Lovforslag nr. L 229. Fremsat den 22. marts 2000 af forskningsministeren (Birte Weiss)

Forslag

til

lov om elektroniske signaturer[1)]

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

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 tydelige 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.
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.

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. 1og 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.
5) Tilsidesættelse af § 7.

Stk. 2. Et nøglecenter pådrager sig erstatningsansvar efter stk. 1, medmindre nøglecenteret 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 hindre, at disse data forevises for underskriveren forud 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 om 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 nøglecenteret 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) hvis 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. 1–2 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.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Loven har til formål at sikre, at der på det danske marked findes elektroniske signatur produkter og nøglecentre, der lever op til en række krav, der gør dem sikre at anvende.

Samfundsøkonomisk er det vigtigt, at der udvikles og udbydes elektroniske signaturer, der har et sådant sikkerhedsniveau, at de kan anerkendes i et bredt forum og kan anvendes til at understøtte udbud af nye tjenesteydelser i både det private og den offentlige sektor.

Det er ikke hensigten med lovgivningen at regulere det samlede udbud af certificeringstjenester. Nøglecentre vil efter lovens gennemførelse stadig have frihed til at udbyde certifikater og elektronisk signatur produkter uden at skulle underlægge sig et omfattende tilsyn, autorisationsordninger eller være tvunget til at benytte bestemte tekniske løsninger.

Loven skal således alene sikre, at der på markedet findes produkter (nemlig de omhandlede kvalificerede certifikater), som der er fastlagt en fælles minimumsstandard for. Både det private erhvervsliv og det offentlige vil dermed have en mulighed for ved udbud af elektroniske tjenesteydelser, hvor der er behov for autentifikation af afsenderen eller modtageren, at stille krav om, at der benyttes et certifikat og en elektronisk signatur, der opfylder visse minimumskrav.

Samtidig skal lovgivningen sikre, at der er klarhed over erstatningsansvaret, når man som afsender benytter sig af, og som modtager fæstner lid til et kvalificeret certifikat. Den valgte ansvarsmodel indebærer, at det er nøglecenterets ansvar at påvise, at nøglecenteret ikke har begået fejl i forbindelse med udstedelsen af certifikatet, spærring, eller ved afgivelse af oplysninger om udløbsdata og anvendelsesbegrænsninger for certifikatet.

A. Lovforslagets baggrund og formål

1. Elektroniske signaturers funktion og betydning

Elektroniske signaturers funktion og betydning kan bedst beskrives med et eksempel:

Indgåelse af aftaler foregår ofte ved, at aftaleparterne underskriver en kontrakt, eller ved at den ene part som bekræftelse på aftalens indgåelse udleverer en nota, en faktura eller lignende til den anden part.

I nogle tilfælde kender parterne på forhånd hinanden og vil derfor ikke være i tvivl om identiteten af den, de har indgået den pågældende aftale med. Men der indgås også et væld af aftaler mellem parter, som ikke kender hinanden på forhånd, og som aldrig kommer til at møde hinanden, eftersom deres kommunikation udelukkende foregår pr. brev, telefax, o.lign.

Når parterne kommunikerer på papir, tjener parternes underskrift og eventuelt et særligt brevpapir til at identificere afsenderen over for modtageren. Papiret tjener også til at sikre, at der ikke senere opstår tvivl om, hvordan det dokument, der anvendes, så ud, da aftalen blev indgået. Ved papirbaseret kommunikation har parterne således mulighed for at se, om en konvolut har været lukket op undervejs, og om der er foretaget synlige ændringer i den skrevne eller trykte tekst.

I praksis foregår kommunikationen oftest uden, at parterne tænker nærmere over disse aspekter. Det er da også kun undtagelsesvis, at der er behov for at være opmærksom herpå.

Når der kommunikeres gennem åbne digitale net, dvs. gennem net hvortil alle har adgang, som f.eks. Internettet, er det på samme måde afgørende, at man kan være sikker på, hvem det er, man kommunikerer med, og at indholdet af det kommunikerede ikke er blevet ændret efterfølgende.

Ved elektronisk kommunikation efterlades der ikke på samme måde som ved papirbaseret kommunikation konkrete spor, der gør, at en modtager bliver opmærksom på, at der kan være ændret i et dokuments indhold, ligesom det kan være vanskeligt eller nogle gange umuligt at få sikkerhed for, hvem der egentlig er afsender af meddelelsen.

Dette betyder, at det i praksis er enklere at foretage ændringer i elektronisk kommunikation eller at udgive sig for at være en anden, uden at det er synligt for modtageren.

F. t. l. om elektroniske signaturer

En elektronisk signatur er en kombineret »underskrift« og »lås«, der kan sikre mod disse problemer. En elektronisk signatur låser med andre ord et dokument med indhold til en bestemt person, efter at signaturen er blevet påført.

De signaturgenereringsdata, som anvendes til at skabe den elektroniske signatur, kan underskriveren opbevare på et plastickort eller som en del af et program på sin computer. Anvendelse vil oftest kræve et password, som underskriveren råder over, eller en anden form for identifikationsmekanisme.

Den elektroniske signatur skal skabe sikkerhed ikke blot for underskriveren, men også for den modtager, der ikke på forhånd kender afsenderen. Modtageren af en elektronisk signatur har med andre ord brug for at kunne stole på, at afsenderen rent faktisk er den, som vedkommende hævder at være, og at afsenderen fortsat har rådighed over sine signaturgenereringsdata (plastikkortet, computerprogrammet eller lignende).

For at sikre troværdighed overfor modtageren skal underskriverens identitet være kontrolleret af en uafhængig tredjepart, et såkaldt nøglecenter. I praksis sker der det, at nøglecentret efter at have kontrolleret underskriverens identitet udsteder et elektronisk certifikat herom.

Nøglecentret skal desuden etablere en servicefunktion, der giver modtageren mulighed for automatisk at undersøge, om et certifikat og dermed en elektronisk signatur er spærret, f.eks. fordi underskriveren har mistet rådigheden over sine signaturgenereringsdata.

Lovforslagets hovedsigte er at fastsætte minimumskrav til nøglecentre, der ønsker at anvende betegnelsen kvalificerede certifikater om de certifikater, som de tilbyder. Disse nøglecentre er som de eneste berettigede til at anvende denne betegnelse og underkastes bl.a. et skærpet erstatningsansvar for, at oplysningerne i certifikatet er korrekte og fyldestgørende, samt at nøglecentrets spærringsfunktion fungerer korrekt.

Der er ikke tale om, at nøglecentre skal autoriseres eller godkendes, men om at de skal underkastes et statsligt tilsyn, som løbende kan kræve at modtage dokumentation for, at loven overholdes, og som kan iværksætte forskellige sanktioner, hvis nøglecentret ikke lever op til kravene i loven.

2. Hvad er en elektronisk signatur, et elektronisk signatur certifikat og et nøglecenter?

En elektronisk signatur er i praksis baseret på to elementer.

Det første element er et såkaldt nøglepar, som man kunne beskrive som to halvdele af en nøgle, en kode eller en lås. Underskriveren råder over den ene halvdel (den private nøgle), mens et uafhængigt nøglecenter opbevarer eller registrerer den anden halvdel (den offentlige nøgle).

Det andet element er et certifikat, som udstedes af et uafhængigt nøglecenter, der attesterer underskriverens identitet og samtidig angiver, at underskriveren råder over den private nøgle, der svarer til eller passer sammen med den offentlige nøgle, som er indeholdt i certifikatet, og som tredjemand kan bruge til at verificere og dokumentere, at det rent faktisk er underskriveren, vedkommende har kommunikeret med.

Som teknologien er i dag, vil kommunikationen herefter foregå sådan, at underskriveren sender modtageren en elektronisk meddelelse, som kan bestå af en tekstfil, nogle billeder, en lydoptagelse, et beregningsprogram eller lignende, eller flere af de nævnte elementer i kombination. Når underskriveren er klar til at afsende meddelelsen, påfører han, ved hjælp af sit signaturgenereringssystem (plastikkort, computerprogram eller lignende), og den hertil knyttede private nøgle, meddelelsen sin elektroniske signatur. Påførslen vil også »låse« dokumentet, sådan at man ved en senere åbning af meddelelsen kan se, om denne – af afsenderen, modtageren eller tredjemand – efterfølgende er søgt ændret.

Herefter sender underskriveren meddelelsen til modtageren. Ofte vil han også medsende sit certifikat, der indeholder nøglecentrets attestering samt den offentlige nøgle, som modtageren skal bruge til at checke meddelelsen.

Imidlertid kan der jo være sket det, at afsenderen har mistet rådigheden over sit certifikat og sin private nøgle, eller at certifikatet er udløbet og derfor ikke længere anvendeligt. For at checke disse forhold henvender modtageren sig til nøglecentret og anmoder om at få bekræftet, at en brugers certifikat ikke er blevet spærret på samme måde som et betalingskort. Modtageren vil desuden af nøglecentret kunne få bekræftet, at certifikatet ikke er udløbet, og om der eventuelt er nogle begrænsninger af, hvad signaturen kan anvendes til eller en beløbsmæssig grænse for, hvor store transaktioner signaturen kan anvendes til.

I en række tilfælde vil både afsender og modtager desuden af bevismæssige årsager have behov for at kunne dokumentere, hvornår de har afsendt, modtaget eller verificeret en meddelelse, der er påført en elektronisk signatur. Nøglecentrene vil som uafhængige tredjeparter med sigte herpå også kunne tilbyde en facilitet, hvorefter elektroniske meddelelser fremsendes til tidsstempling, eventuelt som led i og samtidig med, at meddelelsen i øvrigt sendes til modtageren (en art »poststemplings-funktion«), eller umiddelbart efter at

denne modtages. I hvilket omfang sådanne faciliteter i praksis bliver udbudt, vil afhænge af efterspørgslen efter disse.

De omtalte nøglecentre vil oftest være kommercielle virksomheder, men også offentlige myndigheder, organiationer m.v., kan beslutte at etablere en nøglecenterfunktion. Der vil være forskel på, hvilke produkttyper, de enkelte nøglecentre udbyder. I den forbindelse vil nogle nøglecentre alene tilbyde udstedelse af certifikater, men vil forudsætte, at kunden anskaffer selve den elektroniske signatur (nøgleparret) andetsteds. Andre vil tilbyde begge dele. Nogle nøglecentre vil tilbyde tidsstemplingsfunktioner, men det vil formentlig ikke være alle nøglecentre, der tilbyder dette.

Der kan desuden være stor forskel på, hvordan nøglecentrene i praksis indrettes, herunder hvilke IT-løsninger og sikkerhedsprocedurer de anvender.

En virksomhed, der fungerer som nøglecenter, kan også udøve virksomhed på en række andre områder. Oplagte eksempler er virksomhed inden for kredit- og betalingskort-området, eller andre former for finansiel virksomhed, eller posthåndterings-virksomhed.

Det skal også understreges, at der er tale om et marked og nogle produkter, som først nu er under udvikling, og hvor den anvendte teknologi konstant ændrer sig. Det indebærer også, at beskrivelsen ovenfor af, hvordan en elektronisk signatur og elektroniske signatur certifikater fungerer i dag, alene er et øjebliksbillede, og ikke nødvendigvis vil have gyldighed om 1, 5 eller 10 år.

3. Bruger-interesser i forbindelse med anvendelse af elektronisk signatur og elektroniske signatur certifikater

Som nævnt indledningsvis er brugernes hovedinteresse, at man, når man kommunikerer gennem åbne digitale net som f.eks. Internettet, kan være sikker på, hvem det er, man kommunikerer med, og at indholdet af det kommunikerede ikke er blevet ændret undervejs eller efterfølgende. Det er som et element heri også afgørende efterfølgende at kunne dokumentere, hvad der er sket og hvornår.

Set fra en brugervinkel afhænger sikkerheden – både som afsender og modtager – af følgende forhold:

I) Hvordan og hvor omhyggeligt nøglecentret efterprøver underskriverens identitet forud for udstedelsen.

II) Hvor sikre og omhyggelige nøglecentrets 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.

III) At certifikatets oplysninger om ovennævnte er korrekte og fyldestgørende.

IV) Hvordan nøglecentrets 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 nøglecentret, og dette har ført til tab hos enten afsender eller modtager.

V) 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.

Hvor betydningsfulde ovennævnte forhold er, afhænger af, hvad signaturen ønskes brugt til.

4. I hvilke sammenhænge vil elektroniske signaturer og elektroniske signatur certifikater blive anvendt ?

De seneste års hastige udvikling på det informationsteknologiske område, herunder sammensmeltningen af elektronisk databehandling (edb) og telekommunikation, har medført en øget udbredelse af digital kommunikation i samfundslivet. Brugen af elektronisk post, informationsudveksling og en række andre former for transaktioner via Internettet er kraftigt stigende.

I relation til offentlige myndigheder giver den elektroniske kommunikation mulighed for mere effektiv kommunikation mellem offentlige myndigheder og private borgere og virksomheder. Eksempelvis udvikles der i disse år stadig flere digitale selvbetjeningssystemer, der giver borgerne mulighed for at indgive deres selvangivelse, indsende SU-ansøgninger og -indberetninger, bestille et sygesikringsbevis, pas eller kørekort, indsende byggetilladelsesansøgninger eller flyttemeddelelser eller modtage en elektronisk recept fra lægen f.eks. som opfølgning på en telefonisk konsultation etc., fra en pc i hjemmet eller på arbejdspladsen, eller fra en offentlig info-kiosk.

Forskningsministeriets pilotprojekter med anvendelse af elektroniske signaturer i det offentlige indeholder en række praktiske eksempler på, hvordan elektroniske signaturer kan anvendes i kombination med f.eks. studiekort, SU-udbetaling og –indberetning, udveksling af patientoplysninger, patientjournaler og sygesikringsafregning mellem en række sundhedsinstitutioner. De erfaringer, der høstes i pilotprojekterne, er af stor betydning for opbygningen af en universel infrastruktur for elektroniske signaturer. Projekterne har afsløret mange af de problemstillinger, der opstår, når elektroniske signaturer skal anvendes i praksis.

Inden for erhvervslivet ser man især en stigende udnyttelse af teknologien i forbindelse med elektronisk handel, dvs. aftaleindgåelse og betalingsoverførsel via elektroniske medier, herunder til automatisk udveksling af forretningsdokumenter som f.eks. ordrer og fakturaer (eksempelvis via EDI - Electronic Data Interchange).

Elektronisk udveksling af data mellem erhvervsvirksomheder foregår i dag i en række situationer i såkaldte lukkede systemer, hvor parterne på forhånd har indgået aftale om sikkerhedsaspekter, udvekslingsformater m.v. De fælles standarder for elektronisk datauveksling er et eksempel på et sæt spilleregler, der kan anvendes i sådanne lukkede systemer. Handler man ofte med hinanden, så kan det give mening at indgå sådanne rammeaftaler. Men den løsningsmodel er ikke anvendelig, hvis ønsket er, at principielt alle virksomheder, myndigheder og privatpersoner på nettet indbyrdes skal kunne foretage juridisk bindende dispositioner, f.eks. foretage en enkelt bestilling eller indgå en enkeltstående aftale, uanset om de tidligere har været i kontakt med hinanden eller ej.

Der er derfor en stigende efterspørgsel fra erhvervsside efter en regulering, der kan sikre betryggende rammer for, at man kan foretage juridisk bindende dispositioner via åbne net som f.eks. Internettet uden først at skulle aftale med modtageren, hvordan man gør.

Det er imidlertid ikke kun dansk erhvervsliv, der er interesseret i elektronisk kommunikation. Også private borgere ønsker i stigende omfang at bruge Internettet i kommercielle sammenhænge, dvs. ved bestilling og køb af varer og tjenesteydelser.

I nogle situationer foregår den nævnte kommunikation allerede i dag helt uden brug af en elektronisk signatur. Dette gælder navnlig mindre omfattende dispositioner. Også i de situationer, hvor man ønsker at anvende en elektronisk signatur, er der forskel på den økonomiske risiko, som man løber, og de eventuelle tab der kan opstå m.v.

Tendensen er derfor også, at der udvikles en række elektronisk signaturer og tilhørende certifikater med et gradueret sikkerhedsniveau, som er skræddersyet til forskellige typer anvendelse.

Som borger er det derfor også sandsynligt, at man vil råde over forskellige digitale certifikater og signaturgenereringsdata til forskellige formål, herunder f.eks. til private »små-indkøb«, til kommunikation med det offentlige, eller i arbejdssammenhæng.

Det bør i vidt omfang overlades til markedet selv at sørge for, at der etableres nøglecentre, og at de løsninger, de udbyder, er tilstrækkelig sikre set i relation til de situationer, hvori de tænkes anvendt. Når dette er udgangspunktet, skyldes det ikke mindst, at der fortsat er tale om et marked, som er inde i en rivende udvikling, og hvor en for intensiv offentlig regulering med stor sikkerhed vil hæmme og bremse produktudviklingen. Der vil desuden være stort behov for i givet fald at skulle opdatere denne regulering i takt med de seneste tekniske landvindinger.

Samtidig er der imidlertid tale om et nyt marked med produkter af en sådan teknisk kompleksitet, at det er særdeles vanskeligt for den enkelte private bruger at gennemskue, om man får et produkt med den fornødne sikkerhed.

Der findes på nuværende tidspunkt ingen regulering af virksomheder, der ønsker at udbyde certifikater og elektroniske signaturer.

5. Lovreguleringens rolle i forhold til elektroniske signatur certifikater

Lovforslagets primære sigte er at etablere en fleksibel tilsyns- og kontrolordning for nøglecentre, der ønsker at udbyde certifikater med betegnelsen kvalificerede certifikater, og i tilknytning hertil at regulere de pågældende nøglecentres erstatningsansvar overfor henholdsvis underskrivere og modtagere af kvalificerede certifikater.

Tilsynsordningen indebærer, at de omfattede nøglecentre løbende skal dokumentere, at deres virksomhed og de certifikater, de udsteder, overholder en række minimumskrav, der kan sikre et udbud af løsninger af fornøden kvalitet på det danske marked. De minimumskrav, der opstilles, vedrører punkt I-III i afsnit 2 ovenfor, dvs. sikring af kvaliteten af elektronisk signatur certifikaterne. Overholdes reglerne ikke, vil et nøglecenter kunne miste retten til at anvende det offentligt anerkendte begreb kvalificerede certifikater om deres certifikatprodukter.

For så vidt angår reguleringen af, i hvilket omfang nøglecenteret er ansvarlig i forbindelse med fejl, der opstår på grund af manglende overholdelse af de fastsatte minimumskrav (punkt IV i afsnit 2), er sigtet et culpaansvar med omvendt bevisbyrde.

Tilsynsordningen og ansvarsreguleringen vil ikke omfatte alle de certifikater, der udbydes, eller alle nøglecentre på markedet, men omfatter kun certifikater, som et nøglecenter vælger at benævne »kvalificerede certifikater«. Et nøglecenter vil som led i sin samlede virksomhed kunne udbyde både kvalificerede certifikater, og andre certifikater, herunder også certifikater, som i praksis opfylder lovens minimumskrav, men ikke benævnes kvalificerede certifikater.

Lovforslaget omfatter certifikater, der anvendes i forbindelse med offentligt tilgængelige systemer, men ikke løsninger, der alene anvendes i lukkede net, hvor de deltagende parter indbyrdes har aftalt »spillereglerne«. Denne del af anvendelsen af elektronisk signatur certifikater er derfor ikke omfattet af tilsyns- og erstatningsansvarsreglerne.

6. Lovreguleringens rolle i forhold til elektroniske signaturer

Den ovenfor beskrevne tilsynsordning og den tilhørende regulering af erstatningsansvaret vedrører nøglecentrenes udstedelse af selve elektronisk signatur certifikaterne.

Som beskrevet ovenfor i afsnit 2 er der et andet væsentligt sikkerhedsaspekt forbundet med anvendelsen af elektroniske signaturer, nemlig kvaliteten af selve det nøglepar, der anvendes (også benævnt signaturgenererings- og signaturverificeringsdataene), og den måde hvorpå navnlig den private nøgle anvendes og opbevares (på et plastikkort eller som del af et computerprogram) (også benævnt signaturgenereringssystemet).

I nogle tilfælde vil også signaturgenererings produktet være leveret af nøglecentret, men det vil ikke altid være tilfældet.

