10

Internationale forhold

§ 23. Kvalificerede certifikater udstedt af et nøglecenter etableret i et land uden for Det Europæiske Økonomiske Samarbejde (EØS), skal anerkendes på samme måde som kvalificerede certifikater udstedt af nøglecentre etableret i et land inden for Det Europæiske Økonomiske Samarbejde (EØS) såfremt

1) nøglecentret opfylder kravene i denne lov og er tilsluttet en frivillig akkrediteringsordning i en medlemsstat eller

2) et nøglecenter etableret i en medlemsstat, der opfylder kravene i denne lov, indestår for certifikater udstedt af det pågældende nøglecenter eller
3) certifikatet eller nøglecentret er anerkendt i henhold til en bilateral eller multilateral aftale mellem Fællesskabet og tredjelande eller internationale organisationer.

Kapitel 11

Strafansvar

§ 24. Medmindre strengere straf er forskyldt efter anden lovgivning, straffes med bøde den, der
1) overtræder § 9, stk. 4, § 10, stk. 3, § 12 eller § 15, stk. 2,
2) afgiver urigtige eller vildledende oplysninger til Telestyrelsen eller
3) overtræder påbud eller afgørelser fra Telestyrelsen i medfør af § 18, stk. 2 og 6, og § 19, stk. 1.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Stk. 3. Forældelsesfristen for strafansvar efter stk. 1 og 2 er 5 år.

Kapitel 12

Ikrafttrædelse m.v.

§ 25. Loven træder i kraft den 1. oktober 2000.

§ 26. Loven gælder ikke for Grønland og Færøerne, men kan ved kongelig anordning sættes i kraft for disse landsdele med de afvigelser, som de særlige grønlandske og færøske forhold tilsiger.

Givet på Christiansborg Slot, den 31. maj 2000

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Birte Weiss

BILAG 3

Certifikatpolitik for OCES-personcertifikater (Offentlige Certifikater til Elektronisk Service)

Indholdsfortegnelse

Rettigheder

IT- og Telestyrelsen har alle rettigheder til denne Certifikatpolitik (CP), OCES-navnet og OCES-OID. Brug af betegnelsen OCES-OID i certifikater og udstedelse af OCES certifikater er kun tilladt efter skriftlig aftale med IT- og Telestyrelsen.

Forord

Denne certifikatpolitik er udarbejdet af og administreres af IT- og Telestyrelsen i Danmark.

IT- og Telestyrelsen er den offentlige myndighed, som bemyndiger udstedelsen af OCES-personcertifikater til de udvalgte certificeringscentre (CA'er), og som står for godkendelse af CA'erne i forhold til denne CP.

IT- og Telestyrelsen er tillige ansvarlig for indholdet af denne CP. Den seneste version af denne CP samt tidligere versioner af denne, hvorefter der fortsat eksisterer gyldige certifikater, findes på www.signatursekretariatet.dk.
Henvendelse i øvrigt vedrørende digital signatur til IT- og Telestyrelsen. Se nærmere www.digitalsignatur.dk.

Introduktion

En digital signatur er en elektronisk underskrift, som bl.a. kan bruges, når det er væsentligt at vide, hvem man kommunikerer med elektronisk. Anvendelsen af digital signatur forudsætter, at der er etableret en offentlig nøgleinfrastruktur (PKI).

OCES udgør en sådan offentlig nøgleinfrastruktur. OCES er betegnelsen for Offentlige Certifikater til Elektronisk Service. IT- og Telestyrelsen har udarbejdet tre OCES-certifikatpolitikker (CP'er), en for henholdsvis person-, medarbejder- og virksomhedscertifikater. CP'erne udgør en fælles offentlig standard, der regulerer udstedelsen og anvendelsen af den digitale OCES signatur. CP'erne fastsætter således krav til nøgleinfrastrukturen og herigennem sikkerhedsniveauet for den digitale signatur

Den digitale signatur kan anvendes, når en person er blevet identificeret og registreret hos et certificeringscenter (CA). CA tildeler et personligt elektronisk certifikat, indeholdende personens offentlige nøgle. Desuden sørger CA for, at den nødvendige software, herunder den private nøgle, kan installeres på personens PC. CP'en stiller krav til, hvorledes og under hvilke vilkår, CA skal udføre disse opgaver.

Herudover findes kvalificerede certifikater udstedt i medfør af lov nr. 417 af 31. maj 2000 om elektroniske signaturer. Et kvalificeret certifikat bygger ikke på den oven for nævnte fælles offentlige standard. Der kræves bl.a. personligt fremmøde i forbindelse med udstedelsen af et kvalificeret certifikat.

1 Oversigt og formål

Denne certifikatpolitik (CP) beskriver de retningslinjer, der gælder for udstedelsen af et OCES-personcertifikat, hvor OCES er en forkortelse for Offentlige Certifikater til Elektronisk Service.

CP'en er udarbejdet med udgangspunkt i de retningslinjer, som er angivet i ETSI TS 102 042 v 1.1.1. (2002-04) "*Policy requirements for certification authorities issuing public key certificates*".

Et personcertifikat garanterer, at certifikatindehaveren har den identitet, der fremgår af certifikatet.

Et certifikat er kun et OCES-certifikat, hvis det er udstedt efter en OCES CP og er udstedt af et certificeringscenter (CA), som er godkendt af IT- og Telestyrelsen som udsteder af OCES-personcertifikater.

En CP er en del af aftalegrundlaget mellem IT- og Telestyrelsen og det enkelte certificeringscenter (CA) om ret til udstedelse af OCES-certifikater.

CP'en angiver en række betingelser, som CA skal opfylde for at opnå og bevare retten til udstedelse af OCES-certifikater.

Hovedprincippet for CP'en er således, at den udarbejdes af den for området hovedansvarlige offentlige myndighed, IT- og Telestyrelsen, og angiver styrelsens minimumskrav til de systemer og aftaler, som certificeringscentrene (CA'erne), som de kommercielle udbydere af certifikater, skal opfylde i forhold til deres "kunder", certifikatindehavere og signaturmodtagere, idet formålet er, at certifikatpolitikken skal sikre, at signaturerne kan bruges på en for alle parter betryggende måde.

Denne CP stiller ikke krav om krydscertificering og uafhængig tidsstemplings-tjeneste.

2 Referencer

Opmærksomheden henledes på de nuværende regler:

LOV nr. 417 af 31/05/2000: *Lov om elektroniske signaturer*

LOV nr. 429 af 31/05/2000: *Lov om behandling af personoplysninger*

CEN Workshop Agreement 14167-2:2002: "*Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – part 2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)*"

DS 2391:1995 *"Registrering af identifikatorer I datanetværk"*, del 1 og 3

DS 844: *"Specifikation for kvalificerede certifikater"*

ETSI TS 102 042 v 1.1.1. (2002-04): *"Policy requirements for certification authorities issuing public key certificates"*

ETSI SR 002 176 v 1.1.1. (2003-03): *"Algorithms and Parameters for Secure Electronic Signatures"*

FIPS PUB 140-1: "*Security Requirements for Cryptographic Modules*"

ISO/IEC 15408 (del 1 til 3): "*Information technology - Security techniques - Evaluation criteria for IT security*"

ISO/IEC 9794-8/ITU-T Recommendation X.509: "*Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*"

Såfremt der måtte være uoverensstemmelse mellem tekniske dokumenter eller standarder og denne CP, finder CP'ens bestemmelser anvendelse for CA.

3 Definitioner og forkortelser

3.1 Definitioner

Dette afsnit giver en definition af de specielle termer, som anvendes i denne CP. Engelske termer er angivet i parentes.

certifikat ("public key certificate"): En elektronisk attest, som angiver certifikatindehaverens offentlige nøgle sammen med supplerende information, og som entydigt knytter den offentlige nøgle til identifikation af certifikatindehaveren. Et certifikat skal signeres af et certificeringscenter (CA), som derved bekræfter certifikatets gyldighed.

certifikatindehaver ("subscriber"): En fysisk person, der indgår aftale med det udstedende certificeringscenter (CA), og til hvem et OCES certifikat enten er under udstedelse eller er blevet udstedt.

certificeringscenter ("certification authority" - "CA"): En fysisk eller juridisk person, der er bemyndiget til at generere, signere og udstede certifikater.[1]

certificeringspraksis ("Certification Practice Statement" – "CPS"): En specifikation af, hvilke principper og procedurer, en CA anvender ved udstedelse af certifikater.

certifikatpolitik ("certificate policy"): Et sæt regler, der angiver krav til udstedelse og brug af certifikat i en eller flere specifikke sammenhæng, hvor der findes fælles sikkerhedskrav.

digital signatur: Data i en elektronisk form, som anvendes til autentificering af andre elektroniske data, som den digitale signatur er vedhæftet eller logisk tilknyttet.

kryptografisk modul: Hardwareenhed, som uafhængigt af styresystemet kan generere og opbevare nøgler og anvende den digitale signatur.

offentligt certifikat ("public-key certificate"): Se certifikat.

registreringsenhed ("registration authority" –"RA"): Den fysiske eller juridiske person, der er ansvarlig for identifikation og autentifikation af en (kommende) certifikatindehaver.

rodcertifikat ("root certificate"): Et certifikat udstedt af en CA til brug for validering af andre certifikater. Et rodcertifikat er signeret med sin egen signeringsnøgle (egensignering ("self signing")).

rodnøgle: rodcertifikatets signeringsnøgle (private nøgle).

