BILAG 2

Lov om elektroniske signaturer[1)]

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

Folketinget har vedtaget og Vi ved Vort samtykke stadfæstet følgende lov:

Kapitel 1

Formål og anvendelsesområde

§ 1. Lovens formål er at fremme en sikker og effektiv anvendelse af elektronisk kommunikation gennem fastsættelse af krav til visse elektroniske signaturer og til nøglecentre, der udsteder certifikater til elektroniske signaturer.

§ 2. Loven finder anvendelse på nøglecentre etableret i Danmark, der udsteder kvalificerede certifikater til offentligheden, jf. dog § 12.

Stk. 2. Loven finder desuden anvendelse på efterprøvelse af, at signaturgenereringssystemer overholder de opstillede krav til sikre signaturgenereringssystemer.

Kapitel 2

Definitioner

§ 3. I denne lov forstås ved:

1) Elektronisk signatur: Data i elektronisk form, der knyttes til andre elektroniske data ved hjælp af et signaturgenereringssystem, og som anvendes til at kontrollere, at disse data stammer fra den person, der er angivet som underskriver, og at de ikke er blevet ændret.
2) Avanceret elektronisk signatur: En elektronisk signatur, der
   a) entydigt er knyttet til underskriveren,
   b) gør det muligt at identificere underskriveren,
   c) skabes med midler, som kun underskriveren har kontrol over, og som
   d) er knyttet til de data, den vedrører på en sådan måde, at enhver efterfølgende ændring af disse data kan opdages.
3) Underskriver: En fysisk person, der besidder et signaturgenereringssystem og handler på egne vegne eller på vegne af en anden fysisk eller juridisk person.
4) Signaturgenereringsdata: Unikke data, som for eksempel en kode eller en privat krypteringsnøgle, som anvendes til at fremstille en elektronisk signatur.
5) Signaturgenereringssystem: Et software- eller hardwarebaseret system til behandling og opbevaring af signaturgenereringsdata.
6) Signaturverificeringsdata: Unikke data, som for eksempel en kode eller en offentlig krypteringsnøgle, som anvendes til at verificere en elektronisk signatur.
7) Signaturverificeringssystem: Et software- eller hardwarebaseret system til behandling af signaturverificeringsdata.
8) Certifikat: En elektronisk attest, som knytter bestemte signaturverificeringsdata til underskriveren og bekræfter dennes identitet.
9) Nøglecenter: En fysisk eller juridisk person, der udsteder certifikater.

[1)] Loven indeholder bestemmelser, der gennemfører Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EF-Tidende 2000 nr. L 13, s. 12).

Forskningsmin., j.nr. ITR 4843

AF000162

J. H. Schultz Grafisk A/S

Kapitel 3

Kvalificerede certifikater

§ 4. Betegnelsen kvalificerede certifikater eller betegnelser, der er egnede til at fremkalde det indtryk, at der er tale om kvalificerede certifikater, må kun anvendes om certifikater, der opfylder de i stk. 2 og 3 nævnte krav, og som udstedes af et nøglecenter, der opfylder bestemmelserne i kapitel 4 samt regler fastsat i medfør heraf.

Stk. 2. Et kvalificeret certifikat skal indeholde:

1) En angivelse af, at certifikatet er udstedt som et kvalificeret certifikat.
2) Nøglecentrets navn og hjemsted.
3) Underskriverens navn eller pseudonym med angivelse af, at der er tale om et pseudonym.
4) Eventuelle yderligere oplysninger om underskriveren, for så vidt det er nødvendigt for anvendelsen af certifikatet, herunder oplysninger, der sikrer en entydig identifikation af underskriveren.
5) Certifikatets gyldighedsperiode.
6) En tydelig angivelse af eventuelle begrænsninger i certifikatets anvendelsesområde (formålsbegrænsninger).
7) En tydelig angivelse af eventuelle begrænsninger med hensyn til de transaktionsbeløb, certifikatet kan anvendes til (beløbsbegrænsninger).
8) Certifikatets identifikationskode.
9) De signaturverificeringsdata, der svarer til de signaturgenereringsdata, som var under underskriverens kontrol på udstedelsestidspunktet.

Stk. 3. Et kvalificeret certifikat skal være underskrevet med nøglecentrets avancerede elektroniske signatur.

Kapitel 4

Krav til nøglecentres virksomhed

§ 5. Et nøglecenter skal træffe de foranstaltninger, som er nødvendige for et sikkert, pålideligt og velfungerende udbud af kvalificerede certifikater. Nøglecentret skal herunder

1) anvende betryggende administrative og ledelsesmæssige procedurer, som overholder anerkendte standarder,
2) beskæftige personale med den fornødne ekspertise, erfaring og kvalifikationer, herunder personale med sagkundskab inden for elektronisk signaturteknologi og indgående kendskab til korrekte sikkerhedsprocedurer i forbindelse hermed,
3) anvende pålidelige systemer og produkter, som er beskyttet imod uautoriserede ændringer, og som sikrer den tekniske og kryptografiske sikkerhed af de processer, som disse systemer og produkter understøtter,
4) træffe foranstaltninger mod eventuelle muligheder for forfalskning af certifikaterne og
5) til stadighed have tilstrækkelige økonomiske ressourcer til at drive virksomhed i overensstemmelse med bestemmelserne i denne lov, herunder til at opfylde erstatningsmæssige forpligtelser i henhold til loven.

Stk. 2. Nøglecentre, der udsteder kvalificerede certifikater, skal vælge en ekstern statsautoriseret revisor til varetagelse af systemrevisionen i nøglecentret. Telestyrelsen kan i særlige tilfælde dispensere fra kravet om, at systemrevisor skal være statsautoriseret revisor.

Stk. 3. Forskningsministeren fastsætter nærmere regler om kravene i stk. 1.