Lovforslaget opstiller, i overensstemmelse med det underliggende EF-direktiv om en fællesskabsramme for elektroniske signaturer (direktivet er optrykt som bilag 1 til forslaget og benævnes i det følgende »direktivet« eller »EF-direktivet«), en række grundlæggende krav til signaturgenereringssystemer, der af producenten/leverandøren ønskes benævnt »sikre signaturgenereringssystemer«, således som dette begreb er defineret i EF-direktivet. Lovforslaget indeholder i forlængelse heraf hjemmel til at udpege et eller flere egnede organer eller myndigheder, der vil kunne medvirke til at efterprøve og dokumentere, hvorvidt konkrete produkter lever op til disse minimumskrav.

De pågældende minimumskrav er meget generelt udformede og fokuserer primært på at opstille funktionelle minimumskrav, bl.a. for i videst muligt omfang at sikre en teknologineutral og dermed robust regulering. Dette er nødvendigt, idet der endnu er tale om en teknologi – eller flere konkurrerende teknologier - på et forholdsvis tidligt udviklingsstadie, hvor de teknologiske løsninger konstant forandrer sig, og hvor det derfor ville være umuligt både at gennemføre en stabil regulering, og at fastsætte meget specifikke tekniske minimumskrav.

Det kan, som led i den pågældende udvikling, også tænkes, at der på sigt opstår autentifikationsmetoder, der helt kan erstatte de digital signatur løsninger, vi kender i dag.

Den herved muliggjorte »mærkning« af specifikke signaturgenereringssystemer vil være vejledende for brugere, der ønsker at anskaffe sig et produkt, som de kan have tillid til, og er desuden af betydning i relation til reguleringen af retsvirkningsproblematikken, jf. afsnit E, pkt. 9, nedenfor.

B. Gældende lovgivning

Der findes på nuværende tidspunkt ingen lovgivning om udstedelse af certifikater, der kan anvendes i forbindelse med elektroniske signaturer (nøglecentervirksomhed) i Danmark. Nøglecentre fastlægger selv efter hvilke retningslinjer, de vil udstede certifikater, hvordan de vil kontrollere underskriverens identitet, og er ikke underlagt nogen særlig erstatningsordning, såfremt der er fejl i certifikatet, dette ikke spærres i rette tid eller lignende.

Hvis der sker fejl i forbindelse med udstedelsen eller brugen af det certifikat, der knytter underskriveren og den elektroniske signatur sammen, må forholdet på nuværende tidspunkt bedømmes efter de almindelige erstatningsretlige regler. Det betyder, at det er skadelidte, der må påvise, at der fra nøglecentrets side er begået fejl i forbindelse med udstedelsen eller håndteringen af certifikatet.

C. Danske tiltag i relation til elektroniske signaturer

Den 28. januar 1998 blev der i Folketinget gennemført en redegørelsesdebat om sikker digital kommunikation. Redegørelsen blev afgivet af forsknings-, erhvervs-, justits-, økonomi- og skatteministeren med Forskningsministeriet som hovedansvarlig.

Redegørelsens udgangspunkt var en konstatering af en markant efterspørgsel fra såvel erhvervsliv, offentlige myndigheder som private brugere efter lovgivningsmæssige rammer, der kan sikre betryggende rammer for, at man foretager bindende juridiske dispositioner via nettet.

Debatten i Folketinget viste et udtrykt ønske om at skabe en lovgivningsmæssig ramme for anvendelsen af elektroniske signaturer, der sikrer høj kvalitet og herved etablerer grundlaget for en praktisk ligestilling af digital og papirbaseret kommunikation. Det blev understreget, at brug af elektronisk kommunikation til bindende juridiske dispositioner forudsætter, at der kan kommunikeres med sikkerhed for såvel afsenders som modtagers identitet, indholdets integritet og ofte tillige med sikkerhed for fortrolighed i forhold til andre. Der skal med andre ord foreligge solide tekniske løsninger.

Debatten viste også, at der er behov for via lovgivning at gøre op med nøglecentrets ansvar. Ønsket var, at der skulle anlægges en forbrugermæssig synsvinkel på dette spørgsmål. Reguleringen skal give sikre, men samtidig enkle og brugervenlige systemer, og der skal findes en balance mellem beskyttelse af brugerne og afgrænsning af nøglecentrets ansvar. Man ønskede, at der etableres det fornødne lovgivningsmæssige grundlag for etablering af nøglecentre, der kan udbyde solide kvalitetsløsninger, og at der i denne lovgivning fastlægges klare regler for nøglecentrets ansvar og hæftelse i forbindelse med udstedelse af certifikater til brug i kombination med digitale signaturer.

Forskningsministeriet udsendte på baggrund af debatten i Folketinget i februar 1998 et udkast til et lovforslag om digitale signaturer i offentlig høring. Lovforslaget havde to hovedelementer. For det første et oplæg til en autorisationsordning indeholdende en række minimumskrav til digital signatur certifikater og til nøglecentrene, der ønskede at opnå autorisation, og den blåstempling der ville ligge heri. Autorisationsordningen var kombineret med en restriktiv regulering af de autoriserede nøglecentres erstatningsansvar i situationer, hvor de offentligt regulerede minimumskrav ikke var overholdt i form af objektivt ansvar for tab opstået som følge heraf.

For det andet indeholdt lovforslaget forslag til regulering af retsvirkningerne af anvendelse af digitale signaturer i form af en ligestilling af digitale signaturer med håndskrevne underskrifter. Lovforslaget indeholdt to alternative modeller for, hvordan sidstnævnte i praksis ville kunne gennemføres.

Høringssvarene til dette første lovudkast gjorde det klart, at der var behov for at bearbejde spørgsmålet om eventuel lovregulering af digitale signaturers retsvirkning på områder med formkrav, f.eks. krav om anvendelse af underskrift eller skriftlighed, yderligere. Høringsprocessen gjorde det også tydeligt, at overvejelserne om lovgivning herom ville have tæt sammenhæng med en række tværgående juridiske problemstillinger og bl.a. ville berøre den generelle formuerets-, aftale- og forbrugerbeskyttelseslovgivning, som sorterer under Justitsministeriet.

Det blev derfor besluttet at foretaget en opdeling af arbejdet med at få gennemført lovgivning om anvendelsen af elektroniske signaturer og elektroniske signatur certifikater mellem Justitsministeriet og Forskningsministeriet, således at Justitsministeriet overtog ansvaret for regulering af problemstillingerne i tilknytning til retsvirkningerne af anvendelse af elektroniske signaturer. Med sigte herpå har Justitsministeriet bl.a. nedsat et udvalg, hvori også Forskningsministeriet er repræsenteret, som nærmere skal overveje behovet for at lovgive om, i hvilket omfang elektroniske meddelelser kan/skal bruges på områder med formkrav som nævnt ovenfor, og om retsvirkningerne mellem afsender og modtager i visse nærmere afgrænsede situationer. Udvalgets arbejde er endnu ikke afsluttet.

Høringssvarene gjorde det desuden klart, at der var behov for en yderligere bearbejdning af lovforslagets bestemmelser om autorisation og erstatningsansvar og for at se disse i et internationalt perspektiv, ikke mindst fordi markedet for certifikater og elektroniske signaturer i vidt omfang vil være internationalt og præget af udbud af grænseoverskridende løsninger. En række af høringssvarene påpegede derfor også, at der var behov for at afbalancere den danske regulering i forhold til den regulering, der ville være gældende i andre lande, såfremt man ønskede at fremme, at der også her i landet blev etableret nøglecentre.

D. Den internationale udvikling

Fastlæggelse af rammer for elektroniske signaturer er ikke et isoleret dansk fænomen. Der er i vidt omfang tale om systemer, som skal kunne fungere også globalt, såfremt erhvervsliv og brugere fuldt ud skal kunne udnytte de fordele, systemerne giver.

Det er derfor også relevant at se på, hvor langt andre lande er kommet med hensyn til regulering af elektroniske signatur og hvilke initiativer, der er i støbeskeen i de forskellige internationale samarbejdsfora som f.eks. EU, FN, WTO og OECD.

På den internationale scene har de regulatoriske aktiviteter angående elektroniske signaturer primært været koncentreret omkring Det Internationale Handelskammer (ICC – the International Chamber of Commerce), OECD og UNCITRAL (United Nations Commission om International Trade Law) og EU.

EF-direktivet om en fællesskabsramme for elektroniske signaturer

Direktivet blev endeligt vedtaget den 13. december 1999 og er en opfølgning på to meddelelser fra Kommissionen om elektronisk handel og om kryptering og digital signatur fra henholdsvis april og oktober 1997.

Hovedlinjerne i direktivet

Baggrunden for direktivet er, at Kommissionen er af den opfattelse, at det er en forudsætning for en acceleration af elektronisk handel, at der etableres betryggende rammer for, at man kan foretage juridisk bindende dispositioner via åbne net, som f.eks. Internettet, uden at afsender og modtager først skal aftale, hvordan man gør. Brug af elektronisk kommunikation

til bindende juridiske dispositioner forudsætter, at der kan kommunikeres med sikkerhed for afsenders identitet og for, at indholdet ikke er blevet ændret.

Formålet med direktivet er at lette anvendelsen af elektroniske signaturer samt at medvirke til deres juridiske anerkendelse. Direktivet tilvejebringer en ramme for elektroniske signaturer og de tilknyttede certificeringstjenester m.v. med henblik på at sikre det indre marked med hensyn til elektroniske signaturer.

Anvendelsesområde

Direktivets anvendelsesområde er elektroniske signaturer. Direktivet opererer med en meget bred definition af en elektronisk signatur, idet det definerer en elektronisk signatur som data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre elektroniske data, og som anvendes til autentifikation.

Samtidig opererer direktivet med begrebet »en avanceret elektronisk signatur«, som er en elektronisk signatur, der skal 1) være entydigt knyttet til underskriveren, 2) kunne identificere underskriveren, 3) tilvejebringes med midler, som underskriveren kan bevare den fulde kontrol med, og 4) være knyttet til de data, som den vedrører på en sådan måde, at enhver efterfølgende ændring i disse data kan opdages.

Sondringen mellem en elektronisk signatur og en avanceret elektronisk signatur har betydning for direktivets bestemmelser om retsvirkninger (se nedenfor).

Det er overladt til medlemsstaterne at bestemme på hvilke retsområder, man i lovgivningen vil tillade brugen af elektronisk kommunikation og elektroniske signaturer.

Elektronisk kommunikation i lukkede systemer er ikke omfattet af direktivets generelle regulering. I de tilfælde, hvor parterne på forhånd har indgået en kommunikationsaftale, har denne aftale forrang. Elektroniske signaturer afgivet inden for sådanne systemer må dog ikke udelukkes fra at opnå de retsvirkninger, der fastlægges i direktivet.

Fastlæggelse af en række krav til nøglecentrene og elektroniske signaturer

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 (nøglecentre er i direktivet kaldet certificeringstjenesteudbydere) af såkaldte kvalificerede certifikater til elektroniske signaturer. I den efterfølgende gennemgang af direktivet bruges direktivets betegnelse for disse certifikater.

Nøglecentre er ifølge direktivet en person eller et organ, der udsteder certifikater eller leverer andre tjenesteydelser i forbindelse med elektronisk signatur til offentligheden. Dette betyder bl.a., at tjenesteudbydere, som ikke tilbyder certificering, alligevel bliver omfattet af visse af direktivets regler, hvis de tilbyder »tilknyttede« tjenester, f.eks. tidsstempling af elektronisk post. Direktivet angiver i bilag II en række grundlæggende krav til sådanne udbydere.

Et certifikat til en elektronisk signatur er ifølge direktivet en digital attestering, som knytter et signaturverificeringssystem til en person og bekræfter denne persons identitet.

Et kvalificeret certifikat er ifølge direktivet et certifikat, der opfylder kravene til kvalificerede certifikater i bilag I, og som udstedes af et nøglecenter, der opfylder kravene i bilag II.

Direktivet fastlægger regler for nøglecentrets ansvar over for »enhver person, som med rimelighed forlader sig på certifikatet«. Europa-Kommissionen har præciseret, at denne personkreds også omfatter underskriveren.

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

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

Ansvarsreglerne skal bygge på et princip om, at nøglecentret i det mindste skal have handlet uagtsomt for at ifalde erstatningsansvar i de tre ovennævnte tilfælde. Ifølge direktivet er bevisbyrden for at bevise, at der ikke er handlet uagtsomt, pålagt nøglecentret.

Medlemsstaterne skal herudover sikre, at nøglecentre, der udsteder kvalificerede certifikater, er erstatningsansvarlige for tab, der opstår som følge af manglende spærring af certifikatet, medmindre nøglecentret kan bevise, at der ikke er handlet uagtsomt.

Direktivet indeholder ingen regulering af ansvarsforholdet mellem underskriver og modtager af en elektronisk signatur.

Medlemsstaterne skal sikre, at certificeringstjenesteudbydere samt nationale akkrediterings- og tilsynsorganer opfylder det generelle EF-direktiv 97/46/EF

om persondatabeskyttelse. Det bestemmes, at certificeringstjenesteudbyderen 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.

Et åbent marked

Direktivet indeholder et forbud mod forudgående autorisation af nøglecentre som en betingelse for at kunne udbyde certificeringstjenester til elektroniske signaturer.

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.

Dette skal sikre, at nøglecentrene får mulighed for at udbyde deres produkter på tværs af grænserne i hele EU, med det resultat at den samlede konkurrence på dette specielle område styrkes til fordel for forbrugerne og erhvervslivet. De må derved formodes at få tilbudt en række produkter, der kan give nye muligheder for sikker elektroniske informationsudveksling. Et frit marked vil således stimulere udbudet af certificeringstjenesteydelser i hele EU.

Der indføres dog samtidig en pligt for medlemsstaterne til at etablere et passende tilsyn med nøglecentre, der udsteder kvalificerede certifikater til elektroniske signaturer. Der åbnes mulighed for, at medlemsstaterne kan overlade etableringen af sådanne systemer til markedsaktørerne i form af selv-regulering.

Medlemsstaterne skal anerkende certifikater, udstedt af certificeringstjenesteudbydere fra lande uden for EØS, på lige fod med certifikater udstedt af certificeringstjenesteudbydere fra EØS hvis 1) tredjelands-nøglecenter opfylder direktivets krav og er akkrediteret i forbindelse med en frivillig akkrediteringsordning i et EU-land, 2) hvis et EU-nøglecenter, der opfylder direktivets krav, indestår for tredjelandsudbyderens certifikater, eller 3) hvis tredjelands-certifikatet eller tredjelands-udbyderen er anerkendt i henhold til en international aftale.

Retlig anerkendelse af elektroniske signaturer

Direktivet indeholder i et vist omfang regler om retsvirkningerne af elektroniske signaturer. Direktivet indeholder således 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 signaturers retsvirkninger m.v., alene fordi de er i elektronisk form. Forbudet betyder derimod ikke, at medlemsstaterne ikke af andre årsager kan behandle elektroniske signaturer anderledes end håndskrevne underskrifter. Er en elektronisk signatur f.eks. udvirket ved en teknik, som kun yder en meget begrænset beskyttelse mod forfalskninger m.v., vil det således ikke være i strid med »diskriminationsforbudet« at behandle sådanne signaturer anderledes end håndskrevne underskrifter på grund af det lave sikkerhedsniveau.

Direktivet indeholder også en bestemmelse om, at anvendelse af de ovennævnte »avancerede« elektroniske signaturer, dvs. elektroniske signaturer, som lever op til særligt strenge sikkerhedskrav, skal anses for at opfylde formkrav om underskrift på papirdokumenter. Dette gælder dog, hvis en medlemsstat anerkender anvendelsen af elektroniske signaturer i den pågældende sammenhæng.

Det vil, som anført ovenfor således fortsat være op til medlemsstaterne at bestemme, på hvilke områder man vil acceptere brugen af elektronisk kommunikation og elektroniske signaturer. Bestemmelsen indebærer imidlertid, at medlemsstaterne på de områder, hvor man efter national ret stiller krav om signatur på elektroniske meddelelser, skal acceptere, at avancerede elektroniske signaturer opfylder dette krav. Ved kommunikation med det offentlige giver direktivet dog mulighed for, at medlemsstaterne kan stille strengere sikkerhedskrav til de elektroniske signaturer, hvis disse krav er objektive, gennemsigtige, rimelige og ikke-diskriminerende.

Endelig indeholder direktivet en regel om, at medlemsstaterne skal sikre, at »avancerede« elektroniske signaturer kan anvendes som bevis ved retshandlinger. I præamblen til direktivet er det præciseret, at reglerne ikke ændrer på princippet om retternes frie bevisbedømmelse.

Den danske procedure vedrørende direktivet

Direktivforslaget har været forelagt Folketingets Europaudvalg den 15. maj 1998 med Forskningsministeriets notat af 7. maj 1998 forud for Rådsmødet (telekommunikation) den 19. maj 1998.

Direktivforslaget har endvidere været omtalt i Forskningsministeriets samlenotat af 13. november 1998 med henblik på orientering af Folketingets Europaudvalg forud for Rådsmødet (telekommunikation) den 27. november 1998. Direktivforslaget har endvidere været nævnt i referat til Folketingets Europaud-

valg af Rådsmøde (telekommunikation) den 27. november 1998.

Nordisk samarbejde vedrørende lovgivning om elektroniske signaturer

Forskningsministeriet har deltaget i et uformelt samarbejde mellem de relevante myndigheder i Norge, Sverige, Finland og Island med henblik på at udveksle erfaringer og for at tilstræbe at skabe en lighed mellem lovgivningen i de enkelte lande, hvor det har været muligt.

Sverige har sendt et udkast til en ny lag om certifikat för elektroniske signaturer i høring og forventer i løbet af nogle måneder at kunne fremsætte et forslag i Riksdagen.

Det svenske udkast er på mange måder lig dette forslag. I modsætning til forslaget har man dog i Sverige ønsket at anvende en mindre omfattende tilsynsordning, som bygger på et princip om, at nøglecentre, der ønsker at udstede kvalificerede certifikater, selv deklarerer, at de opfylder kravene i lovgivningen. Som tilsynsmyndighed er foreslået den svenske Post- og Telestyrelse. Tilsynet vil kunne stille krav til nøglecentrene om udlevering af oplysninger med henblik på at kunne kontrollere overholdelsen af loven.

Norge har netop sendt et forslag til lov om elektroniske signaturer mv. i offentlig høring og forventer at kunne fremsætte et forslag i Stortinget til efteråret. Det norske udkast minder ligesom det svenske på mange måder om dette forslag. Ud fra et ønske om ikke at pålægge nøglecentre for store administrative byrder har Norge valgt en tilsynsmodel svarende til den svenske.

Finland og Island arbejder ligeledes i øjeblikket med at færdiggøre udkast til lovgivning, som kan sendes i høring. Finland har allerede gennemført dele af direktivet i 1998 med vedtagelsen af en lov om elektronisk kommunikation.

Øvrige internationale tiltag

Det internationale handelskammer (ICC) har i 1997 lavet et sæt retningslinjer for bedste praksis inden for certificering og sikring af elektronisk handel. Retningslinjernes primære målgruppe er de erhvervsdrivende og samhandlen dem imellem.

Retningslinjerne er hovedsageligt baseret på UNCITRAL's modellov om elektronisk handel.

FNs handelsretskommission, UNCITRAL, har i juni 1996 vedtaget en modellov om elektronisk handel. Modelloven er baseret på den grundtanke, at elektronisk handel kræver, at digitale meddelelser sidestilles med papirmeddelelser, hvis ellers de funktioner, som papiret sikrer, sikres mindst ligeså godt digitalt. Denne tanke om funktionel ækvivalens udtrykkes i modellovens regler i artiklerne 5 - 7 om kravene til blandt andet skriftlighed og underskrift.

Modellovens artikel 5 angiver, at elektroniske meddelelser ikke må frakendes juridisk anerkendelse alene af den grund, at de foreligger i elektronisk form. For skriftlighedskrav anfører modelloven i artikel 6, at disse bør være opfyldt, når den elektroniske information foreligger i en sådan form, at den kan genskabes ved senere lejlighed. Underskriftskrav bør være opfyldt af digital kommunikation, når der benyttes en teknik til sikring af personens identitet og af personens vedkendelse af indholdet. Denne underskriftsteknik skal være så troværdig, som formålet med den pågældende kommunikation måtte kræve.

UNCITRAL har efterfølgende nedsat en arbejdsgruppe om digital signatur, der skal søge at formulere retningslinjer for digital signatur og anden elektronisk identifikation. Arbejdsgruppen holdt senest møde i Wien den 19.- 30. januar 1998.

OECD har i en rekommandation af 27. marts 1997 opfordret medlemslandene til at fjerne eller undgå at skabe unødige forhindringer for digital kommunikation af hensyn til en krypteringspolitik.