[1] I lov om elektroniske signaturer benyttes betegnelsen nøglecenter for denne enhed. Det er dog fundet mest praktisk at ændre terminologien. Et certificeringscenter svarer til et nøglecenter i lov om elektroniske signaturer, bortset fra at certificeringscenteret ikke udsteder kvalificerede certifikater, men OCES-certifikater.

signaturmodtager ("verifier"): En fysisk eller juridisk person, der modtager signerede data fra en certifikatindehaver.

spærreliste ("Certificate Revocation List"): En liste over certifikater, som ikke længere anses for gyldige, fordi de er permanent spærret.

3.2 Forkortelser

CA Certificeringscenter ("Certificate Authority")
CRL Spærreliste ("Certificate Revocation List")
CPR Det Centrale Person Register
CPS Certificeringspraksis ("Certification Practice Statement")
CP Certifikatpolitik ("Certificate Policy")
LDAP "Lightweight Directory Access Protocol"
OCES Offentlige Certifikater til Elektronisk Service
OCSP "Online Certificate Status Protocol"
PID Personspecifikt Identifikationsnummer
PKI "Public Key Infrastructure"
RA "Registration Authority"
UTC Fælles tidsangivelse ("Universal Time Coordinate")

3.3 Notation

Kravene anført i denne CP omfatter:

1 Obligatoriske krav, der skal opfyldes. Disse krav er anført med "skal"
2 Krav, der bør opfyldes. Opfyldes kravene ikke, skal der gives begrundelse herfor. Disse krav er anført med ”bør”
3 Krav, der kan opfyldes, hvis CA ønsker det. Disse krav er anført med "kan"

4 Koncept

En Public Key Infrastruktur (PKI) benyttes til udveksling af information mellem to parter på internettet, hvor en fælles betroet tredjepart står inde for underskriverens identitet. En certifikatpolitik beskriver forholdet mellem disse tre parter.

Hovedprincippet for certifikatpolitikken er, som anført under pkt. 1, at den udarbejdes af den for området hovedansvarlige offentlige myndighed, IT- og Telestyrelsen. Certifikatpolitikken angiver styrelsens minimumskrav til de systemer og aftaler, certificeringscentrene (CA'erne), som kommercielle udbydere af certifikater, skal opfylde i forhold til deres "kunder", certifikatindehavere og signaturmodtagere. Certifikatpolitikken skal sikre, at signaturerne kan bruges på en for alle parter betryggende måde. Certifikatindehavernes og signaturmodtagernes tillid skal således kunne baseres på IT- og Telestyrelsens godkendelse af CA'erne.

4.1 CA

En fysisk eller juridisk person, der er betroet af både certifikatindehavere og signaturmodtagere til at udstede, underskrive og administrere elektroniske certifikater, kaldes et certificeringscenter (CA). CA har det overordnede ansvar for tilvejebringelsen af de tjenester, der er nødvendige for at udstede og vedligeholde certifikater. Det er CA's egne private nøgler, der benyttes til at underskrive udstedte certifikater, ligesom CA er identificeret i certifikatet som udsteder.

CA kan samarbejde med andre parter for at tilbyde de nødvendige tjenester, men CA har altid det overordnede ansvar for alle handlinger vedrørende håndtering af certifikater, ligesom CA er ansvarlig for, at kravene i denne CP til CA's tjenester altid er overholdt.

En OCES CA er øverst i tillidshierarkiet. Derfor vil OCES certifikater være signeret med en signeringsnøgle, som er selvsigneret, det vil sige rodnøglen i dette tillidshierarki.

4.2 CA-tjenester

De nødvendige tjenester for at udstede og vedligeholde certifikater kan opdeles i følgende:

- Registrering: Verificering af certifikatindehaverens identitet og eventuelle andre attributter. Resultatet af registreringen overgives til certifikatgenereringen
- Certifikatgenerering: Generering og elektronisk signering af certifikater baseret på den verificerede identitet og eventuelle andre attributter fra registreringen
- Certifikatdistribution: Distribution af certifikater til certifikatindehaver
- Katalogtjeneste: Offentliggørelse af certifikater, så signaturmodtagere kan få adgang til certifikaterne
- Publikation af forretningsbetingelser: Offentliggørelse af betingelser og regler, herunder CP og CPS

- Spærring af certifikater: Modtagelse og behandling af anmodninger om spærring af certifikater
- Publikation af spærreinformation: Offentliggørelse af statusinformation for alle certifikater, specielt certifikater, der er spærret. Denne tjeneste skal være så realtidsnær som muligt

4.3 CP og CPS

4.3.1 Formål

Formålet med en CP som nærværende er at angive, hvilke krav der skal leves op til, mens formålet med en CPS er at angive, hvorledes der leves op til kravene hos den respektive CA. I certifikatet henvises til CP'en, således at en signaturmodtager kan tage stilling til, hvilke krav der som minimum er opfyldt gennem CA'ens CPS.

4.3.2 Specifikationsgrad

En CP er mindre specifik end en CPS, idet CPS'en angiver den detaljerede beskrivelse af forhold og betingelser, herunder forretnings- og driftsprocedurer for udstedelse og vedligeholdelse af certifikater.

CPS angiver, hvorledes en specifik CA opfylder de tekniske, organisatoriske og proceduremæssige krav identificeret i denne CP.

4.3.3 Forskelle

Indfaldsvinklen for CP og CPS er derfor også forskellig. En CP, som nærværende, er defineret uafhængig af specifikke detaljer i driftsmiljøerne hos CA, hvorimod CPS er skræddersyet til den organisatoriske struktur, driftsprocedurerne og IT-faciliteterne hos CA. Denne CP er udarbejdet af IT- og Telestyrelsen, mens CPS'en altid udarbejdes af en CA.

Da en CPS indeholder forretningsmæssige følsomme informationer, kan det ikke forventes, at hele CPS'en er offentligt tilgængelig. En uvildig tredjepart (systemrevisor) skal foretage en revision af CPS og skal erklære, at CPS overholder alle krav stillet i CP'en, samt at disse krav efterleves af CA.

4.3.4 Andre CA-betingelser

En CA vil typisk ud over CP og CPS'en have andre betingelser og vilkår. Dette vil normalt omfatte de kommercielle betingelser og vilkår, hvorunder CA udsteder certifikater og stiller statusinformation til rådighed.

5 Introduktion til certifikatpolitik

5.1 Generelt

Dette dokument beskriver certifikatpolitik for OCES-personcertifikater.

5.2 Identifikation

Denne CP er identificeret ved den følgende "object identifier" (OID):

Personcertifikat:

{ 1 2 208 stat(169) pki(1) cp(1) nq(1) person(1) ver(2) }.

OID er registreret i Dansk Standard i overensstemmelse med DS 2391:1995, del 1 og 3.

Alle OCES-personcertifikater, der udstedes efter denne CP, skal referere til denne CP ved at angive den relevante OID i "certificate policy"-feltet i OCES-certifikatet. De nævnte OID'er må kun refereres i et certifikat efter skriftlig aftale med IT- og Telestyrelsen.

5.3 Anvendelsesområde

Et OCES-personcertifikat kan anvendes til sikring af afsender- og meddelelsesautencitet, herunder elektronisk signatur samt meddelelsesintegritet. Det kan også anvendes til at sikre hemmeligholdelse (kryptering).

OCES-personcertifikater er ikke kvalificerede certifikater, dvs. de må ikke bruges i situationer, hvor kvalificerede certifikater er påkrævet.

OCES-personcertifikater må ikke anvendes til signering af andre certifikater.

5.4 CA's ret til at udstede OCES-certifikater

CA kan udstede OCES-personcertifikater efter denne version af CP'en, hvis CA,

- har indgået skriftlig aftale med IT- og Telestyrelsen herom og
- har indsendt en rapport jf. 7.1. til IT- og Telestyrelsen, indeholdende en erklæring fra en ekstern systemrevisor. Revisionserklæringen skal godtgøre, at CA opfylder alle krav, der stilles i nærværende CP, samt har indført de kontroller, der er nødvendige for, at kravene til drift og sikkerhed til enhver tid kan overholdes og
- har modtaget en overensstemmelseserklæring fra IT- og Telestyrelsen, der bekræfter, at IT- og Telestyrelsen har godkendt den indsendte rapport og betragter kravene i nærværende CP som værende opfyldt.

6 Forpligtelser og ansvar

6.1 CA's forpligtelser

CA skal sikre, at alle krav som er specificeret i afsnit 7, er implementeret.

Certificeringscentre (CA), der må udstede certifikater ifølge denne CP (OCES-personcertifikater), er offentliggjort på IT- og Telestyrelsens hjemmeside: https://www.signatursekretariatet.dk.

Der er ikke krav om krydscertificering mellem disse centre.

CA skal sikre varetagelsen af alle aspekter i forbindelse med:

- distribution af rodcertifikater
- anvisning af hvorledes nøgler genereres og opbevares
- udsendelse af OCES-personcertifikater til certifikatindehavere
- spærring af OCES-personcertifikater efter anmodning
- publikation af spærrelister
- underretning af certifikatindehavere om snarligt udløb af gyldighed for certifikat og evt. fornyelse af nøglepar
- fornyelse af OCES-personcertifikater

CA skal opretholde et teknisk driftsmiljø, der overholder sikkerhedskravene i denne CP.