OECD udsendte også i 1997 en rapport om certificering i det elektroniske miljø og en anden rapport om politik og teknologiens muligheder for certificering af information i et globalt netværk. Denne rapport blev fulgt op af yderligere en rapport i 1998. Disse dokumenter giver et overblik over retningen i den teknologiske udvikling og vigtige politiske områder inden for området.

Der er i en række enkeltlande initiativer undervejs til fremme af digital kommunikation. Der er dog betydelig uklarhed med hensyn til det konkrete indhold af de forskellige landes kommende lovgivning om f.eks. digital signatur.

I USA har en række delstater vedtaget lovgivning om digitale signaturer. I Utah vedtoges den første egentlige lovgivning om digitale signaturer med regulering både af nøglecentre og retsvirkning af digitale signaturer. Siden har en række andre enkeltstater fulgt op med lovgivningstiltag af meget forskellig rækkevidde og indhold. På føderalt niveau er der dog fortsat uklarhed om, hvilke initiativer den amerikanske forbundsregering vil tage med hensyn til digitale signaturer.

I Europa har Italien, Tyskland, Frankrig og Østrig vedtaget national lovgivning om henholdsvis elektroniske dokumenter/kontrakter og digital signatur.

Sammenfattende kan situationen beskrives således, at der er en række initiativer undervejs såvel nationalt

som i de internationale samarbejdsfora. EF-direktivet om elektroniske signaturer giver et klart pejlemærke for, hvor den internationale regulering vil bevæge sig i retning af.

E. Indholdet af lovforslaget

1. Lovens anvendelsesområde

Lovens territoriale anvendelsesområde er nøglecentre, der er etableret i Danmark. Loven stiller ikke særlige krav til nøglecentre og elektroniske signaturer med oprindelse i andre lande inden for Det Europæiske Fællesskab, eller i tredjelande udenfor EU, men giver dog mulighed for, at disse kan anerkendes på samme måde som certifikater, som udstedes af danske nøglecentre.

Loven finder ikke anvendelse på certifikater og elektroniske signaturer, der udelukkende anvendes inden for lukkede systemer, der er baseret på frivillige aftaler mellem et begrænset antal deltagere.

2. Teknologineutralitet

Lovforslaget tager udgangspunkt i ønsket om at sikre en teknologineutral og robust regulering.

I forlængelse heraf er lovforslagets anvendelsesområde elektroniske signaturer og ikke alene digitale signaturer, som er den i dag fremherskende teknologi.

En elektronisk signatur er en teknisk foranstaltning, der giver samme funktionalitet som en almindelig håndskreven signatur, nemlig at den knytter en bestemt datamængde til en bestemt person. Elektroniske signaturer findes i flere forskellige varianter.

En digital signatur er den tekniske løsning for en elektronisk signatur, der er fremherskende på nuværende tidspunkt. En digital signatur giver sikkerhed for afsenders identitet, og at meddelelsen ikke er blevet ændret undervejs (integritet). En digital signatur frembringes ved hjælp af et edb-program, der bygger på anvendelse af public key-krypteringsteknik.

Public key kryptering er en særlig form for kryptering. Kryptering er en teknik til forvanskning af en informationsmængde efter et bestemt princip. Eksempelvis kan man erstatte hvert bogstav i en tekst med et bogstav en plads længere fremme i alfabetet. I nævnte eksempel bruges samme nøgle til at forvanske og bringe teksten tilbage igen. Ved public key-kryptering bruges derimod to principielt forskellige nøgler, der er forbundet med hinanden således, at en tekst, der er krypteret ved hjælp af den ene nøgle (uanset hvilken), kun kan dekrypteres ved hjælp af den anden nøgle. Navnet »public key« skyldes, at man gennem et sådant system kan etablere et nøglecenter, hos hvem den ene (offentlige) nøgle er registreret, og som overfor potentielle kommunikerende parter erklærer, hvilken person der råder over den pågældende nøgle. Ved hjælp af public key-kryptering kan der dermed gives en høj grad af sikkerhed for afsenders identitet, uden at man behøver at aftale koden eller udveksle nøgler på forhånd.

Der lægges således vægt på, at forslaget ikke alene skal omfatte digitale signaturer, men også skal omfatte fremtidige teknikker, der opfylder samme formål som public key-krypteringsteknikken, hvorved også andre former for digital identifikation kan rummes af forslaget.

Forslaget opererer med sigte herpå med en meget bred definition af en elektronisk signatur, idet en elektronisk signatur defineres som data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre elektroniske data, og som anvendes til autentifikation (identifikation).

Det er vigtigt at understrege, at elektronisk signatur markedet, ligesom så mange andre dele af IT-verdenen, er præget af en voldsom teknologisk udvikling. Det gør det meget vanskeligt at forudsige, hvordan dette marked vil udvikle sig. Det gør også, at billedet af teknologiens muligheder og måder at fungere på konstant ændrer sig, og at en omfattende og teknologispecifik regulering ikke er mulig.

3. Almindelige certifikater kontra kvalificerede certifikater

Der stilles i lovforslaget en række krav til nøglecentre, der udbyder såkaldte kvalificerede certifikater. Kravene omfatter både indholdet af et kvalificeret certifikat og de procedurer og forretningsgange, som nøglecentret anvender. Kravene skal sikre, at der skabes et tilstrækkeligt sikkerhedsniveau i relation til udstedelse og administration af disse certifikater.

Et kvalificeret certifikat er et certifikat, der indeholder de oplysninger, der er kræves i lovforslagets § 4, og som er udstedt af et nøglecenter, der opfylder bestemmelserne i lovforslagets kapitel 4 samt regler udstedt i medfør heraf.

Bestemmelserne er bl.a. en implementering af de krav, der stilles i direktivet til udbudet af »kvalificerede certifikater«.

Indeholder certifikatet en angivelse af, at det er et kvalificeret certifikat, og har det udstedende nøglecenter hjemsted i Danmark, skal kravene i denne lovgivning til udbud af kvalificerede certifikater overholdes.

Et kvalificeret certifikat skal bl.a. indeholde oplysninger, der gør det muligt at identificere underskriveren. Underskriveren (dvs. den person som generer sig-

naturen) er den fysiske eller juridiske person, der fremgår af certifikatet. Det er den person, der har kontrollen med et signaturgenereringssystem, og som besidder signaturgenereringsdataene (den private nøgle).

4. Krav til nøglecentrene der udbyder kvalificerede certifikater til elektroniske signaturer

Lovforslaget indeholder i kapitel 4 en række krav til de nøglecentre, der udbyder kvalificerede certifikater til elektroniske signaturer.

Bestemmelserne pålægger udbyderne af kvalificerede certifikater løbende at træffe de juridiske, organisatoriske, tekniske, personale-, drifts- og sikkerhedsmæssige foranstaltninger, som er nødvendige for, at der er tale om et sikkert og velfungerende udbud af elektroniske signaturer.

Det kræves herunder, at nøglecentre, der udsteder kvalificerede certifikater, skal beskæftige personale, som har den rette ekspertise, erfaringsgrundlag og kvalifikationer, som de tjenesteydelser, der udbydes, kræver. Det kan være forskelligt fra tjenesteudbyder til tjenesteudbyder afhængigt af hvilke ydelser, der udbydes. Personalet skal have sagkundskab inden for elektronisk signatur teknologi og indgående kendskab til etablering og vedligeholdelse af tilstrækkelige og korrekte sikkerhedsprocedurer. Personalet skal have kendskab til de systemer og produkter, der anvendes.

Nøglecentrene skal derudover til stadighed have tilstrækkelige økonomiske ressourcer til at kunne efterleve kravene i dette lovforslag, og herunder leve op til deres økonmiske erstatningsansvar i medfør af den særlige ansvarsregulering. Hvorvidt et nøglecenter har tilstrækkelige økonomiske ressourcer hertil vil bl.a. afhænge af, hvilke typer certifikater, der udbydes. Udbyder et nøglecenter eksempelvis certifikater til anvendelse inden for et område med store økonomiske konsekvenser for de involverede parter, eller certifikater uden formåls- eller beløbsbegrænsninger, må det økonomiske beredskab være tilsvarende højt.

Endelig skal nøglecentret som et helt centralt element i reguleringen overholde visse minimumskrav til, hvordan underskriverens identitet verificeres forud for udstedelse af et kvalificeret certifikat, med henblik på at sikre en betryggende kontrol heraf. Denne identitetskontrol er sammen med de regler, der sikrer betryggende procedurer for nøglecentrenes udformning, opbevaring og administration af certifikaterne, grundstammen i reguleringen af de kvalificerede certifikater. Se nærmere om denne reguelring i bemærkningerne til lovforslagets § 6.

Den systemrevisor, der ifølge lovforslaget skal være tilknyttet nøglecentret, skal årligt overfor Telestyrelsen afgive en vurdering af, om nøglecentret må anses for at overholde de opstillede regler og krav, ligesom nøglecentrets ledelse skal indestå herfor.

Lovforslaget indeholder de overordnede regler om de krav, der stilles til nøglecentre, der udbyder kvalificerede certifikater. Lovforslaget giver samtidig Forskningsministeren hjemmel til, på en række af de ovenfor nævnte områder at fastsætte nærmere regler om det præcise indhold af de krav, der stilles til nøglecentrene.

5. Tilsyn og anmeldelse

Telestyrelsen forudsættes at varetage det overordnede tilsyn med, at nøglecentre overholder lovens bestemmelser.

Telestyrelsen skal føre kontrol med, at kravene i loven til både nøglecentret og de certifikater, nøglecentret udsteder, overholdes. Ved at stille krav om at nøglecentre, der udsteder kvalificerede certifikater, underlægges et statsligt tilsyn, er det hensigten at sikre, at disse nøglecentre har et kvalitets- og sikkerhedsniveau, som brugerne kan have tillid til.

Hovedopgaven for Telestyrelsen vil bestå i at foretage en vurdering af de revisionsrapporter, som et nøglecenter skal indsende til Telestyrelsen, når nøglecentret påbegynder sin virksomhed og herefter i forbindelse med nøglecentrets årlige regnskabsaflæggelse.

Såfremt de oplysninger, som Telestyrelsen modtager fra nøglecentret, dets revision, brugerne eller andre, giver anledning til at betvivle, at nøglecentret overholder lovens krav, skal Telestyrelsen anvende en række reaktionsmuligheder beskrevet i loven.

I modsætning til det tilsyn der i dag føres med virksomheder på det finansielle område, er det ikke meningen, at Telestyrelsen skal foretage egentlige inspektioner af de tilsynsbelagte virksomheder.

Telestyrelsens reaktionsmuligheder omfatter:

I. at kunne afkræve nøglecentret alle relevante oplysninger til brug for sit tilsyn,
II. at kunne give nøglecentret pålæg om at bringe konkrete forhold i overensstemmelse med lovgivningen,
III. fastsætte tvangsbøder, hvis nøglecentret ikke efterkommer et pålæg,
IV. at kunne foranstalte en ekstraordinær revision af nøglecentret iværksat, samt
V. at kunne fratage nøglecentret mulighed for at anvende betegnelsen »kvalificerede certifikater« om sine produkter.

Der er ikke fundet behov for at give Telestyrelsen adgang til at foretage inspektioner af nøglecentrets forretningslokaler.

Nøglecentre, som ikke ønsker at udstede kvalificerede certifikater vil kunne oprettes frit og drive deres virksomhed i henhold til kvalitetskrav og standarder, som de selv vælger. Telestyrelsen fører dog også et tilsyn med, om de danske nøglecentre overholder bestemmelsen i § 12 vedrørende behandling af personoplysninger.

Ved at lade markedet for elektroniske signaturer være åbent for aktører, som ikke opfylder bestemte krav om at være under tilsyn, etc., sikres det, at en eventuel markedsudvikling, hvor private autorisationsordninger eller lignende ordninger måtte blive fremherskende, ikke bremses af en ufleksibel lovgivning.

Baggrunden for at indrette tilsynet som et revisionsbaseret system, hvor en vigtig del af det praktiske tilsyn udføres af den eksterne revision i nøglecentrene, er for det første at udnytte den erfaring og kompetence, som allerede findes i revisionsbranchen med at udføre systemrevision. Det kræver specialistviden at kunne overskue og bedømme den avancerede teknologi, som anvendes i et nøglecenter, og denne viden findes ikke i dag i Telestyrelsen.

For det andet vil opbygning af et større statsligt tilsyn kræve mange ressourcer, som forudsættes betalt af de tilsynsbelagte virksomheder. Dette kunne afholde nøglecentre fra at udstede kvalificerede certifikater, og på den måde risikeres det, at der ikke opstår et marked for elektroniske signaturer af en kvalitet, som forbrugere, myndigheder og virksomheder kan have tilstrækkelig tiltro til. Det vurderes, at de udgifter til revision, som med forslaget pålægges nøglecentrene, i højere grad kommer nøglecentret selv til gode i form af viden, kontrol og erfaringsudveksling med revisionen, end det ville være muligt under en statslig ordning.

Det foreslås, at udgifterne ved tilsynet på kort sigt finansieres af det offentligt, men at udgifterne på længere sigt bør afholdes af de nøglecentre, der udsteder kvalificerede certifikater.

6. Ansvarsregler

I lovforslagets § 11 fastlægges særlige ansvarsregler for nøglecentre, der udsteder kvalificerede certifikater.

Bestemmelsen fastlægger ansvaret i visse tilfælde, hvor en person, der med rimelighed forlader sig på et certifikat, lider tab på grund af nøglecentret. Det drejer sig om tab opstået som følge af fejl og mangler i oplysningerne i et certifikat, manglende spærring af et certifikat, manglende eller fejlagtige oplysninger vedrørende udløbsdatoen eller gældende anvendelsesbegrænsninger for certifikatet samt fejl i nøglecentrets kontrol af, at underskriveren er i besiddelse af de signaturgenereringsdata, som korresponderer med de signaturverificeringsdata, der er indeholdt i certifikatet.

Det er ifølge bestemmelserne pålagt nøglecentret at bevise, at der ikke er sket fejl, som kan tilregnes nøglecentret i forbindelse med udstedelsen af et kvalificeret certifikat til en elektronisk signatur, samt at oplysningerne i certifikatet er korrekte.

Nøglecentret er ligeledes ansvarligt for, at der stilles oplysninger til rådighed om certifikatets udløbsdato, spærring, begrænsninger af hvilke formål certifikatet kan anvendes til eller beløbsmæssige begrænsninger for certifikatet, og at disse oplysninger er korrekte.

Der er således tale om et culpaansvar med omvendt bevisbyrde eller et såkaldt præsumptionsansvar. Begrundelsen for at indføre dette skærpede ansvar for visse nøglecentre er områdets meget tekniske og komplicerede karakter. Det vil for den almindelige bruger af elektroniske signaturer være svært at påvise, at der er sket fejl i forbindelse med håndteringen af signaturtjenesterne. Reglerne har derved et forbrugerbeskyttende sigte. For at der kan pålægges nøglecentret et erstatningsansvar for tab lidt hos underskriveren eller tredjemand efter bestemmelserne i dette lovforslag, skal de øvrige betingelser for at pålægge et erstatningsansvar også være tilstede.

Forhold, som ikke er omfattet af det særlige skærpede ansvar i loven, vil fortsat skulle bedømmes efter dansk rets almindelige bestemmelser.

7. Beskyttelse af peronsoplysninger

Lovforslaget indeholder enkelte supplerende bestemmelser til den gældende lovgivning om beskyttelse af personoplysninger.

Bestemmelserne i lovforslaget angående beskyttelse af persondata gælder for alle nøglecentre etableret i Danmark.

Ifølge forslaget må et nøglecenter kun indhente persondata 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.

Nøglecentret må ikke behandle eller videregive data til andet formål end i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat uden den registreredes udtrykkelige samtykke.

Det sikres herved, at de data, som indsamles af et nøglecenter uden kundernes samtykke, ikke anvendes til f.eks. markedsføring.

8. Sikre signaturgenereringssystemer

Forslaget indeholder, som der er redegjort for ovenfor i afsnit A, underafsnit 5, endvidere en nærmere regulering af minimumskravene til signaturgenereringssystemer, der ønskes benævnt »sikre signaturgenereringssystemer«. Grundlaget herfor er direktivets bilag III, der indeholder en række funktionelle minimumskrav til sådanne signaturgenereringssystemer. Direktivet indeholder desuden en hjemmel til, at Europa-Kommissionen i samarbejde med medlemsstaterne kan træffe beslutning om, hvilke alment anerkendte internationale standarder for sådanne systemer, der anses for at leve op til direktivets minimumskrav. I det omfang der gennemføres en sådan uddybende regulering, vil denne i henhold til lovforslaget udgøre grundlaget også for danske myndigheder m.v.'s efterprøvelse af, om konkrete produkter lever op til de opstillede minimumskrav.

Det er herudover hensigten, at Europa-Kommissionen i samarbejde med medlemsstaterne, med hjemmel i bestemmelserne herom i direktivet, skal fastsætte nærmere fælles retningslinier for udpegningen af de organer eller offentlige myndigheder, der skal medvirke ved efterprøvelsen af, om konkrete signaturgenereringssystemer opfylder de opstillede minimumskrav. Lovforslaget indeholder ligeledes hjemmel til gennemførelse af eventuelle fælles EF-regler herom, eller til gennemførelse af en særskilt dansk regulering heraf, i det omfang der ikke fastsættes fælles retningslinier. Det er ikke umiddelbart hensigten at udnytte hjemlen hertil i lovforslagets § 15, førend det er afklaret, hvorvidt Kommissionen har til hensigt at fremlægge forslag til fælles retningslinier, og der i givet fald er opnået enighed om indholdet af disse.

9. En generel regel om anvendelse af elektronisk signatur på områder med formkrav

Dansk ret indeholder ikke generelle regler om betydningen af, at man underskriver et dokument mv., ligesom der heller ikke findes nogen generel definition af, hvad der skal til, for at noget er en underskrift. På nogle områder indeholder lovgivningen imidlertid bestemmelser med formkrav, f.eks. om at et dokument skal være underskrevet. Bestemmelserne kan være udformet på forskellige måder og kan f.eks. suppleres med et krav om, at underskriftens rigtighed skal attesteres af vitterlighedsvidner. Som følge af bestemmelsernes forskellige udformning er det ikke sikkert, at en underskrift, der opfylder et underskriftskrav i ét regelsæt, også opfylder et sådant krav på et andet retsområde.

Når der kun på enkelte retsområder er fundet behov for at opstille mere detaljerede regler om, hvilke krav en underskrift skal opfylde, hænger det formentlig sammen med, at underskriften har en fast indarbejdet funktion og opleves som en dagligdags og velkendt handling. De midler, der anvendes til at afgive en underskrift (blyant, kuglepen m.v.), er endvidere teknisk ukomplicerede, og bortset fra læsefærdighed kræves der ikke en særlig viden eller adgang til tekniske hjælpemidler for at læse en underskrift.

Der er for så vidt ikke noget til hinder for på samme måde at overlade spørgsmålet om, hvad der udgør en elektronisk signatur, til regulering på hvert enkelt retsområde for sig. Regeringen har imidlertid fundet det mest hensigtsmæssigt, at der indføres en generel bestemmelse om, at ethvert lovbestemt formkrav om signatur på elektroniske meddelelser skal forstås således, at kravet kan opfyldes ved brug af en elektronisk signatur, som lever op til nogle nærmere beskrevne sikkerhedskrav.

Behovet for en sådan regel hænger sammen med, at direktivet om en fællesskabsramme for elektroniske signaturer i artikel 5, stk. 1, indeholder en regel om retsvirkningerne af elektronisk signatur, som bl.a. betyder, at signaturer, der lever op til visse sikkerhedskrav mv., skal anses for at opfylde krav i medlemsstaternes lovgivning om elektronisk signatur. Kun ved kommunikation med det offentlige indeholder direktivet (i artikel 3, stk. 7), en begrænset mulighed for at opstille strengere krav.

Med andre ord indføres der med direktivet en art europæisk standard for elektronisk signatur. Afgiver eller modtager man en signatur, der lever op til direktivets krav, skal man kunne regne med, at den opfylder formkrav om brug af elektronisk signatur i samtlige EU-lande.

En korrekt implementering af direktivet vil således forudsætte, at dansk lovgivning ikke indeholder formkrav om, at elektronisk signatur skal overholde strengere sikkerhedskrav mv. end, hvad der følger af direktivet. Dette sikres bedst ved at indføre en generel regel af det beskrevne indhold.

Hertil kommer, at det er noget mere kompliceret at tage stilling til, hvad der skal til for at opfylde et formkrav om elektronisk signatur, end når det drejer sig om et krav om en traditionel underskrift. Det skyldes, at en elektronisk signatur er baseret på metoder, der er teknisk komplicerede og svære at forstå for de fleste.

De krypteringsalgoritmer, som elektronisk signatur – i hvert fald i øjeblikket – bygger på, har forskellige

sikkerhedsniveauer, og forbedres endvidere løbende. En signatur, som er sikker i dag, vil måske ikke være det om 5 år, og nogle signaturer giver allerede fra begyndelsen en begrænset sikkerhed for, hvem underskriveren er, f.eks. fordi der kun er foretaget en overfladisk undersøgelse af dennes identitet i forbindelse med udstedelsen af certifikatet.

Sikkerhed for, at en signatur stammer fra den angivne underskriver, afhænger endvidere af en række forhold, som modtagerne af signaturen kun i begrænset omfang har mulighed for at kontrollere. Det drejer sig bl.a. om omstændighederne ved udstedelse af certifikatet og de sikkerhedsprocedurer, der knytter sig til brugen af signaturgenereringssystemet (PIN-koder mv.)

Som følge af de mange forskellige signaturtyper med forskellige grader af sikkerhed, vil et formkrav om brug af elektronisk signatur, som kan opfyldes af en hvilken som helst signatur, stort set være uden indhold, og det må på denne baggrund forventes, at det i langt de fleste tilfælde vil blive nødvendigt at give nærmere regler om, hvilke krav en elektronisk signatur skal leve op til for at kunne opfylde et bestemt formkrav i lovgivningen. En generel bestemmelse, der fastlægger indholdet af sådanne formkrav, vil lette udarbejdelsen af lovgivning på de områder, hvor man ønsker at indføre formkrav, der skal kunne opfyldes ved brug af elektronisk signatur. I stedet for, at man i hver retsregel for sig skal fastsætte teknisk prægede bestemmelser om, hvilke krav en elektronisk signatur skal leve op til for at opfylde formkravet, vil man i stedet kunne nøjes med at henvise til den foreslåede generelle bestemmelse.

Det er væsentligt at fremhæve, at den foreslåede bestemmelse ikke har betydning for spørgsmålet om, på hvilke retsområder man kan anvende elektronisk kommunikation. Reglen vil alene få virkning på de retsområder, hvor det efter de i øvrigt gældende regler er muligt at anvende elektronisk kommunikation. Om elektronisk kommunikation kan anvendes på et bestemt retsområde afhænger bl.a. af, om der findes formkrav, som alene kan opfyldes ved brug af papirdokumenter. Justitsministeriets udvalg om retsvirkningerne af digital signatur mv. overvejer i øjeblikket, om der er behov for et lovgivningsinitiativ med henblik på at gøre det muligt at anvende elektronisk kommunikation på alle områder, hvor dette er muligt og hensigtsmæssigt.

Direktivets artikel 5 fastsætter endvidere, at medlemsstaterne skal sikre, at elektronisk signatur kan anvendes som bevis under retssager. Dansk ret bygger på et princip om fri bevisførelse, hvilket betyder, at parterne i en retssag har ret til at føre enhver (relevant) omstændighed som bevis. Efter dansk ret er der således ikke noget til hinder for at benytte elektroniske dokumenter, elektroniske signaturer mv. som bevis under retssager, og det er derfor ikke nødvendigt med lovgivning for at leve op til direktivets krav på dette punkt.

Endelig indeholder direktivet i artikel 5, stk. 2, et generelt forbud mod at nægte elektronisk signatur retskraft, alene fordi signaturen er elektronisk eller ikke opfylder betingelserne for at være en »avanceret elektronisk signatur«. Det må antages, at bestemmelsen har virkning som en art »diskriminationsforbud«, som indebærer, at medlemsstaterne ikke kan fratage elektronisk signatur enhver retlig betydning, alene med den begrundelse, at den er elektronisk. Sådanne regler har tidligere kunnet findes i retssystemerne i andre europæiske lande. Dansk ret indeholder imidlertid ikke regler af dette indhold, og det vil derfor ikke være nødvendigt med lovgivning for at leve op til direktivets krav på dette punkt.

F. Lovens økonomiske, administrative, erhvervsmæssige og miljømæssige konsekvenser

Økonomiske og administrative konsekvenser for stat, kommuner og amtskommuner

Forslaget indebærer oprettelsen af et tilsyn med de nøglecentre, der ønsker at udbyde kvalificerede certifikater. Det foreslås, at Telestyrelsen skal fungere som tilsynsmyndighed. Der vil være behov for yderligere 2-3 årsværk i Telestyrelsen til varetagelse af denne opgave.

Forslaget giver Forskningsministeren hjemmel til at fastsætte regler om, at omkostningerne til dette tilsyn på sigt skal betales af de nøglecentre, der er omfattet heraf. Der er imidlertid behov for en statslig medfinansiering af tilsynsordningen for ikke at belaste markedet i den indledende etableringsfase. Lovforslaget forventes herudover ikke at medføre særlige økonomiske konsekvenser for staten.

Lovforslaget vil styrke mulighederne for i praksis at anvende elektroniske signaturer, også på områder, hvor der er tale om juridisk bindende dispositioner, og hvor der er behov for, at der er sikkerhed for, at der anvendes troværdige produkter (certifikater og signaturer). Det vil bl.a. gøre det muligt for offentlige myndigheder at tilbyde en række nye elektroniske funktioner og serviceydelser, hvor der er behov for, at myndighederne har sikkerhed for, hvem det er, man kommunikerer med, og hvad der kommunikeres om. Brug af elektroniske signaturer vil bl.a. gøre det muligt for offentlige myndigheder at tilbyde løsninger, hvor bor-

gerne via Internettet får adgang til elektroniske selvbetjeningsløsninger. Anvendelse heraf må samtidig på sigt forventes at reducere det administrative ressourceforbrug hos de pågældende offentlige myndigheder.

Administrative og økonomiske konsekvenser for erhvervslivet

Indførsel af en tilsynsordning og en klar regulering af ansvarsforholdet for de nøglecentre, som omfattes heraf, kan medvirke til at øge tilliden til anvendelse af elektroniske signaturer og certifikater og dermed skabe et bedre forretningsgrundlag for nøglecentrene.

Adgangen til elektronisk kommunikation baseret på fælles standarder og et højt sikkerhedsniveau ventes både at medføre rationaliseringsgevinster i den enkelte virksomhed og at øge virksomhedernes konkurrenceevne via en forbedret mulighed for elektronisk samspil med andre virksomheder. Ligeledes vil der forventeligt ske en lettelse af virksomhedernes administrative byrder gennem mulighed for elektronisk indberetning af oplysninger til det offentlige.

Miljømæssige konsekvenser

I takt med at lovforslaget slår igennem, vil det indebære klare miljøgevinster, herunder dels mindre ressourceforbrug til transport af meddelelser, dels besparelser i papirforbrug. Lovforslaget har ingen nævneværdige negative konsekvenser for miljøet.

Administrative konsekvenser for borgerne

De ovenfor beskrevne styrkede muligheder for at kommunikere elektronisk med offentlige myndigheder vil ligeledes udgøre en betydelig administrativ lettelse for borgerne.

G. Høring

Udkast til dette lovforslag har været sendt til høring hos Advokatsamfundet, Akademikernes Centralorganisation, Amtsrådsforeningen i Danmark, Arbejderbevægelsens Erhvervsråd, Arbejdsløshedskassen for selvstændige erhvervsdrivende i Danmark, Arbejdsmarkedsstyrelsen, Arbejdsministeriet, Arbejdsskadestyrelsen, Beredskabsstyrelsen, Brancheforeningen for telekommunikationsindustrien, Brancheorg. for Forbruger Elektronik, By- og Boligministeriet, Børsmæglerforeningen, Canal Digital Danmark A/S, Center for IT-forskning, Center for Ligebehandling af Handicappede, Center for Menneskerettigheder, Christian Rovsing A/S, Civilretsdirektoratet, Copy-Dan, CSC Datacentralen, Danmarks Aktive Forbrugere (DAF), Danmarks Nationalbank, Danmarks Radio, Danmarks Rederiforening, Danmarks Statistik, Dansk Autoriseret Markedsplads A/S, Dansk BiblioteksCenter A/S, Dansk Blindesamfund, Dansk EDI Råd, Dansk Dataforening, Dansk Ejendomsmæglerforening, Dansk Handel & Service, Dansk Industri, Dansk O.T.C., Dansk Standard, Danske Dagblades Forening, Danske Elværkers Forening, De Samvirkende Invalideorganisationer, Debitel Danmark A/S, Den Sociale Ankestyrelse, Den Sociale Sikringsstyrelse, Det Centrale Handicapråd, Det Danske Handelskammer, Det Kommunale Kartel, Det Kongelige Bibliotek, Direktoratet for Arbejdsløshedsforsikringen, Direktoratet for Arbejdstilsynet, Direktoratet for Kriminalforsorgen, Den Danske Dommerforening, Dommerfuldmægtigforeningen v. Retsassessor Carin Heiner Holm, DSB, Eksport Kredit Fonden, Eksportfremmerådet, Elektronikindustrien, Energistyrelsen, Erhvervs- og Selskabsstyrelsen, Erhvervsfremme Styrelsen, Erhvervsministeriet, EU-direktoratet, FDA v/landsformand Viggo Bækgaard, Finansministeriet, Finansrådet, Finanstilsynet, Folketingets Ombudsmand, Fondsrådet, Forbrugerombudsmanden, Forbrugerrådet, Forbrugerstyrelsen, Foreningen af Interne Revisorer, Foreningen af Internetleverandører, Foreningen af Management Konsulenter, Foreningen af Registrerede Revisorer, Foreningen af Statsautoriserede Revisorer, Foreningen for Dansk Internet Handel, Forsvarsministeriet, Frederiksberg Kommune, Færøernes Landstyre, Global One, GN Store Nord, Grossistforeningen for Radio og Elektronik, Grønlands Hjemmestyre, Handelshøjskolen i København, Håndværksrådet, Indenrigsministeriet, InvesteringsForeningsRådet, IT-Brancheforeningen, ITEK, Justitsministeriet, KODA, Kommunedata, Kommunernes Landsforening, Kongeriet Danmarks Hypotekbank, Konkurrencerådet, Kort & Matrikelstyrelsen, Kulturministeriet, Københavns Fondsbørs A/S, Københavns Kommune, Landsorganisationen i Danmark LO, Leverandørforeningen for Radiokommunikation, Miljø- og Energiministeriet, Mobilix, Multi Medie Foreningen, Næstved Kommune, Patentdirektoratet, Pengeinstitutternes Betalings Service PBS A/S, Plantedirektoratet, Post Danmark, Realkreditrådet, Registertilsynet, Rigspolitichefen, Rigsrevisionen, Ringsted Kommune, Rådet for Dansk Forsikring og Pension, Skatteministeriet, Socialministeriet, Sonofon I/S, Statens Arkiver, Statens Bibliotekstjeneste, Statens Bilinspektion, Statens Information, Statens Luftfartsvæsen, Statsadvokaten for Særlig Økonomisk Kriminalitet, Statsministeriet, Sundhedsministeriet, Sundhedsstyrelsen, SU-styrelsen, Søfartsstyrelsen, Tele Danmark A/S, Tele2 A/S, Telekommunikationsforbundet, Telestyrelsen, Telia A/S, Told- og Skattestyrelsen, Trafikministeriet, Udenrigsministeriet, Ud-

lændingestyrelsen, Undervisningsministeriet, Vordingborg Kommune, Værdipapircentralen, Ældre Sagen, Økonomiministeriet, Økonomistyrelsen, Århus Amt, Advokat Hanne Bender, Professor dr.jur. Jens Peter Christensen og professor dr. jur. Karsten Revsbech, Århus Universitet, Centerleder Knud Erik Skouby, Danmarks Tekniske Universitet, samt Professor Mads Bryde Andersen, professor dr. jur. Mogens Koktvedgaard og professor dr. jur. Peter Blume, Københavns Universitet.

H. Skema over konsekvenser af lovforslaget

	Positive konsekvenser/mindreudgifter	Negative konsekvenser/merudgifter
Økonomiske konsekvenser for stat, kommuner og amtskommuner	Mindre ressourceforbrug til varetagelse af forskellige serviceydelser, der kan tilbydes ved anvendelse af elektronisk kommunikation og elektroniske signaturer.	Der er behov for 2-3 yderligere årsværk i Telestyrelsen til varetagelse af opgaven med at føre tilsyn med nøglecentre. Behov for investeringer i ny teknologi, uddannelse af personale, m.v. i forbindelse med, at der tilbydes nye elektroniske serviceydelser
Administrative konsekvenser for stat, kommuner og amtskommuner	Offentlige myndigheder får bedre mulighed for at anvende elektroniske signaturer, som opfylder et tilstrækkeligt højt sikkerhedsniveau til at sikre borgernes behov for blandt andet anvendelighed og beskyttelse af persondata i forbindelse med elektroniske serviceydelser.	Ingen.
Administrative og økonomiske konsekvenser for erhvervslivet	Nøglecentre, der udbyder kvalificerede certifikater skal afholde udgifter til en systemrevisor og til at indsende diverse oplysninger til Telestyrelsen. Herudover er det intentionen på sigt at indføre regler om, at statens udgifter til Telestyrelsens tilsyn skal afholdes af nøglecentrene.	Indførsel af regler om tilsyn og ansvarsforhold for visse nøglecentre forventes af forøge tilliden til anvendelse af elektroniske signaturer og derved forbedre nøglecentrenes forretningsgrundlag. Forbedret mulighed for at benytte og udvikle den elektroniske handel, hvilket kan medføre væsentlige besparelser for erhvervslivet samt forbedre erhvervslivets konkurrenceevne over for udenlandske virksomheder.

	Positive konsekvenser/mindre-udgifter	Negative konsekvenser/mer-udgifter
Miljømæssige konsekvenser	I takt med at anvendelsen af elektroniske serviceydelser slår igennem, vil det indebære klare miljøgevinster, i form af mindre ressourceforbrug til transport af meddelelser, besparelser i papirforbrug, m.v.	Lovforslaget har ingen nævneværdige negative konsekvenser for miljøet.
Administrative konsekvenser for borgerne	De forbedrede muligheder for at kommunikere elektronisk med offentlige myndigheder vil kunne medføre betydelig administrativ lettelse for borgerne.	Ingen negative administrative konsekvenser for borgerne.
Forholdet til EU-retten	Lovforslaget indeholder regler, der gennemfører Europa-Parlamentets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer.	

Bemærkninger til lovforslagets bestemmelser

Til kapitel 1

Formål og anvendelsesområde

Til § 1

Lovforslaget har til formål at sikre, at der på markedet er produkter og nøglecentre, der lever op til en række krav, der gør dem sikre at bruge.

I lovforslaget fastsættes således en række krav til de certifikater, der udbydes under betegnelsen »kvalificerede certifikater«. Udbyderne af disse kvalificerede certifikater vil være underlagt en række minimumskrav, et offentligt tilsyn og en særlig ansvarsregulering. Der er ikke tale om en egentlig forudgående autorisationsordning, men om en ordning baseret på indsendelse af dokumentation (herunder navnlig systemrevisor-rapporter) for overholdelse af disse minimumskrav, kombineret med mulighed for at frakende et nøglecenter retten til at anvende den offentligt regulerede produktbetegnelse »kvalificerede certifikater« om sit produkt, hvis dokumentationen er utilstrækkelig eller kravene ikke overholdes. Lovforslaget skal på den måde medvirke til at fremme en sikker og effektiv anvendelse af digital kommunikation.

Det er ikke hensigten med lovforslaget at regulere ethvert udbud af certifikater til elektroniske signaturer. Det er således frivilligt, om et nøglecenter ønsker anvende betegnelsen »kvalificeret certifikat« om sit produkt med den konsekvens, at nøglecentret bliver omfattet af lovens tilsynsordning og den tilhørende ansvarsbestemmelse.

Udover ovennævnte indeholder lovforslaget en nærmere regulering af minimumskravene til sikre signaturgenereringsystemer, jf. også bemærkningerne til lovforslagets §§ 14-15.

Til § 2

Bestemmelsen fastlægger forslagets anvendelsesområde.

Lovforslaget finder først og fremmest anvendelse på nøglecentre etableret i Danmark og på de kvalificerede certifikater, som disse nøglecentre udsteder til offentligheden.

Lovforslaget indeholder tillige regler for signaturgenererings- og signaturverificeringsdata, som nøglecentrene udbyder i kombination med et kvalificeret certifikat.

Endelig fastsætter forslaget en række krav til sikre signaturgenereringssystemer, som markedsføres og anvendes her i landet, herunder at disse som udgangspunkt, skal efterprøves af et organ eller en myndighed udpeget af forskningsministeren.

Til stk. 1

Lovforslagets territoriale anvendelsesområde omfatter, for så vidt angår den nærmere regulering af nøglecentre, alene nøglecentre etableret i Danmark.

For at et nøglecenter anses for at være etableret i Danmark skal nøglecentret udøve en økonomisk akti-

vitet fra et fast forretningssted i landet i et ikke nærmere angivet tidsrum eller for en bestemt periode.

Et eksempel på et nøglecenter, som utvivlsomt vil være omfattet af denne lovs bestemmelser, er et selskab, der er stiftet og registreret som et dansk selskab i overensstemmelse med den danske selskabslovgivning, og som har sit forretningsmæssige hjemsted i Danmark. En sådan etablering og registrering må tages som udtryk for, at selskabet har dets ledelse og dets primære økonomiske aktivitet her i landet. Vælger dette nøglecenter også at udbyde sine tjenesteydelser i et andet land, vil det fortsat skulle opfylde denne lovs bestemmelser samt være underlagt dansk tilsyn.

Modsat vil et nøglecenter, der udbyder tjenesteydelser via en hjemmeside på Internettet, der er etableret via en dansk internet-udbyder, men som ikke derudover har aktiviteter i Danmark, ikke anses for at være etableret her i landet (dvs. i det land, hvor den benyttede internetudbyder befinder sig). Det er ikke afgørende, i hvilke lande et nøglecenters hjemmeside er tilgængelig.

Hvis et nøglecenter har flere etableringssteder, er det afgørende, fra hvilket etableringssted de pågældende tjenesteydelser leveres. Såfremt en bedømmelse heraf er vanskelig, skal der lægges vægt på, hvor centret for nøglecentrets aktiviteter vedrørende den pågældende tjenesteydelse befinder sig, og i sidste ende også hvor selskabets overordnede forretningsmæssige hjemsted er.

Hvorvidt et nøglecenter skal anses for at være etableret i Danmark eller i et andet land inden for Det Europæiske Økonomiske Samarbejde (EØS), har betydning for, hvilket lands myndigheder eller lignende, der skal føre kontrol med, at nøglecentret opfylder kravene til at udstede kvalificerede certifikater. Direktivets artikel 4, stk. 1, indfører på denne måde en form for arbejdsdeling mellem medlemsstaterne.

Den nærmere afgrænsning af, hvornår et nøglecenter skal anses for at være etableret i Danmark eller i et andet land, må afgøres i praksis, blandt andet ud fra en fortolkning af EF-traktatens regler om retten til fri etablering, samt af andre relevante EF-direktiver.

I overensstemmelse med kravet i direktivets artikel 4, stk. 1 og EF-traktatens principper om fri udveksling af tjenesteydelser, pålægger forslaget ikke nøglecentre etableret i et andet land inden for Det Europæiske Økonomiske Samarbejde (EØS) begrænsninger med hensyn til at markedsføre og udstede certifikater på det danske marked. Nøglecentre etableret i EØS-landene kan, i det omfang de overholder kravene i direktivet, ligeledes markedsføre og udstede certifikater med betegnelsen kvalificerede certifikater i Danmark.

Kvalificerede certifikater, der udstedes af et nøglecenter etableret i disse lande, kan på samme måde som et kvalificeret certifikat udstedt af et nøglecenter etableret i Danmark , anvendes til at opfylde formkrav i lovgivningen, jf. forslagets § 13. Dette gælder ligeledes for certifikater udstedt af nøglecentre i tredjelande, såfremt betingelserne i § 23 er opfyldt.

Hvorvidt et nøglecenter, som ikke er etableret i Danmark, overholder kravene i direktivet til nøglecentre, der udsteder kvalificerede certifikater, skal kontrolleres af den myndighed eller det private organ i etableringslandet, som er udpeget hertil i henhold til dette lands regler. Direktivets artikel 3, stk. 3, stiller krav om, at medlemsstaterne indfører et »passende system til kontrol af« de nøglecentre, der er etableret i medlemsstaten, og som udbyder kvalificerede certifikater. Der opstilles dog ikke nærmere krav til, hvad denne kontrol skal gå ud på, og det vil derfor kunne variere noget fra medlemsstat til medlemsstat, hvor omfattende og detaljeret kontrollen er.