CA skal udfærdige en CPS, der adresserer alle krav i denne CP. CPS'en skal være i overensstemmelse med denne CP.

CA skal underkaste sig revisionskrav jf. denne CP.

Registreringsenheden (RA) kan enten være nøje knyttet til CA, eller den kan være en selvstændig funktion. CA hæfter under alle omstændigheder for RA's opfyldelse af de stillede krav og forpligtelser på ganske samme måde som for sine egne forhold.

CA skal sikre, at den eller de tilknyttede RA følger de bestemmelser, som er fastlagt i denne CP.

CA skal desuden sikre, at RA:

- etablerer en web-adgang for registreringsprocedurer (kan være en del af CA's webtjeneste, hvis RA er en integreret del af CA)
- verificerer ansøgerens identitet og oplysninger
- opretholder et teknisk driftsmiljø i overensstemmelse med kravene i denne CP

6.2 Certifikatindehaverens forpligtelser

CA skal ved aftale forpligte certifikatindehaveren til at opfylde følgende betingelser:

- at give fyldestgørende og korrekte svar på alle anmodninger fra CA (eller RA) om information i ansøgningsprocessen
- at generere, opbevare og anvende nøglepar som anvist af CA. Den private nøgle kan opbevares på harddisk, diskette eller lignende
- at tage rimelige forholdsregler for at beskytte den private nøgle mod kompromittering, ændring, tab og uautoriseret brug
- at beskytte den private nøgle med en aktiveringskode, der mindst består af 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal
- anvendelse af anden aktiveringskode, f.eks. biometrisk – skal have en kompleksitet på mindst 128 bit
- aktiveringskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan dog være minimum fire cifre
- at beskytte aktiveringskoden, så andre ikke får kendskab til den
- at en evt. sikkerhedskopi af den private nøgle skal opbevares i krypteret form på betryggende vis
- ved modtagelse af OCES-certifikatet at sikre sig, at indholdet af OCES-certifikatet er i overensstemmelse med de faktiske forhold
- alene at benytte OCES-certifikatet og de tilhørende private nøgler i henhold til bestemmelserne i denne CP
- omgående at anmode den udstedende CA om spærring af OCES-certifikatet i tilfælde af kompromittering eller mistanke om kompromittering af den private nøgle
- omgående at anmode om fornyelse af certifikatet, hvis indholdet af OCES-certifikatet ikke længere er i overensstemmelse med de faktiske forhold

CA skal desuden orientere certifikatindehaver om, at den private nøgle anses for kompromitteret og skal spærres, hvis andre får kendskab til aktiveringskoden.

6.3 Information til signaturmodtagere

CA skal - bl.a. via sin hjemmeside - orientere signaturmodtagere om vilkår og betingelser for anvendelsen af digital signatur, herunder at tillid til et certifikat kræver, at signaturmodtager sikrer sig:

- at et modtaget certifikat er gyldigt og ikke spærret - dvs. ikke opført på CA's spærreliste
- at det formål, et certifikat søges anvendt til, er passende i forhold til anvendelses-begrænsninger på OCES-certifikatet samt
- at anvendelsen af certifikatet i øvrigt er passende i forhold til niveauet af sikkerhed, som er beskrevet i denne CP.

6.4 Ansvar

CA skal, i forhold til den der med rimelighed forlader sig på certifikatet, påtage sig erstatningsansvar efter dansk rets almindelige regler.

CA skal desuden påtage sig erstatningsansvar for tab hos certifikatindehavere og signaturmodtagere, der med rimelighed forlader sig på certifikatet, såfremt tabet skyldes:

- at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet
- at certifikatet ikke indeholder alle oplysninger som krævet i henhold til 7.3.3
- manglende spærring af certifikatet, jf. 7.3.6
- manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. 7.3.3 og 7.3.6, eller
- tilsidesættelse af 7.3.1,

medmindre CA kan godtgøre, at CA ikke har handlet uagtsomt eller forsætligt.

CA udformer selv sine aftaler m.v. med sine medkontrahenter. CA er berettiget til at søge at begrænse sit ansvar i forholdet mellem sig og sine medkontrahenter i det omfang, disse medkontrahenter er erhvervsdrivende eller offentlige myndigheder. CA er således ikke berettiget til at søge at begrænse sit ansvar i forhold til private borgere, som medkontrahenter.

CA er desuden berettiget til at fraskrive sig ansvar overfor medkontrahenter, som er erhvervsdrivende og offentlige myndigheder, for tab af den i § 11, stk. 3, i lov nr. 417 af 31. maj 2000 beskrevne art.

Forsikring

CA skal tegne og opretholde en forsikring til dækning af eventuelle erstatningskrav mod CA og RA fra såvel alle medkontrahenter (certifikatindehavere og signaturmodtagere) som IT- og Telestyrelsen. Forsikringen skal som minimum have en dækning på kr. 2 millioner pr. år.

7 Krav til CA-praksis

7.1 Certificeringspraksis (CPS)

CA skal udarbejde en certificeringspraksis (CPS), der i detaljer beskriver, hvorledes kravene i denne CP opfyldes, herunder:

- CA's administrative og ledelsesmæssige procedurer
- kvalifikationer, erfaring, m.v. hos CA's personale
- de systemer og produkter, som CA anvender
- CA's sikkerhedsforanstaltninger og arbejdsproces i forbindelse hermed, herunder oplysninger om hvilke foranstaltninger, der gælder med hensyn til at opretholde og beskytte certifikaterne, så længe de eksisterer
- CA's procedurer vedrørende registrering (identitetskontrol), udstedelse af certifikater, katalog- og tilbagekaldelsestjeneste samt registrering og opbevaring af oplysninger vedrørende certifikater, herunder vedrørende identitetsoplysninger
- CA's økonomiske ressourcer
- CA's procedurer vedrørende indgåelse af aftaler om udstedelse af certifikater og dets oplysningsforpligtelser
- i det omfang CA har udliciteret CA-opgaver til andre virksomheder eller myndigheder, skal CPS'en ligeledes omfatte udførelsen af disse opgaver

CA's praksis skal til enhver tid være i overensstemmelse med det i CPS'en beskrevne.

Godkendelse og løbende revision
En CA, der ønsker at udstede OCES-personcertifikater, skal indgå skriftlig aftale med IT- og Telestyrelsen.

CA skal efter underskrivelsen af aftalen udarbejde og indsende en rapport til IT- og Telestyrelsen. Rapporten skal godkendes af IT- og Telestyrelsen og indeholde:

- CA's CPS
- revisionsprotokollen
- en erklæring fra CA's ledelse om, hvorvidt CA's samlede data-, system- og driftssikkerhed må anses for betryggende, samt om at CA opfylder sin egen CPS
- en erklæring fra systemrevisor om, hvorvidt CA's samlede data-, system- og driftssikkerhed efter systemrevisors opfattelse må anses for betryggende, samt at CA opfylder sin egen CPS
- Dokumentation for ansvarsforsikring, der dækker CA's ansvar

Rapporten skal efterfølgende indsendes årligt til IT- og Telestyrelsen. Dette skal ske senest tre måneder efter afslutningen af CA's regnskabsår. Rapportens tidsperiode skal følge regnskabsåret for CA.

Systemrevision
Der skal gennemføres systemrevision hos CA. Ved systemrevision forstås revision af:

- generelle edb-kontroller i virksomheden
- edb-baserede brugersystemer m.v. til generering af nøgler og nøglekomponenter samt registrering, udstedelse, verificering, opbevaring og spærring af certifikater
- edb-systemer til udveksling af data med andre

Valg af systemrevisor - dennes beføjelser og pligter
CA skal vælge en ekstern statsautoriseret revisor til varetagelse af systemrevisionen hos CA. IT- og Telestyrelsen kan i særlige tilfælde dispensere fra kravet om, at systemrevisor skal være statsautoriseret revisor. CA skal senest en måned efter valg af systemrevisor anmelde dette til IT- og Telestyrelsen.

CA skal udlevere de oplysninger, som er nødvendige for systemrevisionen i CA. Herunder skal CA give den valgte systemrevisor adgang til ledelsesprotokollen.

CA skal give den valgte systemrevisor adgang til ledelsesmøder under behandling af sager, der har betydning for systemrevisionen. Ved et ledelsesmøde forstås et møde mellem den øverste ledelse af CA, i praksis ofte et bestyrelsesmøde. Ved udtrykket CA's ledelse forstås i denne sammenhæng den øverste ledelse af CA, dvs. bestyrelse eller tilsvarende ledelsesorgan afhængigt af, hvorledes CA er organiseret. CA skal sikre, at den valgte systemrevisor deltager i ledelsens behandling af pågældende sager, såfremt det ønskes af blot ét ledelsesmedlem.

I CA'er, hvor der afholdes generalforsamling, finder årsregnskabslovens bestemmelser om revisionens pligt til at besvare spørgsmål på et selskabs generalforsamling tilsvarende anvendelse for den valgte systemrevisor.

CA skal gøre den valgte systemrevisor bekendt med, at denne i overensstemmelse med god revisionsskik skal foretage den nedenfor nævnte systemrevision, herunder at påse, at:

- CA's systemer er i overensstemmelse med kravene i denne CP
- CA's sikkerheds-, kontrol- og revisionsbehov tilgodeses i tilstrækkeligt omfang ved udvikling, vedligeholdelse og drift af CA'ens systemer
- CA's forretningsgange såvel de edb-baserede som de manuelle er betryggende i sikkerheds- og kontrolmæssig henseende og i overensstemmelse med CA'ens certificeringspraksis (CPS)

CA skal sikre, at der i forbindelse med systemrevisionen foretages en sårbarheds-vurdering af logningsproceduren.

Den valgte systemrevisor kan samarbejde med den interne revision hos CA'en, såfremt en sådan eksisterer.

I det omfang den valgte systemrevisor konstaterer væsentlige svagheder eller uregelmæssigheder, skal CA's ledelse behandle sagen på næstkommende ledelsesmøde.

CA skal gøre den valgte systemrevisor bekendt med, at denne har pligt til at indberette forholdet eller forholdene til IT- og Telestyrelsen, såfremt systemrevisoren fortsat mener, at der forekommer væsentlige svagheder eller uregelmæssigheder. CA skal

desuden gøre systemrevisor bekendt med, at denne ved forespørgsler fra IT- og Telestyrelsen er forpligtet til at give oplysninger om CA's forhold, der har eller kan have indflydelse på CA's forvaltning af opgaven som udsteder af OCES-certifikater, uden forudgående accept fra CA. Systemrevisor er dog forpligtet til at orientere CA om henvendelsen.

CA og systemrevisor skal straks oplyse IT- og Telestyrelsen om forhold, der er af afgørende betydning for CA's fortsatte virksomhed.

Revisionsprotokol
CA skal gøre den valgte systemrevisor bekendt med, at denne løbende skal føre en særskilt revisionsprotokol, der skal fremlægges på ethvert ledelsesmøde, samt at enhver protokoltilførsel skal underskrives af CA's ledelse og den valgte systemrevisor.

CA skal desuden gøre systemrevisor bekendt med, at indholdet i protokollen skal være som anført nedenfor i dette afsnit.

I den valgte systemrevisors protokol skal der afgives beretning om den gennemførte systemrevision samt konklusionerne herpå. Der skal desuden redegøres for alle forhold, der har givet anledning til væsentlige bemærkninger.

I den valgte systemrevisors protokol skal det endvidere oplyses, hvorvidt denne under sit arbejde har modtaget alle de oplysninger, der er anmodet om.

Ved afslutningen af CA's regnskabsår udarbejder den valgte systemrevisor et protokollat til CA's ledelse.

Protokollatet skal indeholde erklæringer om, hvorvidt

- systemrevisionen er blevet udført i overensstemmelse med god revisionsskik
- den valgte systemrevisor opfylder de i lovgivningen indeholdte habilitetsbetingelser
- den valgte systemrevisor har fået alle de oplysninger, som den valgte systemrevisor har anmodet om
- de anførte systemrevisionsopgaver er udført ifølge denne CP's krav
- den samlede data-, system- og driftssikkerhed må anses for betryggende

IT- og Telestyrelsen kan pålægge CA inden for en fastsat frist at vælge en ny systemrevisor, såfremt den fungerende systemrevisor findes åbenbart uegnet til sit hverv.

Ved revisorskifte skal CA og den eller de fratrådte systemrevisorer hver især give IT- og Telestyrelsen en redegørelse.

Udgifter i forbindelse med systemrevision
CA skal afholde alle udgifter i forbindelse med systemrevision, herunder tillige systemrevision pålagt af IT- og Telestyrelsen.

7.2 Nøglehåndtering

CA's nøglehåndtering skal være i overensstemmelse med ETSI SR 002 176 v 1.1.1. (2003-03): *"Algorithms and Parameters for Secure Electronic Signatures"*, der definerer en liste over anerkendte kryptografiske algoritmer samt krav til deres parametre.

7.2.1 CA nøglegenerering

Generering af CA's rodnøgler og andre private nøgler skal ske under overvågning af to personer med hver sin betroede funktion i CA.

Generering af CA's private nøgler skal ske i kryptografisk modul, der opfylder kravene i FIPS 140-1 level 3, CWA 14167-2, eller højere. Det kryptografiske modul skal opbevares i henhold til kravene i 7.4.4.

Hvis CA's rodnøgler eller andre private nøgler skal overføres fra kryptografisk modul, skal dette ske i krypteret form og under medvirken af mindst to personer med forskellige betroede funktioner i CA.

Certifikatudsteders rodnøgler skal være RSA-nøgler af en længde på mindst 2048 bit eller tilsvarende. Certifikatudsteders rodnøgler skal være gyldige i mindst 5 år.

Certifikatudsteders andre nøgler skal være RSA-nøgler af længde på mindst 1024 bit eller tilsvarende. Andre nøgler skal være gyldige i mindst 2 år.

Betegnelsen "OCES" skal indgå i rodcertifikatets Common Name.

7.2.2 CA-nøglelagring, backup og genskabelse

CA skal sikre, at CA's rodnøgler ikke kompromitteres og til stadighed bevarer deres integritet.

Lagring, sikkerhedskopiering og transport af CA's rodnøgler og andre private nøgler skal ske under overvågning af to personer med hver sin betroede funktion i CA.

CA's rodnøgler og andre private nøgler skal opbevares og bruges i kryptografiske moduler, der opfylder FIPS140-1 level 3 eller højere eller CWA 14167-2.

Sikkerhedskopier af CA's private nøgler skal opbevares i kryptografisk modul, der opfylder kravene i FIPS 140-1 level 3 eller højere eller CWA 14167-2. Det kryptografiske modul skal opbevares i henhold til kravene i 7.4.4.

7.2.3 CA's publicering af den offentlige nøgle

CA's rodcertifikat skal gøres tilgængelig for signaturmodtagere ved Web-adgang med TLS/SSL-kommunikation. Verifikation af rodcertifikatets fingerprint (en kontrolværdi) skal ske via anden kanal.

7.2.4 Nøgleopbevaring og -genskabelse

CA skal sikre, at certifikatindehaverens private nøgler til afsender- og meddelelsesautencitet, herunder elektronisk signatur samt meddelelsesintegritet, ikke opbevares eller kan genskabes hos CA.

CA skal sikre, at certifikatindehaverens private nøgler til sikring af hemmeligholdelse (kryptering) ikke opbevares eller kan genskabes hos CA uden certifikatindehaverens godkendelse.

CA skal sikre, at der ikke kræves en sådan godkendelse fra certifikatindehaverens side som forudsætning for udstedelse af OCES-personcertifikater.

CA skal sikre, at proceduren for udlevering af opbevarede eller genskabte nøgler aftales samtidig med, at certifikatindehaveren giver sin godkendelse til opbevaring og/eller genskabelse.

7.2.5 CA's brug af nøgler

CA skal sikre, at CA's private nøgler ikke bliver benyttet til andet formål end signering af certifikater og statusinformation om certifikater.

CA skal sikre, at certifikatsigneringsnøgler kun benyttes i fysisk sikrede lokaler i henhold til 7.4.4.

7.2.6 CA's afslutning af nøglebrug

CA's private nøgle skal have en fast gyldighedsperiode. Efter udløb skal den private nøgle enten destrueres på en sådan måde, at den ikke kan genskabes eller opbevares sådan, at den ikke kan tages i brug igen.

CA skal sikre, at der inden udløb af den private nøgle, genereres et nyt CA-nøglepar, der benyttes til udstedelse af efterfølgende certifikater.

7.2.7 Håndtering af kryptografiske moduler

CA skal håndtere og opbevare kryptografiske moduler i henhold til kravene i 7.4 i hele de kryptografiske modulers levetid.

CA skal sikre sig, at kryptografiske moduler til certifikat og signering af statusinformation ikke er blevet kompromitteret inden installation.

CA skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering ikke bliver kompromitteret under brug.

CA skal sikre sig, at al håndtering af kryptografiske moduler til certifikat- og statusinformationssignering sker under medvirken af mindst to personer med hver sin betroede funktion i CA.

CA skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering altid fungerer korrekt.

CA skal sikre sig, at nøgler, opbevaret i et kryptografisk modul til certifikat- og statusinformationssignering, destrueres i forbindelse med, at modulet kasseres.

7.3 Certifikathåndtering

7.3.1 Registrering af certifikatindehaver

CA skal sikre, at certifikatindehaver forud for udstedelsen af et OCES-personcertifikat gøres opmærksom på og accepterer vilkår og betingelser for anvendelsen af certifikatet.

Der er ikke krav om personligt fremmøde i forbindelse med udstedelsen af et OCES-personcertifikat.

CA skal etablere en procedure for verifikation af ansøgers identitet, der sikrer, at:

- Certifikatindehaveren angiver CPR-nr. og postnr.
- OCES-certifikatindehaverens navn og folkeregisteradresse indhentes ved online opslag i CPR-registeret i tilmeldingsprocessen
- OCES-certifikatindehaveren udstyres med en engangskode fremsendt via pinkodebrev til folkeregisteradressen

Såfremt CA på forhånd har kendskab til certifikatindehaverens identitet eller anvender andre betryggende procedurer til at foretage identitetskontrol, kan ovennævnte procedure for certifikatansøgning helt eller delvist fraviges.