Lovforslaget finder først og fremmest anvendelse på udbud af kvalificerede certifikater til offentligheden og regulerer således ikke anvendelse af elektroniske signaturer og certifikater inden for lukkede systemer, der er baseret på frivillige aftaler mellem et begrænset antal deltagere. Direktivet indeholder ikke nogen yderligere angivelse af, hvad der skal forstås ved et udbud af certifikater »til offentligheden«, hvorfor det må afgøres i praksis, hvorledes udtrykket skal fortolkes.

Det er dog formentlig afgørende for bedømmelsen af konkrete tilfælde, om et certifikat kan anvendes over for tredjemænd, med hvilke underskriveren ikke har indgået nogen forudgående aftale vedrørende anvendelse eller accept af det pågældende certifikat.

Et eksempel på et lukket system, som ikke reguleres af forslaget, vil være et Internet banksystem, hvor det alene er banken, der skal anvende og acceptere underskriverens certifikat. På samme måde må det formodes, at certifikater, som alene kan anvendes inden for en eller flere organisationer eller virksomheder ikke vil være omfattet.

Lovforslagets regler vedrørende nøglecentre finder med undtagelse af bestemmelsen i § 12 udelukkende anvendelse på de nøglecentre etableret i Danmark, som udsteder kvalificerede certifikater. § 12 gælder derimod samtlige nøglecentre etableret i Danmark uanset, om de udsteder kvalificerede certifikater eller om de udsteder certifikater til offentligheden. Af hensyn til den sproglige udformning af forslagets bestemmelser anvendes udtrykket »nøglecenter« overalt i forslaget. Se endvidere bemærkningerne til § 12.

Til stk. 2

Lovforslaget finder desuden anvendelse på efterprøvelse af, at signaturgenereringssystemer overholder de opstillede krav til sikre signaturgenereringssystemer. Se i øvrigt bemærkningerne til § 15 vedrørende det geografiske anvendelsesområde for disse bestemmelser.

Til kapitel 2

Definitioner

Kapitel 2 indeholder definitionerne på de begreber, der anvendes i lovforslaget. Begreberne stammer bl.a. fra direktivets definitioner i artikel 2 og danner grundlag for, at der kan etableres et indre marked for certificeringstjenester, der opfylder disse krav.

Til § 3

Til stk. 1, nr. 1

Den pågældende bestemmelse definerer, hvad der forstås ved en elektronisk signatur. Den mest udbredte elektroniske signatur teknologi i dag er den såkaldte digitale signatur, der er baseret på et system med en privat og en offentlig signaturnøgle.

Lovforslaget omfatter imidlertid også andre elektroniske systemer, som er beregnet til identifikation af brugeren, f.eks. koder og biometriske værdier. Lovforslaget er således baseret på et princip om teknologineutralitet og omfatter derfor alle former for elektroniske metoder til at fastslå autenticiteten af en meddelelse. Ved en autentifikationsmetode forstås en metode til at kontrollere, om en meddelelse stammer fra den, som er angivet som underskriver af heraf, samt at indholdet af meddelelsen ikke er blevet ændret efter det tidspunkt, hvor den elektroniske signatur blev knyttet til den.

Den digitale signatur fungerer sådan, at underskriveren har en privat signaturgenereringsnøgle, som bruges til at skabe eller generere den digitale signatur med. Til denne private nøgle hører en offentlig signaturverificeringsnøgle. Den offentlige nøgle anvendes til at kontrollere den digitale signatur.

Den private og den offentlige nøgle passer sammen som to halvdele af en lås eller en kode, sådan at en meddelelse signeret med den ene kun kan verificeres med den anden.

Til nr. 2

Nr. 2 indeholder en definition af, hvad der forstås ved en avanceret elektronisk signatur. For at en elektronisk signatur skal kunne anses for at være en avanceret elektronisk signatur, skal signaturen kunne identificere underskriveren og være entydigt knyttet til denne, jf. litra a og b.

Af hensyn til sikkerheden omkring den elektroniske signatur kræves det i litra c, at en avanceret elektronisk signatur er baseret på et signaturgenereringssystem, som underskriveren kan bevare den fulde kontrol med.

Efter litra d kræves det, at en avanceret elektronisk signatur er i stand til at afsløre enhver ændring i de underskrevne data efter signaturen er blevet påført. Det skal således være muligt for brugeren at opdage, hvis der er foretaget ændringer i de underskrevne data, efter signaturen er blevet vedhæftet eller logisk tilknyttet til disse.

Den pågældende definition anvendes i lovforslagets §13, der indeholder første led i en nærmere regulering af retsvirkningerne af anvendelse af elektroniske signaturer.

Til nr. 3

I nr. 3 defineres, hvad der forstås ved en underskriver. Underskriveren er den person, der har kontrollen med et signaturgenereringssystem, og som besidder signaturgenereringsdataene (den private nøgle). Det er således den, der fremgår af certifikatet, og som har udvirket signaturen på de data, der er underskrevet.

Til nr. 4

Nr. 4 definerer, hvad der forstås ved signaturgenereringsdata. Signaturgenereringsdata er de data, der anvendes til at frembringe den elektroniske signatur. I digital signatur teknologien kaldes signaturgenereringsdata for den private nøgle.

Til nr. 5

Nr. 5 fastlægges, hvad der forstås ved et signaturgenereringssystem. Et signaturgenereringssystem er det system, der anvendes til at frembringe den elektroniske signatur og er typisk opbygget af en krypteringsalgoritme og en dekrypteringsalgoritme med tilhørende krypteringsnøgler. En krypteringsalgoritme er en formaliseret måde at frembringe en elektronisk signatur på. Krypteringsnøglerne er parametre, der anvendes til krypteringsalgoritmerne af praktiske grunde. Nøglerne afgør, hvorledes algoritmerne skal frembringe den elektroniske signatur.

Signaturgenereringssystemet anvender signaturgenereringsdataene. Systemet kan både være softwarebaseret eller hardwarebaseret. En mulig hardwareløsning er, den hvor signaturgenereringsdataene er lagret på et såkaldt chipkort (et plastikkort).

Et softwarebaseret signaturgenereringssystem vil typisk være indeholdt i systemet til afsendelse af elektronisk post.

§§ 14 og 15 indeholder yderligere regler vedrørende såkaldt »sikre signaturgenereringssystemer«.

Til nr. 6

Ifølge nr. 6 er signaturverificeringsdata de data, der anvendes til at verificere den elektroniske signatur, dvs. den offentlige del af nøgleparret.

Til nr. 7

Bestemmelsen i nr. 7 fastsætter, hvad der forstås ved et signaturverificeringssystem. Det er et system, der anvendes til at verificere den elektroniske signatur.

Til nr. 8

I nr. 8 defineres et certifikat. Et certifikat til en elektronisk signatur indeholder oplysninger om, hvem der er underskriver. Underskriveren er den person, der besidder et signaturgenereringssystem, og som indgår en aftale med et nøglecenter om udstedelse af et certifikat til underskriverens signatur. Certifikatet er den elektroniske attest, der angiver sammenhængen mellem underskriverens identitet og underskriverens signaturverificeringsdata (også i digital signatur teknologien kaldet den offentlige nøgle).

Til nr. 9

I nr. 9 defineres, hvad der efter lovforslaget anses for at være et nøglecenter. Kernefunktionen for et nøglecenter er at kontrollere identiteten af underskriveren og angive sammenhængen mellem underskriveren og dennes signaturverificeringsdata i et certifikat, som udstedes af nøglecentret. Nøglecentre, der udsteder kvalificerede certifikater til offentligheden skal desuden sørge for en sikker katalog- og tilbagekaldelsestjeneste, jf. § 9.

Nøglecentret kan frit udøve andre former for virksomhed, herunder en række relaterede tjenesteydelser, såsom valideringstjenester, tidsstempling, at indestå for certifikater udstedt af andre nøglecentre, jf. § 11 og § 23, m.v.

Bestemmelserne i kapitel 2 er en delvis implementering af direktivets artikel 2, der indeholder 13 definitioner på begreber, der er anvendt i direktivet. Bestemmelserne i kapitel 2 implementerer direktivets artikel 2, nr. 1-5, 7-9 og 11. Artikel 2, nr. 6 er implementeret i § 14, artikel 2, nr. 10 er implementeret i kapitel 3, og endelig er direktivets artikel 2, nr. 12 implementeret ved § 5, stk. 1, nr. 3. Det er ikke fundet nødvendigt at implementere definitionen af frivillig akkreditering i direktivets artikel 2, nr. 13, jf. også bemærkningerne til § 10, stk. 1, nr. 4.

Til kapitel 3

Kvalificerede certifikater

Kapitel 3 indeholder kravene til udbud af »kvalificerede certifikater«.

Til § 4

Til stk. 1

Et kvalificeret certifikat defineres i stk. 1 som et certifikat, der indeholder de oplysninger, der er krævet i stk. 2 og 3, og som er udstedt af et nøglecenter, der opfylder kravene i kapitel 4, samt regler fastsat i medfør heraf.

Bestemmelserne i stk. 2 og 3 er en implementering af de krav, der stilles i direktivet til udbudet af »kvalificerede certifikater«.

Indeholder certifikatet en angivelse af, at det er et kvalificeret certifikat, og har det udstedende nøglecenter hjemsted i Danmark, skal kravene i denne lov vedrørende udbud af kvalificerede certifikater overholdes.

Nøglecentre, der ikke overholder lovens bestemmelser til udbud af kvalificerede certifikater, må om deres certifikater ikke anvende betegnelsen »kvalificerede certifikater«, eller betegnelser der egner sig til at give det indtryk, at der er tale om kvalificerede certifikater.

Til stk. 2

Stk. 2 indeholder kravene til, hvilke oplysninger et kvalificeret certifikat skal indeholde.

Ifølge *nr. 1* skal det i et kvalificeret certifikat angives, at certifikatet udstedes som et kvalificeret certifikat.

Nr. 2 kræver, at nøglecenteret angiver, hvor det har hjemsted. Oplysningen herom gør det klart for den, der fæstner lid til certifikatet, hvilket land der fører tilsyn med nøglecentrets virksomhed.

Nr. 2 indeholder ligeledes et krav om, at certifikatet skal indeholde en identifikation af nøglecentret. Dette indebærer, at navnet på det pågældende nøglecenter skal fremgå af certifikatet. Det mest hensigtsmæssige vil i de fleste tilfælde være at bruge den identifikation, som udbyderen almindeligvis anvender over for offentligheden, da det umiddelbart vil give modtagerne af certifikatet et indtryk af, hvem der er udsteder. Andre entydige identifikationskendetegn end nøglecentrets navn kan også indgå, herunder eksempelvis nøglecentrets eventuelle SE-nummer, CVR-nummer eller

aktieselskabsnummer, eller det formelt registrerede selskabsnavn, såfremt dette afviger fra det navn eller varemærke, som selskabet almindeligvis anvender overfor offentligheden.

Ifølge *nr. 3* skal et kvalificeret certifikat indeholde navnet på underskriveren. Navnet på underskriveren kan også være angivet med et pseudonym, men i så fald skal det være angivet, at der er tale om et pseudonym.

Det er afgørende for, at der kan fæstnes lid til den elektroniske signatur, at det umiddelbart fremgår hvem, der er underskriver. Ifølge § 6 er nøglecentret forpligtet til at kontrollere identiteten af den person, til hvem der udstedes et kvalificeret certifikat.

Nr. 4 fastsætter, at certifikatet skal indeholde yderligere oplysninger om underskriveren, i det omfang det er nødvendigt for anvendelsen af certifikatet. Hvad, der anses for relevante yderligere oplysninger, afhænger af det konkrete formål med certifikatet, men kan blandt være oplysninger, der sikrer, at underskriverens identitet kan fastslås entydigt. Er der f.eks. tale om et certifikat, der alene skal bruges til kommunikation med et forsikringsselskab, kan det være hensigtsmæssigt at lade certifikatet indeholde underskriverens policenummer. Forslaget tager ikke stilling til, hvorvidt der i et kvalificeret certifikat kan angives underskriverens personnummer eller lignende form for identifikation. Dette må afgøres efter den almindelige lovgivning om behandling af personoplysninger.

Ifølge *nr. 5* er det krævet, at et kvalificeret certifikat indeholder en ikrafttrædelses- og en udløbsdato, dvs. en angivelse af certifikatets gyldighedsperiode.

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. Om et antal år vil det, der i dag er en sikker elektronisk signatur muligvis ikke længere være sikker mod forfalskning etc.

Ved anvendelse af elektroniske signatur skal brugerne nøje overveje, hvordan deres digitale dokumenter opbevares. Dokumenter, der kan få betydning ud over udløbsperioden af de involverede signaturer, skal opbevares med omtanke. Problematikken omkring forældelse af certifikater betyder, at det konkret bør overvejes, om en given type af meddelelser egner sig til at blive kommunikeret elektronisk.

Bestemmelsen i *nr. 6* kræver, at eventuelle begrænsninger af anvendelsesområdet (formålsbegrænsninger) for certifikatet tydeligt skal fremgå af certifikatet.

Bestemmelsen i *nr. 7* kræver, at eventuelle begrænsninger med hensyn til de transaktionsbeløb, som certifikatet kan anvendes til (beløbsbegrænsninger), tydeligt skal fremgå af certifikatet.

Bestemmelsen i *nr. 8* kræver, at et kvalificeret certifikat skal indeholde en unik identifikationskode, et såkaldt referencenummer. Det skal således være muligt entydigt at identificere certifikatet.

I *nr. 9* kræves det, at det kvalificerede certifikat indeholder de signaturverificeringsdata, der korresponderer med underskriverens signaturgenereringsdata.

Indeholder certifikatet ikke de nævnte oplysninger, vil det ikke umiddelbart være muligt at kontrollere den elektroniske signatur. Signaturen kan først kontrolleres, når signaturverificeringsdataene er hentet hos nøglecentret. Dette kunne afholde nogen fra at kontrollere signaturen med deraf følgende usikkerhed. Der stilles derfor krav, om at et kvalificeret certifikat indeholder signaturverificeringsdataene, sådan at det umiddelbart er muligt at kontrollere signaturen.

Til stk. 3

Ifølge stk. 3 skal et kvalificeret certifikat være underskrevet med det udstedende nøglecenters avancerede elektroniske signatur. Signaturen vedhæftes eller knyttes logisk til certifikatet efter, at alle oplysningerne er indsat i det. Det sikres herved, at der ikke kan ændres i certifikatet, efter det er udstedt, uden at det afsløres, og modtageren vil dermed være advaret.

Nøglecentrets signatur og identifikationen af nøglecentret i certifikatet, jf. stk. 2, nr. 2, vil tjene som identifikation af, hvem et eventuelt erstatningskrav efter § 11 kan rettes imod.

Til kapitel 4

Krav til nøglecentres virksomhed

Til § 5

Til stk. 1

Bestemmelsen pålægger de nøglecentre, der udbyder kvalificerede certifikater løbende at træffe de foranstaltninger, som er nødvendige for, at der er tale om et sikkert, pålideligt og velfungerende udbud af kvalificerede certifikater. Hvad, der anses for nødvendige foranstaltninger, må vurderes under hensyn til hvilke tjenesteydelser, der udbydes og til hvilke kundegrupper. Nøglecentret er forpligtet til løbende at vurdere sine foranstaltninger, såfremt porteføljen af udbudte tjenesteydelser udvides eller på anden måde ændres.

Nr. 1 pålægger nøglecentret at følge de standarder inden for administrative og ledelsesmæssige procedu-

rer, der er anerkendte inden for den teknologi, som udbyderen tilbyder tjenesteydelser inden for.

Nr. 2 fastsætter, at nøglecentre, der udsteder kvalificerede certifikater, skal beskæftige personale, som i forhold til de tjenesteydelser, der udbydes, har den rette ekspertise, erfaringsgrundlag og kvalifikationer. Det kan være forskelligt fra tjenesteudbyder til tjenesteudbyder afhængigt af hvilke ydelser, der udbydes.

Personalet skal have sagkundskab inden for teknologien for elektroniske signaturer og indgående kendskab til korrekte sikkerhedsprocedurer. Det skal således så vidt muligt undgås, at det er personalemæssige årsager, der er skyld i sikkerhedsbrud.

Nr. 3 forpligter nøglecentre, der udsteder kvalificerede certifikater, til at anvende sikre IT-produkter og systemer i virksomheden. Nøglecentre skal bl.a. benytte systemer og produkter, som er beskyttet mod uautoriserede ændringer.

Det er afgørende for sikkerheden i den infrastruktur, der bygges op omkring de elektroniske signaturer, at nøglecentret, som netop skal stå som den troværdige tredjepart, anvender pålidelige systemer og produkter, og at de systemer og produkter, der anvendes, er indrettet på en sådan måde, at sikkerheden omkring nøglecentrets virke er optimal.

Nr. 4 pålægger nøglecentre at træffe foranstaltninger og etablere procedurer, der imødegår eventuelle muligheder for forfalskninger af certifikaterne. Bestemmelsen skal sikre, at certifikatet ikke efter udstedelse forfalskes. Et certifikats integritet kan blandt andet sikres ved, at nøglecentret påfører certifikatet sin egen elektroniske signatur. Se hertil § 4, stk. 3.

Efter *nr. 5*, kræves det, at nøglecentre, der udsteder kvalificerede certifikater, til stadighed har tilstrækkelige økonomiske ressourcer til at kunne honorere kravene i denne lov herunder særligt evnen til at kunne bære et eventuelt erstatningsansvar.

Hvorvidt, et nøglecenter har tilstrækkelige økonomiske ressourcer, vil bl.a. afhænge af hvilke tjenesteydelser, nøglecentret udbyder. Det vil betyde, at såfremt nøglecentret udbyder certificeringstjenesteydelser til anvendelse inden for et område med store økonomiske konsekvenser for de involverede parter, skal det økonomiske beredskab være tilsvarende højt. Nøglecentret skal således opretholde et balanceret forhold mellem dets økonomiske ressourcer og omfanget og karakteren af de aktiviteter, som udøves. Kravet kan bl.a. opfyldes ved, at nøglecentret tegner en passende forsikring. Der er i stk. 3 givet hjemmel til, at Forskningsministeren fastsætte nærmere krav til nøglecentrenes økonomiske ressourcer, herunder krav om at nøglecentret tegner en forsikring, hvor dette skønnes nødvendigt samt regler om de nærmere krav til en sådan forsikring.

Nr. 3- 5 implementerer direktivets bilag II, litra f-h.

§ 5 stk. 1, nr. 1 og 2 fastlægger krav, der implementerer direktivets bilag II, litra a og e.

Til stk. 2

I *stk. 2* stilles der krav om, at et nøglecenter, der udsteder kvalificerede certifikater, skal vælge en ekstern statsautoriseret revisor til varetagelse af systemrevisionen i nøglecentret. Bestemmelsen er en minimumsbestemmelse i den forstand, at hvis der i selskabslovgivningen, årsregnskabsloven, eller anden lovgivning stilles krav om, at nøglecentret skal have en eller flere finansielle revisorer, finder disse regler fortsat anvendelse på nøglecentret. Lovforslagets bestemmelser omhandler alene den anvendelse af eksterne revisorer, der er påkrævet med sigte på at opfylde denne lovs regler.

Kravet om, at et nøglecenter skal have en systemrevisor, er begrundet i de særlige krav, som stilles til nøglecentre, der udbyder kvalificerede certifikater i nærværende lovforslag. Disse krav vedrører hovedsagelig nøglecentrets IT-systemer og sikkerheden i forbindelse hermed.

Ved systemrevision forstås i dette lovforslag revision af 1) generelle edb-kontroller i virksomheden, 2) edb-baserede brugersystemer til udstedelse, verificering, opbevaring og spærring af certifikater, og 3) edb-systemer til udveksling af data med andre. Den valgte systemrevisor skal i forbindelse med sin gennemgang vurdere, hvorvidt nøglecentret overholder bestemmelserne i loven og regler fastsat i medfør heraf.

Revision af de generelle edb-kontroller omfatter blandt andet, at den valgte systemrevisor skal efterprøve de generelle sikringsforanstaltninger til etablering af et tidssvarende IT-sikkerhedsniveau i nøglecentret. Revision af edb-baserede brugersystemer omfatter såvel edb-baserede som manuelle forretningsgange,

Udgifterne ved den valgte systemrevisor afholdes af det enkelte nøglecenter.

Se også bemærkningerne til § 17, herunder til § 17, stk. 4, der indeholder hjemmel til at fastsætte nærmere regler om kravene til systemrevisionens gennemførelse og til systemrevisors kvalifikationer.