Generering og installation af certifikatindehavers nøgler

CA skal etablere en installationsprocedure, der teknisk sikrer, at:

- certifikatindehaver skal angive sin engangskode for at starte installation af den private nøgle og tilhørende certifikat
- nøglepar genereres hos certifikatindehaver
- certifikatindehavers nøgler er RSA-nøgler med en længde på mindst 1024 bit eller tilsvarende
- den offentlige nøgle overføres til CA sammen med oplysninger i en meddelelse signeret med den private nøgle
- den private nøgle er krypteret og beskyttet af aktiveringskode
- aktiveringskode til aktivering af den private nøgle genereres og indtastes i forbindelse med nøglegenereringen
- den private nøgle er aktiveret, når certifikatindehaveren har angivet aktiveringskode, der består af mindst 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal
- anvendelse af anden aktiveringskode – f.eks. biometrisk – skal have en kompleksitet på mindst 128 bit
- aktiveringskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan dog være minimum fire cifre
- rodcertifikatet er installeret hos certifikatindehaver

- rodcertifikatet kan verificeres via anden kanal
- tidspunkt og dato for udstedelsen af certifikatet efterfølgende kan fastlægges

CA skal understøtte, at generering og lagring af nøgler kan foregå ved brug af hardware.
CA skal over for certifikatindehavere anvise kryptografiske moduler til dette formål. Der er ikke angivet specifikke krav til OCES-certifikatindehaveres kryptografiske moduler.

CA skal efter anmodning om muligt anvise metode for certifikatindehaver til at lave evt. sikkerhedskopi af den private nøgle, således at den opbevares i krypteret form på betryggende vis.

RA skal godkende en certifikatansøgning, hvis:

- proceduren gennemføres som anvist
- ansøgeren kan verificeres via online opslag hos CPR-registeret, og
- ansøgeren giver korrekt engangskode i højst 5 forsøg

CA skal sikre, at der fra det tidspunkt, en RA har modtaget en certifikatansøgning og til nødvendig information for udstedelse af et certifikat er afsendt til certifikatansøgeren, over en løbende måned i gennemsnit maksimalt må gå en arbejdsdag, dog max. tre arbejdsdage. Såfremt certifikatansøgerens adresse ikke kan indhentes ved opslag i CPR-registeret, må der dog gå op til 5 arbejdsdage, inden nødvendig information for udstedelse er afsendt.

7.3.2 Certifikatfornyelse

Fornyelse af et OCES-certifikat betyder udstedelse af et nyt certifikat til den samme certifikatindehaver som i det eksisterende certifikat, men med en ny nøgle, ny gyldighedsperiode, et nyt certifikat-serienummer og det gældende OID. Et OCES-certifikat må fornyes for to år ad gangen.

Et certifikat kan efter anmodning fra certifikatindehaveren og mod behørig identifikation kun blive fornyet, hvis nøglernes gyldighedsperiode ikke er udløbet, og den private nøgle ikke er kompromitteret.

CA skal sikre, at anmodningen om fornyelse signeres med certifikatindehaverens private nøgle.

CA skal godkende bevis for besiddelsen af den private nøgle tilhørende det eksisterende certifikat som værende tilstrækkelig autentifikation i det tilfælde, hvor et certifikat skal fornyes. RA skal således sikre, at certifikatindehaveren besidder den private nøgle, som svarer til den offentlige nøgle, som præsenteres i certifikatansøgningen.
Det er tilstrækkeligt at verifikationen sker ved, at certifikatindehaveren signerer certifikatansøgningen med sin private nøgle. Den verificerende RA skal validere signaturen ved hjælp af den offentlige nøgle givet i certifikatansøgningen.

Certifikatansøgning og -udstedelse skal opfylde kravene i afsnit 7.3.1 om generering og installation af certifikatindehavers nøgler, dog med undtagelse af udsendelse af engangskode, som ved fornyelse erstattes af validering med det eksisterende certifikat.

Efter spærring eller udløb, eller hvis den private nøgle er blevet kompromitteret, kan et certifikat ikke fornyes. CA skal i disse tilfælde sikre, at der kan ske udstedelse af nyt certifikat med ny nøgle, og at behandlingen af anmodning om nyt OCES-certifikat i dette tilfælde sker som ny udstedelse efter samme retningslinjer, som angivet i 7.3.1.

CA skal senest 14 dage før udløb notificere certifikatindehaveren via e-post til den i certifikatet angivne e-postadresse eller til folkeregisteradressen.

CA skal sikre, at anmodning om og udstedelse af fornyet OCES-certifikat kan ske on-line.

7.3.3 Certifikatgenerering

OCES-personcertifikater skal benytte DS 844: Specifikation for kvalificerede certifikater, idet dog QcStatements ikke må angive, at der er tale om et kvalificeret certifikat.

OCES-personcertifikater skal indeholde:	***Løsning***
Den udstedende CA's identifikation og det land, som certificeringscenteret er etableret i	Issuer – information indeholder den krævede information. Dvs. min. entydigt navn og landekode
Certifikatindehaverens navn eller pseudonym; i sidstnævnte tilfælde skal det fremgå, at der er tale om et pseudonym	Common Name indeholder navn og/eller pseudonym. Hvis der benyttes pseudonym, lægges pseudonymet tillige i Pseudonym-feltet.
Særlige oplysninger om certifikatindehaveren, der tilføjes, hvis det er relevant, afhængigt af formålet med certifikatet	Subject serialNumber og andre attributter indeholder informationen med passende kvalifikatorer. Se uddybning i ETSI TS 101 862 og RFC 3039. Formatet for Subject SerialNumber skal følge anvisningerne for personcertifikater i DS 844, pkt. 4.3
De signaturverificerings-data, som svarer til de signaturgenereringsdata, som er under underskriverens kontrol	X.509.v3.
Certifikatets ikrafttrædelses- og udløbsdato	X.509.v3 og RFC 2459.
Certifikatets identifikationskode	CA tildeler certifikatet et for CA'en unikt løbenummer. Sammen med

OCES-personcertifikater skal indeholde:	***Løsning***
	CA's identifikation er nummeret totalt unikt. X.509.v3 og RFC 2459.
Den udstedende CA's avancerede elektroniske signatur	X.509.v3 og RFC 2459.
Eventuelle begrænsninger i certifikatets anvendelsesområde	KeyUsage, CertificatePolicies og ExtendedKeyUsage.

Certifikatfeltet subject

I kolonnen "Krav" benyttes M for Mandatory (=krav) og O for Optional(=frivilligt).

Attribut	**Krav**	**Kommentarer**
countryName:	M	Landekode
organizationName:	O	"Ingen organisatorisk tilknytning"
OrganizationalUnitName:	M	Se regler neden for
serialNumber:	M	Kvalifikator PID: konkateneret med løbenummer Se DS 843-1 Personspecifikke Identifikationsnumre (PID)
givenName:	O	Personens fornavne
surname:	O	Personens efternavn
commonName	M	Personens fulde navn eller pseudonym. Se regler nedenfor
postalAddress	O	Personens folkeregisteradresse
emailAddress	O	Personens e-post-konto
pseudonym	O	Personens pseudonym

Eksempel:
countryName=DK,
serialNumber= PID:9208-2001-3-279815395,
commonName=navn // PID:279815395,
emailAddress=navn@<gyldigt DNS domæne>

Regler:
countryName=DK, serialNumber, givenName, surName, commonName og **pseudonym** skal tilsammen entydigt udpege personen, der er indehaver af certifikatet.
OrganizationName: Hvis dette felt benyttes, sættes indholdet til "Ingen organisatorisk tilknytning".
SerialNumber: Benyttes til en unik identifikation (Se: Personspecifikke Identifikationsnumre: DS 843-1).
Pseudonym: Må ikke benyttes, dersom **givenName** eller **surName** benyttes.

Hvis der i et OCES-certifikat er et pseudonym i **commonName**, anføres pseudonymet også i **pseudonym**.
OrganizationalUnitName: Hvis personen er myndig, er feltet tomt/fraværende. Hvis personen på udstedelsestidspunktet er under 18 år, men er fyldt 15 år angives: "Ung mellem 15 og 18 – Kan som udgangspunkt ikke lave juridisk bindende aftaler". Hvis personen er under 15 år på udstedelsestidspunktet tilføjes: "Ung under 15 – kan ikke selv lave juridisk bindende aftaler".
CommonName: Hvis personen er under 18 år på udstedelsestidspunktet tilføjes: "(Ung under 18)".
Ikke nævnte felter er valgfrie.

Øvrige felter (extensions)

Versionsnummer skal være "v3".

Ved et kombineret certifikat, som skal anvendes til signering, autentifikation samt kryptering, skal **keyUsage** "extension" have de følgende specifikationer sat:

digitalSignature (0)
contentCommitment (1)
keyEnchipherment (2)
dataEncipherment (3)
keyAgreement (4)

Certifikater, der anvendes til autentifikation og signatur, skal have følgende specifikationer sat:

digitalSignature (0)
contentCommitment (1)

contentCommitment specifikationen sættes for, at certifikatet kan anvendes til at verificere signaturer, som har til hensigt at styrke uafviselighed og de som ikke har det.