Til stk. 3

Stk. 3 bemyndiger Forskningsministeren til at fastsætte nærmere regler om indholdet af de i stk. 1 nævnte krav til nøglecentre, der udsteder kvalificerede certifikater til offentligheden.

Direktivet åbner i artikel 9 mulighed for, at Kommissionen kan præcisere de krav, der er fastlagt i bilagene til direktivet til udbydelse af kvalificerede certifikater. Hjemlen i stk. 3 vil blandt andet kunne anvendes til implementering heraf, men vil også kunne anvendes til at fastsætte særskilte danske regler herom. Det er herunder blandt andet hensigten at fastsætte nærmere regler om minimumskravene til nøglecentrenes økonomiske ressourcer og/eller forsikringsforhold, jf. også bemærkningerne ovenfor til stk. 1.

Til § 6

Ifølge § 6 pålægges det nøglecentret at fastsætte og anvende betryggende procedurer for nøglecentrets kontrol af identitet og andre forhold vedrørende underskriveren forud for udstedelsen af et kvalificeret certifikat.

Bestemmelsen forhindrer ikke, at nøglecentret kan udpege en anden organisation, en såkaldt registreringsmyndighed, til at forestå den krævede identitetskontrol.

Det vil dog fortsat være nøglecentret, som i henhold forslagets § 11 er ansvarlig for, at oplysningerne i certifikatet er korrekte. For underskriveren af et kvalificeret certifikat eller for en tredjemand, som med rimelighed forlader sig på et kvalificeret certifikat, er det således uden betydning, hvorvidt en fejl i forbindelse med en identitetskontrol kan tilskrives nøglecentret selv eller en af nøglecentret udpeget registreringsmyndighed. I det tilfælde at nøglecentret har måttet udbetale en erstatning i henhold til § 11 på grund af en fejl begået af registreringsmyndigheden, kan nøglecentret efterfølgende søge regres over for registreringsmyndigheden efter dansk rets almindelig regler om erstatning.

Der vil i medfør af bemyndigelsen i stk. 3 blive fastsat nærmere minimumskrav til, hvilke typer kontrolprocedurer, der anses for at opfylde kravene om gennemførelse af en betryggende identitetskontrol.

Den umiddelbart sikreste måde at foretage kontrol af identiteten af den person, til hvem der udstedes et certifikat, er ved at kræve, at denne møder personligt op og samtidig fremviser relevant billedlegitimation. Samtidig er der allerede i dag en udbredt praksis for, og regulering af, at eksempelvis bankkonti, kredit- og betalingskort m.v. kan udstedes uden personligt fremmøde, forudsat at der fremsendes betryggende skriftlig dokumentation, og forudsat at der anvendes visse nærmere angivne kontrolprocedurer. I en række situationer forekommer det ubegrundet at stille strengere krav til oprettelse af et elektronisk signatur certifikat, end f.eks. et betalingskort. Hvilke procedurer, der må anses for betryggende, kan imidlertid også afhænge af, til hvilke formål, de kvalificerede certifikater kan anvendes.

Den nærmere regulering af minimumskravene til identitetskontrol vil blive fastlagt med udgangspunkt i ovennævnte, og efter høring af alle relevante parter. Der kan eventuelt heri indgå en differentieret regulering af forskellige kategorier af certifikater.

Det vil herunder også indgå i overvejelserne, at det i sidste ende er nøglecentret, der ansvarsmæssigt hæfter for, at certifikatets oplysninger er korrekte, jf. lovforslagets § 11, og der vil derfor være et betydeligt forretningsmæssigt incitament for nøglecentrene til på eget initiativ at etablere betryggende procedurer for kontrol med identiteten af de parter, som man udsteder certifikater til, idet det som udgangspunkt vil være nøglecentret, der ifalder erstatningsansvar, hvis certifikatets oplysninger ikke er korrekte, og modtageren af et certifikat af denne grund lider tab, f.eks. fordi man ikke i praksis kontraherer med den part, man på grundlag af certifikatets oplysninger mener at kontrahere med. Der kan således udmærket tænkes situationer, hvor nøglecentret vælger at anvende mere omfattende kontrolprocedurer, end bekendtgørelsesreguleringen kræver, med sigte på at minimere sin egen risiko.

Det vil ligeledes indgå, at et krav om, at der i alle tilfælde, hvor der udstedes et kvalificeret certifikat, skal ske personligt fremmøde, formentlig vil virke urimeligt hæmmende for udbredelsen af elektroniske signaturer og tilhørende kvalificerede certifikater.

Reglerne vil derudover under alle omstændigheder blive udformet sådan, at der er mulighed for i praksis at delegere selve identitetskontrollen til tredjemand eller at lade tredjemand indestå for underskrivernes identitet, dog fortsat under nøglecentrets ansvar, jf. ovenfor. Der kan således bl.a. tænkes situationer, hvor identiteten af den, til hvem der skal udstedes et kvalificeret certifikat, mere hensigtsmæssigt kan kontrolleres af tredjemand, f.eks. i situationer, hvor en virksomhed eller en offentlig myndighed ønsker, at der udstedes certifikater til alle medarbejdere. Oftest har organisationen allerede tilstrækkelig information om medarbejderne, til at der kan udstedes et certifikat til den enkelte medarbejder, uden at denne behøves at møde personligt frem til registrering hos nøglecentret.

I stk. 2 kræves det herudover, at nøglecentret overfor enhver oplyser om, hvordan identiteten er kontrolleret. Det er afgørende for modtageren, at vedkommende har mulighed for at vurdere, om den kontrol, nøglecentret udfører, opfylder det sikkerhedsniveau, som modtageren kræver.

Kravet, om at nøglecentret skal foretage en kontrol af underskriveren af certifikatets identitet gennemfører direktivets bilag II, litra d.

Til § 7

Til stk. 1

Stk. 1 pålægger nøglecentre, der udsteder kvalificerede certifikater, at sikre, at underskriveren af den elektroniske signatur på udstedelsestidspunktet er i besiddelse af signaturgenereringsdata, der korresponderer med de signaturverificeringsdata, der certificeres. Stk. 1 implementer i sammenhæng med § 11 direktivets artikel 6, stk. 1, litra b.

Til stk. 2

I stk. 2 fastlægges det, at udstedelsen af certifikater kan foregå ved, at underskriveren af den elektroniske signatur selv genererer de signaturgenereringsdata og signaturverificeringsdata, der skal certificeres.

Det kan også foregå ved, at nøglecentret udsteder et chipkort, hvor den elektroniske signatur ligger på. I disse tilfælde er signaturgenereringsdataene typisk genereret af nøglecentret.

I de tilfælde, hvor det er nøglecentret, der skaber signaturgenereringsdataene, skal nøglecenteret sikre disse datas fortrolighed under genereringsprocessen. Det er også nøglecentrets pligt at sikre sig, at der alene anvendes signaturgenereringsdata og signaturverificeringsdata, der hører sammen på en unik måde.

Stk. 2 skal ses i sammenhæng med § 11 og gennemfører direktivets artikel 6, stk. 1, litra c og g.

Til stk. 3

Nøglecentret skal fastlægge en procedure for udstedelse af certifikater, og det skal ved hjælp af denne procedure senere være muligt at fastslå dato og tidspunkt for udstedelsen. Det kan være afgørende ved eventuelle tvister, at det kan fastslås, om og hvornår certifikatet er udstedt. Bestemmelsen gennemfører direktivets bilag II, litra c.

Til § 8

§ 8 pålægger nøglecentre, der udsteder kvalificerede certifikater, at der som grundlag for ethvert kundeforhold med sigte på udstedelse af et kvalificeret certifikat skal foreligge en skriftlig beskrivelse af de præcise kontraktsvilkår for udstedelse og eventuelle af nøglecentret fastsatte betingelser for anvendelse af det kvalificerede certifikat.

Nøglecentret er forpligtet til at give alle de oplysninger, der kan sætte kunden i stand til at vurdere betingelserne og omkostninger for anvendelsen af det kvalificerede certifikat. Dette skal give kunden mulighed for at vurdere fordele og ulemper ved det pågældende certifikat ved sammenligning med andre certifikater.

Til stk. 1

Nr. 1 pålægger nøglecentret at give oplysning om vilkårene for anvendelse af et udstedt kvalificeret certifikat.

Nøglecentret skal forud for indgåelse af en aftale om udstedelse af et kvalificeret certifikat give oplysning om, der er fastsat nogle formåls- eller beløbsbegrænsninger for certifikatet. Nøglecentret kan ligeledes stille betingelser til anvendelse af særligt sikkerhedsudstyr eller lignende hos underskriveren. Stilles sådanne betingelser, skal det oplyses.

I medfør af *nr. 2* kan nøglecentret stille krav til, hvorledes underskriveren skal opbevare og beskytte de til certifikatet tilknyttede signaturgenereringsdata.

Nøglecentret vil således kunne gøre det til en betingelse for udstedelse af et kvalificeret certifikat, at signaturgenereringsdataene er opbevaret på et chipkort. Der vil ligeledes kunne stilles krav om, at den elektroniske signatur skal være beskyttet af en PIN-kode eller lignende.

Ifølge *nr. 3* skal der fastsættes vilkår for omkostningerne ved erhvervelse og anvendelse af certifikatet samt nøglecentrets øvrige tjenester.

I *nr. 4* pålægges det nøglecentret at oplyse om eventuelle frivillige akkrediteringsordninger, som nøglecentret er tilknyttet.

Ved en akkrediteringsordning forstås enhver ordning, hvor der gives en tilladelse, der fastsætter rettigheder og forpligtelser, der er særlige for certificeringstjenester, og som efter anmodning fra det pågældende nøglecenter tildeles denne af et offentligt eller privat organ, der har til opgave at udarbejde og føre tilsyn med overholdelse af sådanne rettigheder og forpligtelser, og hvor nøglecentret ikke er berettiget til at udøve de rettigheder, tilladelsen giver, før denne har modtaget organets afgørelse.

Betydningen af, at et nøglecenter er tilknyttet en frivillig akkrediteringsordning, er ikke, at kravene i denne ordning har forrang i forhold til bestemmelserne i denne lov om udbud af kvalificerede certifikater. Nøglecentret vil fortsat skulle leve op til bestemmelserne i denne lov.

Derimod kan en frivillig akkrediteringsordning sikre udbud af tjenesteydelser på et mere avanceret niveau. Såfremt flere nøglecentre underlægger sig samme akkrediteringsordning, vil det kunne betyde, at deres certifikater vil kunne bruges i samme situationer.

Oplysninger om tilknytning til en akkrediteringsordning vil kunne have betydning for kundens valg af nøglecenter.

Efter *nr. 5* skal der fastlægges vilkår for bilæggelse af tvister, samt hvorledes der klages. Branchen vil kunne etablere et uafhængigt organ til varetagelse af klager over behandlingen hos et nøglecenter.

Til stk. 2

Stk. 2 sikrer, at oplysninger, som kræves efter stk. 1, kan afgives elektronisk, såfremt det sker efter en protokol, der er umiddelbart identificerbar for modtageren og dermed læsbar. Meddelelsen skal desuden afgives på en sådan måde, at det senere er muligt at bevise under hvilke vilkår, aftalen er indgået.

Det vil ikke være tilstrækkeligt, at nøglecentret henviser til en hjemmeside, hvor der kan opnås information om de oplysninger, der skal gives forud for aftalens indgåelse. En hjemmeside er under kontrol af nøglecentret, som derfor til enhver tid kunne ændre i vilkårene uden eller med ringe mulighed for andre at kunne bevise, hvilke betingelser, der var gældende ved udstedelsen.

§ 8 fastsætter krav, der implementerer direktivets bilag II, litra k.

Til § 9

Til stk. 1

Stk. 1 pålægger nøglecentre, der udsteder kvalificerede certifikater at sikre, at der etableres en hurtig og sikker katalog- og tilbagekaldelsestjeneste for de af nøglecentret udstedte certifikater.

Denne tjeneste skal give mulighed for, at det hurtigt og sikkert kan undersøges, om et kvalificeret certifikat er spærret, hvilken gyldighedsperiode certifikatet har, eller om certifikatet indeholder formåls- eller beløbsgrænsninger. Oplysningerne skal sætte modtageren af et certifikat i stand til at vurdere, om certifikatet er gyldigt, og om det er anvendt inden for de eventuelle begrænsninger, der måtte være fastsat for brugen af certifikatet.

Samtidig pålægges der i § 11 nøglecentret et skærpet erstatningsansvar for, at katalog- og tilbagekaldelsestjenestens oplysninger er korrekte og omfatter de i bestemmelsen krævede oplysninger.

Bestemmelsen forhindrer ikke, at nøglecentret indgår en aftale med et andet nøglecenter eller en anden virksomhed om at stille tjenesten til rådighed. Nøglecentret er dog fortsat ansvarlig efter § 11 for tab opstået i relation til tjenesten.

Til stk. 2

Det er efter stk. 2 pålagt nøglecentre at spærre et kvalificeret certifikat, straks efter at det har modtaget anmodning herom fra underskriveren. Ved spærring forstås dels, at nøglecentret registrerer underskriverens ønske om at spærre certifikatet, samt at oplysningen herom gøres offentligt tilgængelig, jf. stk. 1.

Bestemmelsen skal desuden ses i sammenhæng med erstatningsbestemmelsen i § 11, der pålægger nøglecentrene et præsumptionsansvar for manglende efterkommelse af anmodninger om spærring mv.

Til stk. 3

I følge stk. 3 kræves det, at det umiddelbart skal være muligt for brugerne at få adgang til oplysningerne.

Bestemmelsen implementerer kravene i direktivets bilag II, litra b og k. Bestemmelsen i § 11 udvider omfanget af kravene til, hvilke oplysninger nøglecentret skal stille til rådighed i forbindelse med katalog- og tilbagekaldelsestjenesten, sammenholdt med hvad der kræves i direktivet. Begrundelsen for denne udvidelse er at forøge brugervenligheden og dermed også sikkerheden ved at anvende kvalificerede certifikater.

Til stk. 4

Stk. 4 forbyder, at et kvalificeret certifikat opføres i en offentligt tilgængelig database, medmindre underskriveren har givet sit samtykke hertil.

En væsentlig fordel ved den elektroniske signatur er, at man kan kommunikere sikkert med personer, man ikke tidligere har kommunikeret med, endsige indgået en kommunikationsaftale med.

En måde at gøre dette på er ved at hente den kommende modtagers certifikat i en offentligt database. Der vil derfor være et incitament til at oprette sådanne databaser. Nøglecentret kan dog som nævnt ikke opføre et kvalificeret certifikat i en sådan database, førend underskriveren har givet sit samtykke hertil. Forbudet er en implementering af direktivets bilag II, litra l, 3. punkt.

Til stk. 5

Bestemmelsen indeholder hjemmel til, at forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1-3.

Der vil herunder kunne fastsættes nærmere regler om nøglecentrenes forpligtelse til at foranstalte spærring straks efter modtagelse af en anmodning fra underskriveren herom og de procedurer, der skal anvendes i forbindelse hermed, om nøglecentrets pligt til at sikre underskriverne enkle og effektive muligheder for umiddelbart at kunne kontakte nøglecentret, og

om nøglecentrets pligt til straks at kvittere for en sådan anmodning, således at underskriveren har sikkerhed for, at anmodningen er modtaget m.v.

Til § 10

Til stk. 1

Stk. 1 fastsætter, at nøglecentre, der udsteder kvalificerede certifikater, skal registrere alle relevante oplysninger om certifikaterne i minimum seks år. Dette er navnlig nødvendigt for at kunne fremlægge bevis for certificering, hvis det er påkrævet i retssager. Bestemmelsen implementerer direktivets bilag II, litra i.

Kravet om at de omfattede oplysninger skal opbevares i minimum seks år er fastsat ud fra en vurdering af kravene til opbevaring af bogføringsmateriale i bogføringsloven og til forældelsesreglerne i 1908-loven med tillæg af et år svarende til den indeværende regnskabsperiode.

Bestemmelsen er ikke til hinder for, at nøglecentret indgår aftaler med underskriveren om, at de omfattede oplysninger skal opbevares i længere tidsperioder. Dette kan være særligt relevant i forbindelse med kontraktforhold, som kan forventes at løbe over længere tidsperioder

Registreringen af oplysningerne kan ske elektronisk, idet oplysningerne i så fald må sikres på betryggende vis.

Til stk. 2

I stk. 2 kræves det, at nøglecentre, der udsteder kvalificerede certifikater, skal benytte pålidelige systemer til opbevaring af certifikater i verificerbar form. Dvs. det skal efterfølgende være muligt at verificere indholdet af certifikatet. Det skal sikres, at kun bemyndigede personer kan foretage tilføjelser og ændringer i certifikatet. Såfremt sikkerheden omkring indeholdet af certifikatet, samt oplysningerne om hvorvidt det er spærret, kan ændres af enhver i nøglecenterets organisation, eller der ikke er fastlagt klare retningslinjer for, hvorledes disse ændringer kan foretages og af hvem, kan det have betydning for tilliden til den elektroniske signatur.

Tekniske ændringer i nøglecenterets elektronisk signatur produkter, dvs. et software eller hardware baseret produkt, som anvendes af et nøglecenter til levering af tjenesteydelser i forbindelse med elektronisk signatur, eller som anvendes i forbindelse med generering eller verificering af en elektronisk signatur, der kan bringe kravene til nøglecentrets systemer og produkter i fare, skal være synlige for det personale i nøglecentret, der bruger systemerne. Det skal sikres, at det personale, der betjener nøglecenterets produkter og systemer, bliver gjort opmærksom på at handlinger, der foretages, kan bringe sikkerhedskravene i fare.

Det er således ikke ved enhver teknisk ændring, der skal gøres opmærksom på, at sikkerhedskravene kan bringes i fare. Det er alene ændringer, der kan medføre, at certifikatets ægthed ikke kan kontrolleres, at certifikater offentliggøres, hvor underskriveren ikke har givet sit samtykke hertil, eller ændringer der indebærer, at der kan foretages ændringer i certifikaterne af personer, der ikke er autoriseret hertil.

Bestemmelsen forpligter således nøglecentret til ved hjælp af den teknologi, der til enhver tid er til rådighed at sikre de systemer, der anvendes i nøglecentret.

Til stk. 3

Det er ifølge stk. 3 forbudt for et nøglecenter, der udsteder kvalificerede certifikater at opbevare eller kopiere de personers signaturgenereringsdata, som det har udstedt et certifikat til.

Opbevaring og kopiering af signaturgenereringsdata vil kunne udgøre en alvorlig trussel mod den juridiske anerkendelse af elektroniske signaturer. Der bør være sikkerhed for, at det alene er underskriveren, der har adgang til signaturgenereringsdataene, og dermed, at det kun er underskriveren, der har haft mulighed for at benytte sin elektroniske signatur.

Bestemmelsen er en implementering af direktivets bilag II, litra j.

Til kapitel 5

Erstatningsansvar

Til § 11

Til stk. 1

Bestemmelsen fastlægger de ansvarsregler, der gælder for nøglecentre, der udsteder kvalificerede certifikater, eller som overfor offentligheden indestår for sådanne certifikater. Et dansk nøglecenter kan overfor offentligheden indestå for, at et andet nøglecenters, herunder også et udenlandsk nøglecenters, certifikater overholder reglerne for udstedelse af kvalificerede certifikater, jf. stk. 1.

Nøglecentret er ansvarlig for tab hos den, der med rimelighed forlader sig på et certifikat. Det vil både sige modtageren af en elektronisk signatur med et tilknyttet certifikat, men også underskriveren. Der kan også blive tale om, at nøglecentret kan pådrage sig et erstatningsansvar for tab hos en tredjemand, der lider tab som følge af nøglecentrets uagtsomhed.

Bestemmelsen vedrører ikke forholdet mellem afsender og modtager af et kvalificeret certifikat.

Nøglecentret er i følge *nr. 1* ansvarlig for, at alle oplysningerne i certifikatet er korrekte. Heri ligger eksempelvis, at de pågældende oplysninger om underskriverens identitet skal være korrekte, jf. også bemærkningerne til lovforslagets § 6.

Nøglecentret er ifølge *nr. 2* erstatningsansvarlig for tab, der skyldes, at et kvalificeret certifikat ikke indeholder alle de oplysninger, der er krævet i § 4.

Nøglecentret er ifølge *nr. 3* erstatningsansvarlig for tab, der opstår som følge af manglende spærring af et certifikat straks efter, at der er modtaget anmodning herom, jf. § 9, stk. 2.

Ifølge *nr. 4* er et nøglecenter ansvarlig for tab, der følger af, manglende eller fejlagtig information om spærring af certifikatet. Nøglecentret bliver ligeledes ansvarlig for tab, der opstår som følge af, at der ikke er givet information om, at et certifikat er udløbet, eller der ikke er oplyst om eventuelle formålsbegrænsninger eller beløbsbegrænsninger, jf. §§ 9, stk. 1 og 3.