Ved certifikater, der udelukkende anvendes til kryptering, skal følgende specifikationer sættes til:

keyEnchipherment (2)
dataEncipherment (3)
keyAgreement (4)

I alle tilfælde skal denne ekstension defineres som kritisk.

I de følgende oversigter anvendes disse koder:
O: Valgfri.("Optional")
C: Ekstension skal markeres kritisk ("Critical").
X: Ekstension må ikke markeres kritisk.
(C): Valgfrit for CA at markere ekstension som kritisk ("Critical").
R: Ekstension er krævet ("Required").
M: Håndtering af ekstension skal være tilstede ("Mandatory").
- : Ekstension har ingen mening.

Ekstension		Generering		
		Signatur		
	1. Anvendelse	2. CA	3. Slut bruger	4. Key Man.
AuthorityKeyIdentifier	O	O	O	O
SubjectKeyIdentifier	O	O	O	O
KeyUsage	CM	CMR	CMR	CMR
ExtendedKeyUsage	O	O	O	O
PrivateKeyUsagePeriod	O	O	O	O
CertificatePolicies	M	(C)MR	(C)MR	(C)MR
PolicyMappings	O	O	-	-
SubjectAltName	O	O	O	O
IssuerAltName	O	O	O	O
SubjectDirectoryAttributes	O	O	O	O
BasicConstraints	M	CMR	O	O
NameConstraints	O	O	-	-
PolicyConstraints	O	O	-	-
CRLDistributionPoints	M	R	R	R
QcStatements	O	O	O	O

Kommentarer til skemaet:
Håndtering af "extensions" er delt i 4 kolonner:
1. Software, der anvender udstedte certifikater.
2. Generering af certifikater til CA-software.
3. Generering af certifikater til slutbruger til brug for elektronisk signatur
4. Generering af certifikater til slutbruger til brug for nøgle håndtering/udveksling, f.eks. i forbindelse med autentifikation / kontrol af adgangsrettigheder.

CertificatePolicies skal i det mindste angive de relevante "object identifiers" for denne CP.

Når CA har udstedt et certifikat, kan certifikatindehaveren notificeres ad anden kanal end benyttet i udstedelsesproceduren.

7.3.4 Publicering af vilkår og betingelser

CA skal orientere certifikatindehaver om, at OCES-personcertifikater ikke kan anvendes til signering af andre certifikater.

CA skal orientere certifikatindehaver om, at den private nøgle ikke må benyttes, førend OCES-certifikatet er modtaget af certifikatindehaveren, bortset fra den brug, der sker ved certifikatansøgningen.

CA skal orientere certifikatindehaver om, at den private nøgle ikke må benyttes til signering efter anmodning om spærring, notifikation om spærring eller efter udløb.

Desuden skal CA orientere certifikatindehaver om, at ved mistanke om at den private nøgle er kompromitteret, må denne kun anvendes til anmodning om spærring.

I begge tilfælde må den private nøgle dog stadig benyttes til dekryptering af data, der er krypteret med den tilhørende offentlige nøgle før spærringen/mistanken om kompromittering.

CA skal orientere certifikatindehaver om, at et OCES-personcertifikat givet til en certifikatindehaver er gyldigt maksimum to år, hvorefter det kan fornyes.

7.3.5 Publicering af certifikater

CA skal gøre følgende typer af information tilgængelige for alle:

- det rodcertifikat, der anvendes for udstedelse af certifikater ifølge denne CP, samt rodcertifikatets "fingerprint" ad anden kanal
- andre certifikater, der anvendes for signering af information mellem CA og certifikatindehavere og signaturmodtagere
- denne CP, så længe der er gyldige certifikater udstedt efter denne CP og så længe, der er certifikater på spærrelisten for denne CP
- den af systemrevisor godkendte CPS, med undtagelse af forretningshemmeligheder
- alle OCES-personcertifikater i mindst to måneder efter udløb af gyldighedsperiode, undtagen de certifikater, som skal holdes hemmelige
- spærreliste for OCES-personcertifikater udstedt efter denne CP.

Spærrelisteinformation skal være tilgængelig for læsning uden nogen form for adgangskontrol.

CA skal sikre, at de krav, CA stiller til certifikatindehaver og signaturmodtager på baggrund af denne CP, uddrages og dokumenteres, jf. afsnit 6.2 og 6.3.

7.3.6 Certifikatspærring

CA skal omgående spærre et OCES-certifikat, hvis pågældende forhold er meddelt CA:

- der er vished eller mistanke om, at certifikatindehaverens private nøgle er kompromitteret
- den private nøgle er ødelagt
- der er konstateret unøjagtighed i certifikatets indhold eller anden information knyttet til certifikatindehaveren
- certifikatindehaveren ønsker at afslutte brugen af OCES-certifikatet
- certifikatindehaver er afgået ved døden
- certifikatindehaver er kommet under værgemål med fratagelse af den retlige handleevne

CA bør spærre et certifikat, hvis CA får kendskab til, at:

- certifikatindehaveren har mistet adgang til den private nøgle, feks. som følge af bortkommen aktiverings-kode

CA kan spærre et certifikat, hvis CA får kendskab til, at:

- reglerne i denne CP ikke er overholdt
- bestemmelserne i aftalen mellem CA og certifikatindehaver er misligholdt

CA's misligholdelse af CP giver ikke CA ret til at spærre et certifikat.

CA skal sikre, at en anmodning om spærring af certifikat i videst muligt omfang sker ved angivelse af specifik tilbagetrækningskode tildelt af CA ved udstedelsen eller ved signering med certifikatindehaverens private nøgle.

Er tilbagetrækningskoden eller den private nøgle bortkommet eller ikke tilgængelig, skal CA sikre, at identifikationen sker på en måde, der sikrer identiteten bedst muligt f.eks. ved en kombination af navn, folkeregisteradresse og e-postadresse.

De følgende kan anmode om spærring af certifikat:

- certifikatindehaveren mod behørig dokumentation.
- CA, hvis reglerne i denne CP ikke er overholdt, eller hvor forholdene i øvrigt tilsiger dette
- en af Skifteretten udpeget bobestyrer eller arvinger efter certifikatindehaver, såfremt certifikatindehaver er afgået ved døden
- værge mod behørig dokumentation
- Tilsyn eller kurator, såfremt certifikatindehaver har anmeldt betalingsstandsning eller tages under konkursbehandling

CA skal sikre, at proceduren for anmodning om spærring så vidt muligt ikke tillader, at der foretages uautoriserede spærringer samtidig med, at autoriserede spærringer tilgodeses via telefonisk henvendelse, via e-post eller via Web-adgang.

CA skal sikre, at der ved telefonisk spærring angives information som angivet ovenfor plus årsag til spærring. CA skal kvittere for spærring via e-post til den oplyste e-postadresse samt via post sendt til den officielle postadresse som angivet i CPR-registeret.

CA skal ved anmodning via e-post sikre sig, at e-posten er signeret med den private nøgle.

CA skal sikre, at der ved anmodning via web angives årsag til spærring, og at web-formularen signeres med den private nøgle eller angivelse af tildelt spærringskode.

CA skal kvittere for spærring via signeret e-post, om muligt sendt til den e-postadresse som angivet i certifikatet og ellers med almindelig post. Certifikatindehaver kan kræve, at kvitteringen sendes med almindelig post.

Hvis CA foretager spærring uden at være anmodet om det, skal CA sende meddelelse med angivelse af årsag til spærring via signeret e-post til certifikatindehaver samt via post til den officielle postadresse som angivet i CPR-registeret.

I tilfælde af konkurs kan anmodningen om spærring ske af skifteret eller kurator. Ovennævnte metoder kan ligeledes anvendes. CA skal dog ligeledes sende kvittering for spærring til den af skifteretten hhv. kurator angivne postadresse.

CA skal sikre, at der, efter at en anledning til spærring er konstateret, anmodes om spærring uden ugrundet forsinkelse.

CA skal sikre, at spærring sker umiddelbart efter anmodning er modtaget og eventuel bekræftelse for anmoders identitet er sket.

CA skal offentliggøre opdateret spærreliste samtidig med, at der udsendes kvittering for spærring af certifikat. Dette skal ske senest 1 minut efter spærring er sket.

CA skal sikre, at der er en separat spærreliste for OCES-certifikater.

CA skal som minimum offentliggøre en ny spærreliste hver 12. time.

CA skal gøre spærrelister tilgængelige for download via LDAP og HTTP som CRL-fil samt for manuelt opslag fra Web browser.

Et OCES-certifikat kan ikke suspenderes. Ved mistanke om kompromittering af den private nøgle skal CA sikre, at certifikatet spærres.

CA skal sikre spærrelister mod kompromittering, og at spærrelisterne og OCSP-tjenester er tilgængelige via internet daglig mellem klokken 0 og 24. Tjenesterne skal have en gennemsnitlig svartid, der ikke overstiger 1 sekund målt på serverindgang – dvs. fra serveren har registreret forespørgslen, til den returnerer et svar.

For spærrelister skal CA benytte en profil som angivet i IETF RFC 2459.
thisUpdate og **nextUpdate** skal angives i **UTCTime** format YYMMDDHHMMSSz.