Nr. 5 fastsætter, at nøglecentret er ansvarlig for tab opstået som følge af, at de sikkerhedsforskrifter, der er opregnet i § 7, ikke er blevet overholdt.

Til stk. 2

§ 11 har et forbrugerbeskyttende sigte, idet bestemmelsen fastsætter et culpaansvar med omvendt bevisbyrde. Der påhviler således nøglecentret et ansvar at godtgøre, at centret ikke har handlet uagtsomt eller forsætligt.

Begrundelsen for at indføre dette skærpede ansvar for visse nøglecentre er 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 nøglecentret har begået fejl eller forsømmelser, der kan bedømmes som værende culpøse eller forsætlige.

Bestemmelsen er udformet i overensstemmelse med lignende regler om præsumptionsansvar i anden lovgivning.

Pålæggelse af et skærpet erstatningsansvar kan være med til at sikre den fornødne tillid og dermed en øget anvendelse af kvalificerede certifikater.

For at der kan pålægges nøglecentret et erstatningsansvar for tab lidt hos underskriveren eller tredjemand efter bestemmelsen, skal de øvrige betingelser efter den almindelige erstatningsret ligeledes være opfyldt.

Til stk. 3

Stk. 3 fritager et nøglecenter for tab, der opstår ved brug af et kvalificeret certifikat udenfor de begrænsninger, der er fastsat for certifikatet. Såfremt certifikatet anvendes uden for formåls- og beløbsbegrænsninger for certifikatet, er nøglecenteret ikke ansvarlig for tab, der må opstå som følge heraf.

Det er en forudsætning for, at nøglecentret kan undgå erstatningsansvaret efter stk. 1 og 2, at begrænsningerne fremgår tydeligt af certifikatet, jf. § 4, og at de på forespørgsel oplyses af nøglecentrets katalog- og tilbagekaldelsestjeneste, jf. § 9, stk. 1 og 3.

Til stk. 4

I stk. 4 fastsættes det, at ikke er muligt at fravige det særlige ansvar efter stk. 1-3 ved forudgående aftale.

Til stk. 5

Bestemmelsen i stk. 5 fastslår, at såfremt et kvalificeret certifikat anvendes i situationer, der både er omfattet af dette lovforslag og af reglerne i det forslag til lov om visse betalingsmidler, som er under behandling i Folketinget, finder denne lov kun anvendelse i det omfang, tabet ikke dækkes efter i §§ 10 og 11 i lov om visse betalingsmidler.

Bestemmelsen skal sikre, at forhold, der måtte være omfattet af både lov om visse betalingsmidler og dette lovforslag, bedømmes efter det strengeste regelsæt. Skadelidte har herved størst mulig sikkerhed for at få sit tab erstattet.

Anvendes et kvalificeret certifikat, som findes på et såkaldt »multi-applikationskort« - det vil sige et kort, der kan anvendes både som betalingsmiddel og til andre formål - i situationer, der ikke er omfattet af lov om visse betalingsmidler, skal et eventuelt ansvar for nøglecentret bedømmes efter dette forslags § 11.

§ 11, stk. 1, nr. 1 og 2 er en implementering af direktivets artikel 6, stk. 1, litra a. Stk. 2, nr. 3 implementerer direktivets artikel 6, stk. 2. Bestemmelsen udvider dog ansvaret til også at omfatte manglende oplysninger om, at certifikatet er udløbet, samt oplysninger om at der er fastsat begrænsninger for brugen af certifikatet.

Med henvisningen til § 7 i forslagets § 11, stk. 2, nr. 4 implementeres direktivets artikel 6, stk. 1, litra b og c, hvorefter et nøglecenter er erstatningsansvarlig for tab, der opstår som følge af den underskriver, der er identificeret i certifikatet, ikke på udstedelsestidspunktet var i besiddelse af de signaturgenereringsdata, der svarer til de i certifikatet indeholdte signaturverificeringsdata. Nøglecentret pådrager sig ligeledes et erstatningsansvar, såfremt signaturgenereringsdata og signaturverificeringsdata ikke kan anvendes komplementært i de tilfælde, hvor det er nøglecentret, der har leveret begge datasæt, jf. § 11, stk. 2, nr. 4 sammenholdt med § 7, stk. 2.

Bestemmelserne i § 11 indeholder et særligt strengt erstatningsansvar for nøglecentrene i visse i bestemmelsen angivne situationer. Uden for disse situationer gælder dansk rets almindelige erstatningsregler.

§ 11 regulerer ikke spørgsmål om, hvorvidt nøglecentret kan søge regres over for andre for erstatninger udbetalt efter § 11.

Til Kapitel 6

Supplerende krav til behandling af personoplysninger

Kapitel 6 gælder for alle nøglecentre etableret i Danmark, uanset om de udbyder kvalificerede certifikater, eller om de udbyder certifikater til offentligheden.

Til § 12

Bestemmelsen regulerer adgangen til at behandle personoplysninger i forbindelse med udøvelse af nøglecentervirksomhed omfattet af denne lov.

Bestemmelsen gælder for alle nøglecentre, etableret i Danmark, jf. også bemærkningerne til § 2.

Bestemmelsen finder anvendelse både i relation til indsamling af personoplysninger i forbindelse med udstedelsen af et certifikat og ved den efterfølgende opretholdelse af certifikatet.

Reglerne i det fremsatte forslag til lov om behandling af personoplysninger vil i øvrigt finde anvendelse med de afvigelser, som følger af bestemmelsen.

Efter stk. 1 må et nøglecenter kun indsamle personoplysninger i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat. Oplysninger må desuden kun indsamles fra den registrerede, som normalt vil være lig med underskriveren, medmindre denne har givet sit udtrykkelige samtykke til at indsamling af oplysninger også kan ske fra andre. Udtrykket »udtrykkelige samtykke« skal forstås i overensstemmelse med § 3, nr. 8 sammenholdt med § 6, stk. 1, nr. 1, i lov om behandling af personoplysninger.

Stk. 2 fastsætter, at et nøglecenter kun må behandle og videregive personoplysninger indsamlet efter stk. 1 til andre formål end til at udstede og opretholde et certifikat, såfremt den registrerede har givet sit udtrykkelige samtykke hertil.

Telestyrelsen fører, jf. § 18, tilsyn med overholdelsen af bestemmelsen og kan i den forbindelse udstede påbud til et nøglecenter om at overholde bestemmelsen og eventuelt pålægge det tvangsbøder.

Bestemmelsen implementerer direktivets artikel 8.

Til kapitel 7

Elektronisk signatur og formkrav

Til § 13

Den foreslåede bestemmelse indeholder en »udfyldningsregel«, som har til formål at give visse formkrav i retsregler andre steder i lovgivningen et bestemt indhold. Det drejer sig om retsregler, der indebærer et krav om, at en elektronisk meddelelse skal være forsynet med underskrift, signatur eller lignende. Af bestemmelsen følger, at sådanne krav skal anses for opfyldt, hvis der anvendes en elektronisk signatur, der lever op til visse sikkerhedskrav, fordi der er tale om en avanceret elektronisk signatur, jf. § 3, stk. 1, nr. 2, som endvidere er baseret på et kvalificeret certifikat, jf. § 4, og fremkommet ved brug af et sikkert signaturgenereringssystem, jf. § 14 og § 15.

Bestemmelsen har alene virkning for underskriftskrav m.v., som kan opfyldes ved brug af en elektronisk signatur, og har således ikke betydning for spørgsmålet om, hvornår dette er tilfældet. På nuværende tidspunkt indeholder dansk ret ikke regler, der foreskriver anvendelse af elektroniske signaturer. Derimod findes der en del retsregler, der indeholder krav om underskrift.

Om et sådant formkrav kan opfyldes ved brug af en elektronisk signatur, skal som hidtil afgøres efter reglerne på det pågældende retsområde. Fører en fortolkning af disse regler til, at kravet kan opfyldes ved anvendelse af en elektronisk signatur, følger det imidlertid af den foreslåede bestemmelse, at en meddelelse, der er forsynet med en avanceret elektronisk signatur, som opfylder de ovenfor nævnte betingelser, ikke vil kunne afvises eller i øvrigt fratages virkning med den begrundelse, at den ikke opfylder det pågældende krav om underskrift.

Til et formkrav om signatur mv. vil der kunne være knyttet andre betingelser. Ofte vil opfyldelse af sådanne formkrav formentlig forudsætte, at signaturen stammer fra og dermed identificerer en bestemt person. Elektronisk signatur vil ofte være knyttet til en bestemt person, men der vil også kunne udstedes certifikater med et pseudonym, jf. § 4, stk. 2, nr. 3, ligesom det vil kunne forekomme, at et certifikat identificerer en juridisk person (et selskab, en forening, en fond eller lignende), men derimod ikke den person, der afgiver signaturen for den juridiske person. Den foreslåede bestemmelse har alene betydning for spørgsmålet om, hvad der skal til for at opfylde et krav om, at en meddelelse skal være forsynet med signatur eller lignende. Derimod regulerer bestemmelsen

f.eks. ikke, om man kan anvende en signatur med et pseudonym til at opfylde et sådant formkrav.

Den foreslåede bestemmelse indebærer, at der som udgangspunkt ikke vil kunne stilles strengere krav end dem, der følger af reglerne i denne lov om avancerede elektroniske signaturer, kvalificerede certifikater og sikre signaturgenereringssystemer, for at anse et krav om underskrift for opfyldt ved brug af en elektronisk signatur. Direktivets artikel 5, stk. 1, litra a, som tilsigtes gennemført ved bestemmelsen, giver således som udgangspunkt ikke mulighed for at stille sådanne strengere krav.

Der vil dog kunne stilles strengere krav til elektroniske meddelelser til og fra offentlige myndigheder. Dette følger af direktivets artikel 3, stk. 7, som indeholder en begrænset undtagelse herom. I givet fald skal sådanne krav være objektive, gennemsigtige, forholdsmæssige og ikke-diskriminerende.

For så vidt angår muligheden for at opfylde kravene i denne bestemmelse med et kvalificeret certifikat, udstedt af et nøglecenter etableret uden for Danmark, henvises til bemærkningerne til § 2 og § 23.

Til kapitel 8

Sikre signaturgenereringssystemer

Til § 14

Til stk. 1-2

Stk. 1-2 indeholder de krav, som et signaturgenereringssystem, jf. definitionen heraf i § 3, nr. 5, skal opfylde for at kunne betegnes som et sikkert signaturgenereringssystem. Kravene svarer til indholdet af direktivets bilag III.

Hvorvidt en elektronisk signatur er skabt ved brug af et sikkert signaturgenereringssystem har betydning for, hvilke retsvirkninger den pågældende signatur kan tillægges, jf. herved bemærkningerne til § 13.

Til stk. 3

Bestemmelsen implementerer direktivets artikel 3, stk. 5, 2. pkt., der kræver, at Medlemsstaterne formoder, at signaturgenereringssystemer, der overholder almindelig anerkendte standarder, som Kommissionen har fastsat efter proceduren i direktivets artikel 9 og offentliggjort i EF-Tidende, opfylder kravene til et sikkert signaturgenereringssystem, jf. direktivets bilag III.

Det vides endnu ikke, hvornår Kommissionen vil være i stand til at fastsætte og offentliggøre sådanne standarder.

Bestemmelsen udfylder de meget overordnede krav, som er fastsat i medfør af stk. 1 på den måde, at en virksomhed, der ønsker at udvikle et sikkert signaturgenereringssystem kan indrette systemet, så det overholder de offentliggjorte standarder og dermed få større sikkerhed for, at det kan blive efterprøvet med et positivt resultat.

Bestemmelsen kan medvirke til at skabe et indre marked for sikre signaturgenereringssystemer og skal ses i sammenhæng med § 15, stk. 3.

Til § 15

Til stk. 1

I stk. 1 bemyndiges Forskningsministeren til at udpege et eller flere egnede organer eller myndigheder til at medvirke til at efterprøve, om signaturgenereringssystemer opfylder kravene til sikre signaturgenereringssystemer, jf. § 14.

Bestemmelsen giver mulighed for, at et privat organ kan udpeges til at forestå de nævnte efterprøvelser.

Muligheden for at få efterprøvet et signaturgenereringssystem af et organ eller en myndighed udpeget efter stk. 1 omfatter ikke kun udbydere af sådanne systemer, som er etableret i Danmark men også nøglecentre etableret i et land inden for Det Europæiske Økonomiske Samarbejde (EØS).

Endvidere gives der i bestemmelsen hjemmel til, at Forskningsministeren kan fastsætte regler om de nærmere procedurer, efter hvilke efterprøvelsen skal foretages. Disse kan strække sig fra en egentlig kontrol af, om systemet overholder kravene i § 14, stk. 1 og 2, til forskellige grader af selv-deklarering efter på forhånd fastlagte procedurer og i samarbejde med et bemyndiget organ, sålede som det kendes fra eksempelvis reguleringen af radio- og teleterminaludstyr.

I medfør af direktivets artikel 3, stk. 4, skal Kommissionen fastlægge en række kriterier for, hvorledes Medlemsstaterne afgør, om et organ eller en myndighed er egnet til at blive udpeget til at efterprøve signaturgenereringssystemer.

Hjemlen i stk. 1 vil formentlig først blive udnyttet, når Kommissionen har fastlagt sådanne kriterier, hvorved det vil det være muligt at fastsætte de administrative rammer for etablering af et eller flere prøvningsorganer, jf. også de almindelige bemærkninger.

Udgifterne i forbindelse med efterprøvelse af, om et signaturgenereringssystem opfylder kravene i § 14, stk. 1 og 2, forudsættes afholdt af producenterne af de pågældende systemer. Regler herom vil kunne fastsættes i medfør af bemyndigelsen i § 15, stk. 1.

Til stk. 2

For at et signaturgenereringssystem skal kunne betegnes som et sikkert signaturgenereringssystem, skal det være efterprøvet, at produktet lever op til minimumskravene i § lovens 14. Efterprøvelsen skal ske i henhold til de i medfør at stk. 1 fastsatte regler.

Betegnelsen et sikkert signaturgenereringssystem må således kun anvendes, når en efterprøvelse som nævnt i stk. 1 er sket.

Til stk. 3

I stk. 3 fastslås det, at et sikkert signaturgenereringssystem, som er blevet efterprøvet af et organ eller en myndighed udpeget i et andet EØS-land, ikke skal godkendes efter stk. 1 for at blive markedsført eller anvendt i forbindelse med avancerede elektroniske signaturer på det danske marked.

Bestemmelsen implementerer direktivets artikel 3, stk. 4, 2. pkt. og artikel 4, stk.2.

Signaturgenereringssystemer, som er efterprøvet efter stk. 1, vil tilsvarende kunne markedsføres og anvendes i andre EØS-lande, uden at skulle efterprøves i disse lande. Herved skabes der mulighed for etableringen af et indre marked for signaturgenereringssytemer.

Til kapitel 9

Tilsyn m.v.

Bestemmelserne i kapitel 9 er en implementering af direktivets krav i artikel 3, stk. 3, om at medlemsstaterne skal sikre, at der føres tilsyn med udbyderne af kvalificerede certifikater. Tilsynet omfatter desuden overholdelsen af § 12, som stiller krav til samtlige nøglecentre etableret i Danmark.

Til § 16

Til stk. 1

Nøglecentre, som udsteder kvalificerede certifikater, skal overholde en række krav fastsat i kapitel 4, og bestemmelser som fastsættes i medfør heraf.

For at Telestyrelsen kan blive informeret om eksistensen af et nyt nøglecenter på det danske marked, fastsættes det, at nøglecentret skal foretage en anmeldelse til Telestyrelsen senest samtidig med, at det påbegynder udstedelse af kvalificerede certifikater.

På denne måde får Telestyrelsen et overblik over virksomhederne på det danske marked og kan fra starten gå ind og kontrollere, at virksomheden og dens tjenester overholder lovens krav.

Det følger af bestemmelsen i § 2, at anmeldelseskravet til Telestyrelsen kun finder anvendelse på nøglecentre etableret i Danmark, der udsteder certifikater til offentligheden.

Der er ikke tale, om at nøglecentret skal godkendes eller autoriseres af Telestyrelsen for, at nøglecentret kan påbegynde sin virksomhed. Et sådant krav vil være i strid med direktivets artikel 3, stk. 1, der forbyder medlemsstaterne at stille krav om forudgående autorisation som en betingelse for, at et nøglecenter kan drive virksomhed.

Manglende overholdelse af anmeldelseskravet i stk. 1 medfører ikke, at nøglecentret kan forbydes at drive virksomhed som nøglecenter. Telestyrelsen kan give nøglecentret et pålæg om at foretage en anmeldelse og eventuelt pålægge tvangsbøder for den manglende anmeldelse. Telestyrelsen kan desuden i ekstraordinære tilfælde give udbyderen pålæg om ikke at betegne sine certifikater som kvalificerede certifikater, jf. § 18, stk. 6.

Til stk. 2

I stk. 2 fastsættes det, hvilke oplysninger et nøglecenter skal fremsende til Telestyrelsen i forbindelse med anmeldelsen. De nævnte oplysninger skal tjene som en generel orientering af Telestyrelsen om nøglecentret. Der stilles ikke krav om, at et nøglecenter, der udsteder kvalificerede certifikater, skal være organiseret i en bestemt selskabsform.

Til Stk. 3

Stk. 3 fastsætter, at nøglecentret skal anmelde enhver ændring i nøglecentrets navn, hjemsted, evt. selskabsform, ledelse og systemrevisor til Telestyrelsen, senest 8 dage efter at ændringen er sket.

Til stk. 4

Bestemmelsen bemyndiger Telestyrelsen til at fastsætte nærmere krav til, hvilke oplysninger et nøglecenter skal indsende, udover de i stk. 2 nævnte oplysninger.

Til § 17

Det er som nævnt i de indledende bemærkninger og i bemærkningerne til § 5 og § 18 tanken, at det tilsyn, som Telestyrelsen skal føre med nøglecentre, der udsteder kvalificerede certifikater, i vidt omfang skal baseres på oplysninger, som nøglecentrets valgte systemrevision udarbejder.

Rapporten skal sætte Telestyrelsen i stand til at vurdere, om der er forhold, som indikerer, at tilsynet bør anvende sine reaktionsmuligheder i henhold til loven ved at afkræve nøglecentret yderligere oplysninger eller eventuelt skride ind over for nøglecentret ved at give forskellige pålæg, idømme tvangsbøder eller i gi-

vet fald at fratage nøglecentret retten til at anvende betegnelsen kvalificerede certifikater om de certifikater, som det udsteder.

Til stk. 1

I medfør af stk. 1 skal nøglecentret indsende en rapport til Telestyrelsen samtidig med, at det foretager en anmeldelse i medfør af § 16. Rapporten skal give Telestyrelsen et grundlag for at bedømme, om nøglecentret overholder lovgivningens krav til nøglecentre, der udsteder kvalificerede certifikater.

Til stk. 2

Rapporten skal ifølge *nr. 1* for det første indeholde en beskrivelse af nøglecentrets virksomhed og de systemer, som anvendes af nøglecentret. Af beskrivelsen skal det særligt fremgå, hvorledes kravene i kapitel 4 til nøglecentret konkret sikres overholdt.

For det andet skal nøglecentrets ledelse, jf. *nr. 2* i rapporten afgive en erklæring om, hvorvidt den samlede data-, system- og driftssikkerhed i nøglecentret må anses for betryggende og i overensstemmelse med kapitel 4, samt regler fastsat i medfør heraf.

Ved udtrykket nøglecentrets ledelse forstås i denne sammenhæng bestyrelsen, direktionen i virksomheder uden bestyrelse, eller et tilsvarende ledelsesorgan afhængigt af, hvorledes nøglecentret er organiseret. Ledelsens erklæring til Telestyrelsen giver sammen med den lignende erklæring fra den valgte systemrevisor Telestyrelsen en viden om, hvorvidt nøglecentret har de nødvendige forretningsgange, sikkerhedsprocedurer, m.v., som gør det muligt for nøglecentret at overholde kravene i lovens kapitel 4 og bestemmelser fastsat i medfør heraf.

I *nr. 3* fastsættes krav om, at den valgte systemrevisor, jf. § 5, stk. 2, skal afgive en særskilt erklæring om, i hvilket omfang den samlede data-, system- og driftssikkerhed i nøglecentret må anses for betryggende og i overensstemmelse med kapitel 4, samt regler fastsat i medfør heraf.