Versionsnummer skal være angivet og sættes til "v2". Der er ikke krav om benyttelse af CRL-extensions.

En CA kan tillige tilbyde online (F.eks. via Online Certificate Status Protocol, OCSP) kontrol af status.

CA skal sikre, at svaret er elektronisk signeret og indeholder OCES-certifikatets unikke identifikationsnummer, status for certifikatet samt tidspunktet for svaret angivet i UTC-format med en nøjagtighed på 1 sekund.

For OCSP skal CA benytte en profil i overensstemmelse med IETF RFC 2560.

thisUpdate feltet må højst være 1 minut ældre end **producedAt** feltet. Begge felter angives i **generalizedTime.**

Version 1 skal understøttes. Der er ikke krav om benyttelse af OCSP-extension.

7.4 CA styring og drift

7.4.1 Sikkerhedsimplementering

CA skal sikre, at dens administrative og ledelsesmæssige procedurer er tilstrækkelige og lever op til anerkendte standarder.

CA skal gennemføre en risikoanalyse af de forretningsmæssige risici og indføre de nødvendige sikkerhedstiltag samt driftsmæssige procedurer.

CA skal påtage sig det fulde ansvar for alle tjenester, der stilles direkte eller indirekte til rådighed for håndteringen af certifikatudstedelsen og statusinformationen.

CA skal implementere en IT-sikkerhedsorganisation, der til enhver tid skal have ansvaret for en sikkerhedsmæssig korrekt drift af CA'ens funktioner.

CA skal sikre, at personer med auditørfunktioner hos CA ikke personalemæssigt refererer til samme ledelse som driftsansvarlige og administratorer.

IT sikkerheden i CA skal defineres i henhold til internationalt anerkendte standarder og være underlagt IT sikkerhedsorganisationens tilsyn.

De sikkerhedskontroller og driftsprocedurer, der gælder for CA's lokaliteter, systemer og data vedrørende certificeringstjenester, skal være dokumenteret, implementeret og skal løbende vedligeholdes.

I tilfælde, hvor ansvaret for CA'ens certificeringsfunktioner outsources til en anden organisation eller enhed, skal CA sikre, at informationssikkerheden opretholdes tilsvarende.

7.4.2 Identifikation og klassifikation af IT-aktiver

CA skal gennemføre en risikoanalyse af alle IT-aktiver, hvor sårbarheder listes.

De enkelte IT aktiver skal klassificeres i henhold til deres betydning for driften af CA's primære funktioner og i overensstemmelse med den gennemførte risikoanalyse.

7.4.3 Personalesikkerhed

Krav til kvalifikationer, erfaring og sikkerhedsklassifikation

Personer med betroede funktioner hos CA, herunder også systemrevisor, skal have verificerede kvalifikationer inden for deres ansvarsområde og mindst 1 års erfaring.

Alle personer med ledelsesfunktioner hos CA skal være bekendte med sikkerhedsprocedurer for ansatte med sikkerhedsansvar samt have erfaring i IT-sikkerhed og risikovurdering.

Procedurer for sikkerhedsklassifikation
CA skal kontrollere, at ledere og medarbejdere, der skal udføre betroede opgaver i eller for CA, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv.

Krav til uddannelse
Alle personer med betroede funktioner hos CA skal have en for deres arbejdsområde relevant uddannelse eller træning. CA'ens ledelse er ansvarlig for, at hver medarbejder er egnet til det pågældende hverv.

Krav om og hyppighed af opdatering af kvalifikationer
Generelt
Relevante kvalifikationer hos medarbejdere i CA skal opdateres, hvis de ikke har været anvendt i de seneste fire år.

CA-driftspersonale
CA-driftspersonale skal opdatere deres viden en gang årligt.

Procedure for håndtering af uautoriserede handlinger
Der skal etableres klare procedurer for håndtering af enhver form for uautoriserede handlinger. Procedurerne skal være udmeldt til alle personer med betroede funktioner hos CA.

Kontrol af underleverandører
CA skal sikre, at personale hos underleverandører opfylder samme krav til uddannelse, erfaring og sikkerhedsklassifikation som CA's egne medarbejdere i de funktioner, underleverandørens personale varetager.

CA skal ved adgangsprocedurerne sikre, at personale hos underleverandører ikke kan arbejde uovervåget noget sted hos CA.

Dokumentation til brug for personale
CA skal dokumentere og gøre alle procedurer, regler og sanktioner tilgængelige for personalet i CA. CA's ledelse skal kunne dokumentere, at alt personale er blevet gjort bekendt med procedurer, regler og sanktioner.

7.4.4 Fysisk sikkerhed
Generelt
CA skal beskrive klart, på hvilken lokalitet man har placeret medarbejdere og datacentre i forbindelse med CA's virke. De lokaler, hvor udstyr til nøglegenerering er placeret, benævnes CA driftslokaler.

Alle lokaler, der benyttes til medarbejdere i CA, skal være defineret som særligt sikkerhedsområde i henhold til DS 484.

CA driftslokaler
CA driftslokaler skal defineres til et sikkerhedsniveau og overholde kravene i DS 484 del 2.

CA driftslokalet skal være fysisk adskilt fra CA's øvrige lokaler.

I tilfælde af evakuering skal CA's driftslokaler kunne fungere med uændret drift via fjernbetjening. Ved fjernbetjening forstås mulighed for f.eks. via en PC at betjene CA-funktionerne fra et fra CA-driften fysisk adskilt lokale, f.eks. hvor CA har etableret reservesystem.

CA's driftslokaler skal beskyttes mod indtrængende luftforurening, røg og radioaktivt nedfald.

Fysisk adgang
Generelt
CA skal sikre, at alle lokaler har en perimeterbeskyttelse svarende til DS 471 eller bedre.

CA skal sikre, at adgang til og ophold i centrale CA-driftslokaler er begrænset til specifikke personalekategorier ved elektronisk adgangskontrol.

CA skal sikre, at der etableres vagt 24 timer i døgnet.

CA-driftslokaler
CA skal sikre, at adgang til og ophold i de centrale driftslokaler videoovervåges.

Elforsyning og luftkonditionering
CA skal beskytte elforsyningen mod udfald. Beskyttelsen skal dække alle driftssystemer samt alt telekommunikationsudstyr placeret hos CA.

CA-driftslokaler
CA skal dublere og beskytte luftkonditionering i CA-driftslokaler mod elforsyningsudfald.

CA skal beskytte luftkonditionering mod forurening, røg og radioaktivt nedfald via luftindtaget.

Vandtryk
Generelt
CA skal foretage sikring mod vandindtrængning og rørlækager.

CA-driftslokaler
CA skal sikre, at der ikke forekommer vandinstallationer i CA-driftslokaler, ej heller må vandinstallationer føres gennem CA-driftslokaler, jf. DS 484 del 2, punkt S.6.5.1.

CA skal implementere detektering af vand i CA-driftslokaler og alarmering i forbindelse hermed.

Forebyggelse af og beskyttelse mod brand
Generelt
CA skal installere automatisk brandalarmeringsanlæg.

CA-driftslokaler
CA skal etablere de enkelte funktionsrum som separate brandceller.

CA skal endvidere installere automatisk brandslukningsanlæg.

Opbevaring af lagringsmedie
CA skal etablere arkiver for opbevaring af lagringsmedier med sikkerhedskopierede data og programmer i separate, funktionsadskilte celler.

Affaldshåndtering
Generelt
CA skal sikre, at affald, der indeholder fortrolig information, betragtes som fortroligt materiale og destrueres på forsvarlig vis.

CA-driftslokaler
CA skal sikre, at affald fra CA-driftslokaler behandles særskilt og destrueres, inden det fjernes fra området.

Reservesystem på anden lokalitet
Etablerer CA evt. reservesystemer på anden lokalitet, skal CA sikre, at disse opfylder samme krav som hovedsystemer. Såfremt reservesystemer etableres skal CA sikre, at det sker fysisk så langt fra hovedsystemet, at risikoen for kumulative nedbrud er minimeret.

7.4.5 Styring af IT-systemers og netværks drift
CA skal definere, hvilke betroede funktioner der haves, og der skal udarbejdes en beskrivelse af hver betroede funktions ansvarsområde i CA.

Generelt
CA skal sikre, at der medvirker mindst to personer med forskellige betroede funktioner hos CA ved alle opgaver, hvor der er mulighed for ændring i opsætninger og funktionalitet.

CA skal sikre, at alt it - udstyr og data sikres mod vira, fejlbehæftet og uautoriseret software.

CA skal søge at minimere skader som følge af sikkerhedsbrud og fejl ved hjælp af hændelsesrapportering og procedurer for umiddelbar opfølgning.

CA skal sikre, at alle benyttede medier beskyttes mod skade, tyveri og uautoriseret brug.

CA skal sikre, at følsomme data ikke kan genskabes via kasserede medier.

CA-driftslokaler
CA skal sikre, at der medvirker mindst to personer med forskellige betroede funktioner hos CA ved alle opgaver i CA-driftslokaler.

CA skal sikre, at medarbejdere i hver betroet funktion kan identificeres entydigt ved tydelig billeddokumentation.

CA skal sikre, at adgang til systemer knyttes til hver enkelt betroet funktion. Hvor der er krav om flere personers adgang til systemer, skal CA sikre, at dette understøttes teknisk i størst mulig omfang.

7.4.6 Kontrol af adgang til systemer, data og netværk

CA skal sikre, at alt benyttet IT-udstyr er sikkert og driftes korrekt med et minimum af fejlmuligheder.

CA skal gennem opstillede regler og ved tekniske foranstaltninger begrænse adgangen til CA-systemerne til et absolut minimum.

CA skal begrænse eksterne personers adgang til CA-systemerne mest muligt.

CA's interne netværk skal være beskyttet mod andre netværk med korrekt konfigurerede firewalls.

CA skal sikre, at følsomme data beskyttes, når de udveksles over netværk. Normalt ved brug af kryptering.

CA skal sikre, at administration af brugerrettigheder til systemerne er beskrevet i skriftlige instrukser, at alle ændringer i rettigheder logges, og at der føres kontrol med disse logs.

CA skal sikre, at alle systemer understøtter en stringent kontrol med adgang til data og forhindrer utilsigtet udveksling på tværs af betroede funktioner hos CA.

CA skal sikre, at adgang til systemer kun opnås efter korrekt identifikation fra den enkelte ansatte.

CA skal sikre, at der udpeges en ansvarlig for tildeling af adgange til ethvert system. CA skal desuden sikre, at tiltag i tilfælde af uregelmæssigheder er klargjort for den enkelte ansatte.

Driftslokaler
CA skal sikre, at alle netværks komponenter er placeret i fysisk sikrede lokaler i henhold til 7.4.4, samt at netværkskomponenternes konfiguration revideres periodisk.

CA skal sikre, at alle it - komponenter i driftslokaler konstant er overvåget, og at der er alarmer for alle forsøg på adgang til og ændring af konfigurationer og data.

CA skal sikre, at der er alarmer for alle uautoriserede ændringer i data vedrørende certifikater og tilhørende information samt statusinformation.

7.4.7 Udvikling, anskaffelse og vedligeholdelse af IT-systemer

CA skal benytte anerkendte systemer og produkter, som er beskyttet mod ændringer. Produkterne skal overholde en tilstrækkelig beskyttelsesprofil i henhold til ISO/IEC 15408 eller tilsvarende.

Ved egen udvikling skal CA sikre, at der foreligger en ledelsesgodkendt plan for indbygning af sikkerhed i systemerne. Dette gælder også ved bestilt udviklingsarbejde.

CA skal sikre, at der etableres kontrolprocedurer for nye versioner, ændringer og reservesystemer

7.4.8 Beredskabsplanlægning

Følgende hændelser skal betragtes som alvorlige:

- Kompromittering af CA's private nøgle
- Mistanke om kompromittering af CA's private nøgle
- Nedbrud og kritiske fejl på CA's driftskomponenter (spærrelister etc.)
- Stop af CA-driftsmiljøet som følge af brand, elforsyningssvigt osv.

CA skal sikre, at der foreligger en beredskabsplan, der kan bringe CA's drift tilbage til normal hurtigst muligt, efter at en alvorlig hændelse er indtrådt.
Beredskabsplanen skal herefter revideres med henblik på at undgå, at lignende hændelser gentages.

CA skal i tilfælde af kompromittering af CA's private nøgle eller mistanke herom informere alle certifikatindehavere og IT- og Telestyrelsen. I det omfang det er muligt, skal signaturmodtagere informeres. Det kan for eksempel ske igennem offentlige medier og ved annoncering i dagspressen.

CA skal i tilfælde af alvorlige hændelser på databehandlingsudstyr, programmel og/eller data orientere certifikatindehavere herom i det omfang, det er relevant for deres brug af CA-tjenesterne. Så vidt muligt skal signaturmodtagere informeres. Det kan for eksempel ske igennem offentlige medier og ved annoncering i dagspressen.

CA skal sikre, at alle procedurer omkring spærrelister, herunder anmodning om spærring, har højeste prioritet i forbindelse med retablering af forretningsgange.

7.4.9 Ophør af CA

CA skal sikre, at al udstedelse og fornyelse af certifikater straks stoppes, når en CA-funktion vil ophøre med at fungere.

CA skal sikre den fortsatte operationelle drift af spærrelister og anmodninger om spærringer, indtil alle certifikater udstedt af denne CA er udløbet eller eventuelt overdraget til anden CA, der opfylder kravene i denne CP.

CA skal sikre, at arkiver er tilgængelige i mindst 6 år efter udløb af sidste certifikat udstedt af denne CA.

7.4.10 Overensstemmelse med lovgivningen

CA skal sikre overensstemmelse med lovgivningsmæssige krav særligt i relation til persondata.

Særlige forpligtelser med henblik på beskyttelse af fortrolig information

Information, som ikke indgår i certifikater og spærrelister, anses som fortrolig.

Information, som indgår i certifikater, anses som ikke fortrolig og ikke privat.

Personrelateret information, som ikke indgår i certifikatet, anses som privat information.

CA skal sikre, at en certifikatindehaver har mulighed for at kræve, at navne- og adresseinformation, herunder e-postadresse ikke fremgår af certifikatet *(gælder kun personcertifikat).*

CA skal sikre, at fortrolig information er beskyttet mod kompromittering og må ikke benytte fortrolig information til andet, end hvad der er påkrævet for driften af CA.

CA skal sikre, at privat information er beskyttet mod kompromittering og må ikke benytte privat information udover, hvad der er påkrævet for drift af CA.

CA skal sikre, at statistiske oplysninger om anvendelse af OCES-personcertifikater ikke kan henføres til det enkelte OCES-certifikat.

I tilfælde af tvistigheder, som ikke kan løses ved forhandling mellem parterne, er almindelig dansk ret gældende.

7.4.11 Opbevaring af certifikatinformation

CA er ansvarlig for etablering af et datalagringssystem, der skal indeholde alle data, der er nødvendige for sikker drift af CA i overensstemmelse med denne CP. CA skal desuden sikre, at:

- Al anden information beskyttes mod uretmæssig adgang
- Alle aktiviteter, der kræver deltagelse af mere end en person, logges
- Alle informationer om registrering, herunder certifikatfornyelser, logges
- Alle adgange og adgangsforsøg til områder, der skal beskyttes af adgangskontrol, logges
- Al videoovervågning logges
- Der er skriftlige regler for regelmæssig gennemgang af alle logs
- Alle audit-logs signeres elektronisk og tidsstemples
- Audit-logs behandles som fortroligt materiale

- Der foretages backup af audit-logs med regelmæssige mellemrum

CA skal sikre, at back-up-medier opbevares i overensstemmelse med kravene i 7.4.4 i medie-brandskab.

CA skal sikre, at IT- og Telestyrelsen informeres om væsentlige uregelmæssigheder i logningsproceduren samt notificeres en gang årlig i alle andre tilfælde.

CA skal sikre, at følgende information arkiveres:

- Alle logs
- Certifikatanmodninger og tilhørende kommunikation
- Signerede ordrer og skriftlig aftaler
- Certifikatfornyelser
- CPS og CP

CA skal sikre, at arkiveret information kan gøres tilgængelig i tilfælde af tvister, og at alt arkiveret materiale opbevares i mindst 6 år.

CA skal sikre, at alt materiale i arkiv opbevares i overensstemmelse med kravene i afsnit 7.4.4.

CA skal sikre, at alt elektronisk arkivmateriale sikkerhedskopieres med regelmæssige mellemrum.

CA skal sikre, at alt elektronisk arkivmateriale påføres elektronisk tidsstempling på arkiveringstidspunktet. Andet arkivmateriale indføres i en log.

7.5 Organisatoriske aspekter

CA's organisation skal være pålidelig.

CA skal være en registreret fysisk eller juridisk person.

CA skal sikre, at alle tjenester tilbydes til alle indenfor OCES-personcertifikaternes anvendelsesområde på lige fod. Dette betyder, at der ikke må gøres forskel på vilkår og betingelser for adgang til tjenester.

Alle CA's administrative og forretningsmæssige procedurer skal være tilpasset det nødvendige sikkerhedsbehov, driften af en CA foreskriver.

CA skal have tilstrækkelig finansiel styrke til at dække det ansvar, man påtager sig som CA, herunder også forpligtelserne i 7.4.9, dels gennem forsikring, dels gennem egenkapital.

CA skal til enhver tid have tilstrækkelig med uddannet personale til at kunne drive alle udbudte tjenester på forsvarlig vis. Personalet skal til enhver tid have den kompetence, de enkelte definerede betroede funktioner foreskriver.

CA skal sikre, at der foreligger politikker og procedurer for håndtering af alle former for kundehenvendelser eller henvendelser fra signaturmodtagere.

CA skal sikre, at der foreligger skriftlige aftaler med alle underleverandører af CA-tjenester.

7.6 Placering af datacentre

CA'er, der ønsker at placere hele eller dele af driftsmiljøet i udlandet, skal opfylde de samme krav i henhold til denne CP som en herværende CA. Den løbende kontrol skal således kunne gennemføres, uanset hvor CA geografisk er placeret.

Foretages systemrevisionen ikke af en statsautoriseret revisor, kræves der, jf. afsnit 7.1., en dispensation fra IT- og Telestyrelsen.