Formålet med at stille krav til både ledelsen af nøglecentret og den valgte systemrevisor om at afgive en erklæring i tilknytning til den rapport, som skal indsendes til Telestyrelsen, er at få to uafhængige vurderinger af, om nøglecentret overholder loven. Selskabets ledelse er ansvarlig for den løbende overholdelse af kravene i loven og må forventes at have det mest detaljerede kendskab til, om der kunne være problemer i den forbindelse. Den valgte systemrevisor må formodes også at have et solidt kendskab til nøglecentrets virksomhed og har derudover særlig ekspertise i relation til revision, dokumentation, etc.

Til stk. 3

I stk. 3 stilles der krav om, at nøglecentret en gang årligt skal udarbejde en ny opdateret rapport vedrørende nøglecentrets overholdelse af kravene i lovgivningen.

Rapporten med erklæringer skal indsendes til Telestyrelsen inden et tidspunkt, som fastsættes af Telestyrelsen. Telestyrelsen fastsætter samtidig, hvilken tidsperiode rapporten skal vedrøre. Som udgangspunkt bør indsendelsestidspunktet ikke fastsættes til at være mere end 3 måneder efter denne tidsperiode for at sikre, at de oplysninger, som modtages, ikke er forældede.

Telestyrelsen kan bestemme indsendelsestidspunktet for rapporter fra de enkelte nøglecentre med henblik på at undgå, at samtlige rapporter indsendes på det samme tidspunkt. Herved kan der sikres en bedre udnyttelse af styrelsens ressourcer. Samtidig kan der tages hensyn til de enkelte nøglecentre, som blandt kan have forskellige regnskabsår, eller lignende.

Det forudsættes, at tidspunktet for det enkelte nøglecenters indsendelse af den årlige rapport ikke kan ændres i de følgende år, medmindre særlige grunde taler herfor.

Den opdaterede rapport og erklæringerne fra ledelsen og den valgte systemrevisor er et vigtigt redskab for Telestyrelsens løbende tilsyn af, om nøglecentret overholder lovens krav.

Til stk. 4

I stk. 4 bemyndiges Telestyrelsen til at fastsætte nærmere krav til indholdet af den rapport, som skal indsendes til Telestyrelsen første gang i forbindelse med anmeldelsen af nøglecentret og efterfølgende en gang årligt, til de erklæringer, som ledelsen og den valgte systemrevisor skal afgive samt om systemrevisionens gennemførelse i nøglecentre, der udsteder kvalificerede certifikater.

Bemyndigelsen giver mulighed for, at der fastsættes mere præcise krav til indholdet af dokumentation, sådan at dokumentationen fra de forskellige nøglecentre får et sammenligneligt indhold, samt giver mulighed for at afgrænse, hvilke typer af oplysninger, som Telestyrelsen vurderer er nødvendige, for at styrelsen kan udføre sine opgaver i henhold til loven.

Der kan desuden fastsættes yderligere krav til indholdet af den erklæring, som ledelsen og den valgte systemrevisor skal indsende til Telestyrelsen.

Endelig bemyndiges Telestyrelsen til at fastsætte de overordnede rammer for, hvorledes systemrevisionen skal gennemføres i et nøglecenter, herunder blandt andet krav til omfanget af systemrevisionen, krav til sy-

stemrevisionens arbejdsvilkår, dens adgang til deltagelse i ledelsesmøder, udarbejdelse af en særskilt revisionsprotokol, samarbejde med den interne revision i nøglecentret, såfremt en sådan eksisterer, krav vedrørende systemrevisors kvalifikationer, m.v.

Til § 18

Til stk. 1

Telestyrelsen udpeges til at varetage det overordnede tilsyn med overholdelsen af loven.

Telestyrelsen skal føre kontrol med, at kravene i loven til både nøglecentret, og de certifikater nøglecentret udsteder, overholdes. Ved at stille krav om at nøglecentre, der udsteder kvalificerede certifikater, underlægges et statsligt tilsyn, er det hensigten at sikre, at de nøglecentre, som benytter betegnelsen kvalificerede certifikater om de certifikater, de udsteder, har et kvalitets- og sikkerhedsniveau, som brugerne kan have tillid til.

Telestyrelsen skal kun i begrænset omfang føre tilsyn med nøglecentre, som ikke ønsker at udstede kvalificerede certifikater. Lovens regler finder med undtagelse af § 12 ikke anvendelse på disse virksomheder. Disse nøglecentre vil kunne oprettes frit og drive deres virksomhed i henhold til kvalitetskrav og standarder, som findes i markedet.

I modsætning til det tilsyn der i dag føres med virksomheder på det finansielle område, er det ikke hensigten, at Telestyrelsen skal foretage inspektioner af de tilsynsbelagte virksomheder

Hovedopgaven for Telestyrelsen vil være at foretage en vurdering af de rapporter, som nøglecentrene skal udarbejde og indsende til Telestyrelsen, når nøglecentret påbegynder sin virksomhed og herefter en gang årligt.

Såfremt de oplysninger, som Telestyrelsen har modtaget fra nøglecentret, dets revision, brugerne eller andre, giver anledning til at betvivle, at nøglecentret overholder lovens krav, skal Telestyrelsen benytte sig af de reaktionsmuligheder, som der er givet hjemmel til i loven.

I bestemmelsen fastsættes endvidere de nærmere regler for Telestyrelsens kompetence til at træffe afgørelser over for de nøglecentre, der udsteder kvalificerede certifikater. Styrelsen har mulighed for at udstede påbud, idømme tvangsbøder og fratage et nøglecenter retten til at betegne de certifikater, det udsteder som kvalificerede certifikater.

Der kan forekomme tilfælde, hvor et nøglecenter samtidig er underlagt andre tilsynsordninger, f.eks. på det finansielle område. Bestemmelsen regulerer ikke dette. Det forudsættes dog, at Telestyrelsen og de relevante tilsynsmyndigheder i nødvendigt omfang samarbejder med henblik på at undgå unødvendig dobbeltregulering, og lignende af nøglecentre.

Til stk. 2

I stk. 2 gives der hjemmel til, at Telestyrelsen kan udstede påbud til et nøglecenter med henblik på at sikre, at lovens bestemmelser overholdes.

I *nr. 1* gives der hjemmel til, at Telestyrelsen kan påbyde et nøglecenter at foretage en anmeldelse, jf. § 16, herunder at kræve yderligere oplysninger, hvis nøglecentrets anmeldelse er mangelfuld.

I medfør af *nr. 2* kan Telestyrelsen påbyde et nøglecenter at indsende rapporter, jf. § 17 til Telestyrelsen, herunder at indsende yderligere oplysninger, m.v., såfremt nøglecentret har indsendt en mangelfuld rapport til Telestyrelsen.

I medfør af *nr. 3* kan Telestyrelsen i de tilfælde, hvor styrelsen mener, at et nøglecenter ikke overholder bestemmelserne i denne lov, udstede påbud til nøglecentret om at bringe det pågældende forhold vedrørende nøglecentrets virksomhed i overensstemmelse med lovgivningen.

Ved en konkret mistanke om, at der er begået en strafbar handling kan bestemmelsen ikke anvendes til at påbyde det pågældende nøglecenter eller systemrevisor at fremskaffe yderligere oplysninger, eller foretage undersøgelser vedrørende forhold, der er omfattet af mistanken. I så fald skal myndigheden gå frem efter strafferetsplejens regler. Tilsvarende gælder i relation til oplysningsforpligtelserne i forslagets § 19, stk. 1 og 2 og § 20, stk. 2 og 3, samt ved iværksættelse af en ekstraordinær revision, jf. § 19, stk. 5.

Til stk. 3

I forbindelse med udstedelse af et påbud efter stk. 2 fastsætter Telestyrelsen en tidsfrist for nøglecentrets opfyldelse heraf. Tidsfristens længde må afhænge af forholdene i den konkrete situation, herunder om Telestyrelsen finder, at der muligvis kan være behov for at anvende hjemlen i stk. 6 til at fratage et nøglecenter retten til at udstede kvalificerede certifikater.

Til stk. 4

Telestyrelsen bemyndiges i stk. 4 til at pålægge et nøglecenter tvangsbøder, såfremt det ikke efterkommer påbud udstedt i medfør af stk. 2

Til stk. 5

I medfør af stk. 5 kan Telestyrelsen foranstalte en ekstraordinær systemrevision i et nøglecenter, der udsteder kvalificerede certifikater. Bestemmelsen giver Telestyrelsen mulighed for at skaffe sig selv og nøg-

lecentrets ledelse et overblik over en række forhold i virksomheden, som Telestyrelsen ud fra de foreliggende oplysninger har fundet behov for at få oplyst. Telestyrelsen udpeger den systemrevisor, som skal udføre den ekstraordinære systemrevision og fastsætter de nærmere rammer for gennemførelsen heraf. Den udpegede systemrevisor kan enten være den af nøglecentret valgte systemrevisor eller en anden systemrevisor.

Telestyrelsen kan pålægge nøglecentret at afholde udgifterne i forbindelse med en ekstraordinær systemrevision. Dette vil normalt være tilfældet, hvor anledningen til Telestyrelsens iværksættelse af den ekstraordinære systemrevision har været afgivelse af utilstrækkelige oplysninger til Telestyrelsen fra nøglecentrets ledelse eller den valgte systemrevisor.

Til stk. 6

I medfør af stk.6 kan Telestyrelsen fratage et nøglecenter retten til at anvende betegnelsen kvalificerede certifikater i grovere tilfælde, hvor nøglecentret trods et påbud og idømmelse af tvangsbøder ikke efterlever påbud fra Telestyrelsen, groft eller gentagne gange har overtrådt lovens regler, eller hvis nøglecentret anmelder betalingsstandsning eller kommer under konkurs.

Det er en forudsætning for, at bemyndigelsen kan bringes i anvendelse over for et nøglecenter, at der er tale om en situation, hvor der er umiddelbart behov at beskytte brugerne af de udstedte certifikater.

Til stk. 7 og 8

Bestemmelserne fastsætter, at en afgørelse fra Telestyrelsen efter stk. 6 om at fratage et nøglecenter retten til at anvende udtrykket kvalificerede certifikater kan kræves indbragt for domstolene. Samtidig fastsættes regler for, i hvilke situationer, der kan træffes afgørelse om, at en indbringelse af Telestyrelsens afgørelse for domstolene kan tillægges opsættende virkning.

Til § 19

Bestemmelsen fastsætter en adgang for Telestyrelsen til at kræve meddelt oplysninger med henblik på varetagelse af styrelsens tilsynsrolle.

Som nævnt ovenfor til bemærkningerne til § 18, stk. 2, kan oplysningsforpligtelsen ikke anvendes til at afkræve en person eller en virksomhed yderligere oplysninger i tilfælde, hvor der er en konkret mistanke om, at der er begået en strafbar handling.

Til stk. 1

I bestemmelsen gives Telestyrelsen adgang til at indhente oplysninger hos alle nøglecentre, som udsteder kvalificerede certifikater, samt af andre virksomheder og personer med henblik på at kunne vurdere, hvorvidt de er omfattet af loven.

Til stk. 2

I stk. 2 pålægges nøglecentrets ledelse og system revisor en forpligtelse til straks at meddele Telestyrelsen om forhold, der er af afgørende betydning for nøglecentrets fortsatte virksomhed. Større systemnedbrud i nøglecentret eller problemer med at overholde kravet i § 5, stk.1, nr. 5 om nøglecentrets økonomiske ressourcer, herunder tilfælde, hvor nøglecentret kommer under konkurs eller anmelder betalingsstandsning, vil være eksempler på situationer, hvor Telestyrelsen skal underrettes. Telestyrelsens reelle mulighed for at gribe ind over for et nøglecenter, som af den ene eller anden grund har vanskeligt ved at overholde krav i loven, afhænger i vidt omfang af, om Telestyrelsen modtager de relevante oplysninger i tide.

Til § 20

Til stk. 1

Der gives Telestyrelsen en bemyndigelse til at påbyde et nøglecenter inden for en fastsat tidsfrist at vælge en ny systemrevisor i et nøglecenter, hvis fungerende systemrevisor findes åbenbart uegnet til at varetage sit hverv.

Den kontrol, som systemrevisionen udfører af nøglecentrets virksomhed, udgør en meget vigtig del af det tilsyn, som føres med nøglecentrene, og derfor er det særlig vigtigt, at systemrevisionens kontrol er af høj kvalitet. Telestyrelsen bemyndiges derfor til at kunne gribe ind i de tilfælde, hvor det skønnes, at en revisor for et nøglecenter åbenbart må anses for uegnet til sit hverv.

Til stk. 2

I *stk. 2* gives Telestyrelsen hjemmel til i særlige tilfælde at afkræve revisionen i et nøglecenter oplysninger om nøglecentret uden tilladelse fra nøglecentrets ledelse. Formålet er at give Telestyrelsen mulighed for bedre at foretage en vurdering af, om der er i problemer ved nøglecentrets virksomhed set i forhold til lovens bestemmelser.

Til stk. 3

I henhold til stk. 3 skal nøglecentret og systemrevisor hver især give Telestyrelsen en redegørelse i de tilfælde, hvor en revisor har fratrådt sit hverv. Telestyrelsen bliver hermed gjort opmærksom på eventuelle problemer i nøglecentret.

Vedrørende anvendelsen af bestemmelserne i stk. 2 og 3 i situationer, hvor der er konkret mistanke om, at der er begået en strafbar handling, henvises til bemærkningerne ovenfor til § 18, stk. 2.

Til § 21

I bestemmelsen fastsættes det, at Telestyrelsens afgørelser truffet i medfør af loven eller bestemmelser fastsat i medfør af loven ikke kan påklages til en anden administrativ myndighed. Klagere vil derfor være henvist til at indbringe Telestyrelsens afgørelser til domstolene eller Ombudsmanden.

De afgørelser, Telestyrelsen vil kunne træffe i medfør af loven, må forventes hovedsageligt at vedrøre driftsmæssige og tekniske forhold, i relation til den virksomhed et nøglecenter kan udføre.

Det må forventes, at antallet af nøglecentre omfattet af loven i hvert fald i den nærmeste fremtid vil være ganske beskedent. Da en ankeinstans dels skal have indgående teknisk kendskab vedrørende elektroniske signaturer og nøglecentres virksomhed for at være i stand til at vurdere Telestyrelsens afgørelser og formentlig kun vil skulle træffe afgørelse i et mindre antal sager, er det fundet uhensigtsmæssigt at anvende ressourcer hertil.

Til § 22

Forskningsministeren bemyndiges til at fastsætte regler om, at statens udgifter i forbindelse med Telestyrelsens tilsyn afholdes af de nøglecentre, der udsteder kvalificerede certifikater.

Fordelingen af disse udgifter på de bidragspligtige nøglecentre tilsigtes foretaget ud fra en beregning af de ressourcer, som Telestyrelsen har anvendt til at føre tilsyn med det enkelte nøglecenter.

I medfør af stk. 2 gives der hjemmel til, at skyldige bidrag kan inddrives ved udpantning.

Til kapitel 10

Internationale forhold

Til § 23

Bestemmelsen implementerer direktivets artikel 7 og fastsætter de betingelser, som certifikater udstedt af et nøglecenter etableret i et tredjeland - det vil sige et land uden for EØS - skal opfylde for at kunne ligestilles retligt med et kvalificeret certifikat udstedt af et nøglecenter inden for EØS-området.

Det følger af § 11, at et nøglecenter etableret i Danmark, der indestår for kvalificerede certifikater udstedt af et nøglecenter fra et tredjeland, er ansvarlig for disse certifikater, for så vidt angår de typer af tab, der er omfattet af bestemmelsen, på samme måde som for de certifikater det danske nøglecenter selv har udstedt.

Til kapitel 11

Strafansvar

Til § 24

Bestemmelsen fastsætter, hvilke bestemmelser, der er strafbelagte at overtræde.

Stk. 2 sikrer, at der kan pålægges selskaber m.v. (juridiske personer) straffeansvar efter reglerne i straffelovens kapitel 5.

Til kapitel 12

Ikrafttrædelse m.v.

Til §§ 25 – 26

Loven træder i kraft den 1. oktober 2000. Herved gives der mulighed for, at der kan udarbejdes nærmere regler, der udmønter bemyndigelserne i loven til Forskningsministeren og Telestyrelsen.

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 signaturprodukter 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

---

(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).

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 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;

---

(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

(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[7];

(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

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

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.

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. Certificeringstje-

nesteudbyderen 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[8].

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[9].

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.

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

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

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.

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
N. FONTAINE
Formand

På Rådets vegne
S. HASSI
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.

Til lovforslag nr. L 229. Skriftlig fremsættelse (22. marts 2000)

Forskningsministeren (Birte Weiss):

Herved tillader jeg mig for Folketinget at fremsætte:

Forslag til lov om elektroniske signaturer.
(Lovforslag nr. L 229).

Lovforslaget indeholder regler for nøglecentre, der udsteder certifikater til elektroniske signaturer, og regler for visse elektroniske signaturer.

Sigtet med forslaget er at fremme en sikker og effektiv anvendelse af elektronisk kommunikation ved at fastsætte en række krav til de nøglecentre i Danmark, der ønsker at udstede certifikater til elektroniske signaturer til offentligheden under betegnelsen "kvalificerede certifikater". Der er to elementer i denne regulering: En række tekniske og sikkerhedsmæssige minimumskrav til nøglecentrenes virksomhed og en skærpet ansvarsregulering i forhold til de omhandlede nøglecentre.

Ved at benytte en elektronisk signatur og et certifikat hertil, kan der skabes sikkerhed for, at en elektronisk meddelelse stammer fra den, som er angivet som underskriver af meddelelsen, og for at meddelelsens indhold ikke efterfølgende er blevet ændret.

Elektroniske signaturer kan således medvirke til at gøre det mere sikkert og attraktivt for både forbrugere, private virksomheder og offentlige myndigheder at bruge Internetttet til for eksempel elektronisk handel, udveksling af oplysninger og levering af serviceydelser m.v. Eksemplerne rækker fra erhvervsvirksomheders elektroniske aftaler om køb af varer og tjenesteydelser og kontakt til underleverandører, til forbrugernes køb af alle former for forbrugsvarer over nettet. Også borgeres og virksomheders kontakt med offentlige myndigheder i forbindelse med udstedelse af tilladelser, indbetaling af skat og afgifter, og andre former for juridisk bindende kommunikation med det offentlige, er en mulighed.

Med sigte på at skabe et marked for certifikater med et tilstrækkeligt sikkerhedsniveau, indeholder lovforslaget en række krav vedrørende sikkerhed, organisation, økonomiske ressourcer, revision m.v., som skal opfyldes af de nøglecentre, som ønsker at benytte betegnelsen "kvalificerede certifikater". Der etableres samtidig et statsligt tilsyn med disse virksomheder i Telestyrelsen. Tilsynet skal foregå i et samarbejde med en systemrevisor, som skal rapportere til tilsynsmyndigheden vedrørende nøglecentrets systemer og dets overholdelse af reglerne i loven. Også nøglecentrets ledelse skal indestå for oplysningerne.

Et andet element i reguleringen af kvalificerede certifikater er, som nævnt ovenfor, skærpede regler om de omhandlede nøglecentres erstatningsansvar overfor indehavere og modtagere af kvalificerede certifikater i form af et præsumptionsansvar (omvendt bevisbyrde).

Desuden indeholder lovforslaget minimumskrav til de konkrete digital signatur produkter (signaturgenereringssystemerne), som anvendes til at afgive en elektronisk underskrift og til at opbevare denne. Minimumskravene skal overholdes, hvis en producent ønsker at kunne anvende betegnelsen et "sikkert signaturgenereringssystem" om sit produkt.

Endelig indeholder forslaget en bestemmelse, der sikrer elektroniske signaturer, som opfylder nærmere beskrevne kvalitetskrav, retsvirkninger i de tilfælde, hvor der i den øvrige lovgivning findes krav om anvendelse af en underskrift i forbindelse med elektronisk kommunikation. Bestemmelsen udgør sammen med en række definitionsbestemmelser byggestenene for regulering af retsvirkninger i de forskellige dele af særlovgivningen.

For at tage højde for den hurtige udvikling inden for informationsteknologien er forslaget søgt udformet sådan, at det er neutralt i relation til de konkrete teknologier, som anvendes af nøglecentrene.

Forslaget gennemfører Europa-Parlamentets og Rådets direktiv 1999/93/EF om en fællesskabsramme for elektroniske signaturer og skaber derved grundlag for skabelsen af et Indre Marked for tjenester vedrørende elektroniske signaturer og certifikater til disse.

Idet jeg i øvrigt henviser til lovforslaget med bemærkninger, tillader jeg mig at anbefale lovforslaget til velvillig behandling i det høje Ting.