§ 6. Nøglecentre skal fastsætte og anvende betryggende procedurer til at kontrollere identiteten og andre forhold vedrørende underskriveren forud for udstedelsen af certifikatet.

Stk. 2. Oplysninger om procedurerne som nævnt i stk. 1 skal være offentligt tilgængelige.

Stk. 3. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1 og 2.

§ 7. Et nøglecenter skal ved udstedelse af et kvalificeret certifikat sikre, at underskriveren på tidspunktet for udstedelsen er i besiddelse af de signaturgenereringsdata, som korresponderer med de signaturverificeringsdata, der er indeholdt i certifikatet.

Stk. 2. Ved udstedelse af kvalificerede certifikater, hvor det er nøglecentret, der leverer signaturgenereringsdata og signaturverificeringsdata, må der kun anvendes signaturgenereringsdata og signaturverificeringsdata, som hører sammen på en unik måde. Nøglecentret skal sikre signaturgenereringsdataenes fortrolighed under genereringsprocessen.

Stk. 3. Et nøglecenter skal fastlægge procedurer for udstedelse af certifikater, der gør det muligt at fastslå dato og tidspunkt for udstedelsen.

§ 8. Ved indgåelse af en aftale om udstedelse af et kvalificeret certifikat skal nøglecentret skriftligt oplyse underskriveren om:

1) Vilkårene for anvendelsen af certifikatet, herunder eventuelle formåls- eller beløbsbegrænsninger.
2) Eventuelle krav til underskriverens opbevaring og beskyttelse af signaturgenereringsdataene.
3) Underskriverens omkostninger ved erhvervelse og anvendelse af certifikatet og brug af nøglecentrets øvrige tjenester.
4) Hvorvidt nøglecentret er tilknyttet en frivillig akkrediteringsordning.
5) Procedurer for behandling af klager og bilæggelse af tvister.

Stk. 2. Kontraktsvilkårene kan afgives elektronisk, forudsat at det sker i en for modtageren umiddelbart læsbar form.

Stk. 3. De relevante dele af de i stk. 1 nævnte oplysninger skal på anmodning stilles til rådighed for tredjemand, der forlader sig på et kvalificeret certifikat.

Stk. 4. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1-3.

§ 9. Nøglecentre skal sørge for en hurtig og sikker katalog- og tilbagekaldelsestjeneste, som giver mulighed for, at det kan undersøges, om et kvalificeret certifikat er spærret, hvilken gyldighedsperiode certifikatet har, og om certifikatet indeholder formåls- eller beløbsbegrænsninger.

Stk. 2. Et nøglecenter skal spærre et certifikat straks efter at have modtaget anmodning fra underskriveren herom, eller hvis forholdene i øvrigt tilsiger dette.

Stk. 3. Oplysninger efter stk. 1 skal være umiddelbart tilgængelige.

Stk. 4. Et kvalificeret certifikat må kun gøres offentligt tilgængeligt, hvis underskriveren har givet samtykke hertil.

Stk. 5. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1-3.

§ 10. Et nøglecenter skal registrere og opbevare alle relevante oplysninger om certifikaterne i en rimelig periode, dog mindst seks år.

Stk. 2. Et nøglecenter skal benytte pålidelige systemer til opbevaring af certifikater i verificerbar form.

Stk. 3. Nøglecentre må ikke opbevare eller kopiere de personers signaturgenereringsdata, som nøglecentret gennem udstedelsen af certifikater måtte have fået kendskab til.

Stk. 4. Forskningsministeren kan fastsætte nærmere regler om kravene i stk. 1 og 2.

Kapitel 5

Erstatningsansvar

§ 11. Nøglecentre, der udsteder kvalificerede certifikater til offentligheden, eller som over for offentligheden indestår for sådanne certifikater udstedt af et andet nøglecenter, er ansvarlig for tab hos den, der med rimelighed forlader sig på certifikatet, såfremt tabet skyldes,

1) at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet,
2) at certifikatet ikke indeholder alle oplysninger som krævet i henhold til § 4,
3) manglende spærring af certifikatet, jf. § 9, stk. 2,
4) manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. § 9, stk. 1 og 3, eller
5) tilsidesættelse af § 7.

Stk. 2. Et nøglecenter pådrager sig erstatningsansvar efter stk. 1, medmindre nøglecentret kan godtgøre, at nøglecentret ikke har handlet uagtsomt eller forsætligt.

Stk. 3. Et nøglecenter er ikke ansvarlig for

1) tab opstået som følge af anvendelse af et kvalificeret certifikat uden for de formålsbegrænsninger, som gælder for certifikatet, eller for
2) tab opstået som følge af en overskridelse af de beløbsbegrænsninger, som gælder for certifikatet,

forudsat at de pågældende begrænsninger tydeligt fremgår af certifikatet, jf. § 4, og på forespørgsel oplyses, jf. 9, stk. 1 og 3.

Stk. 4. Stk. 1-3 kan ikke ved forudgående aftale fraviges til skade for skadelidte.

Stk. 5. Stk. 1-3 finder ikke anvendelse, i det omfang tabet dækkes efter lov om visse betalingsmidler.

Kapitel 6

Supplerende krav til behandling af personoplysninger

§ 12. Et nøglecenter må kun indsamle personoplysninger i forbindelse med nøglecentervirksomheden direkte fra den registrerede eller med den registreredes udtrykkelige samtykke og kun i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat.

Stk. 2. Personoplysninger indsamlet i medfør af stk. 1 må ikke behandles eller videregives til andet formål end nævnt i stk. 1 uden den registreredes udtrykkelige samtykke hertil.

Kapitel 7

Elektronisk signatur og formkrav

§ 13. Bestemmelser i lovgivningen, hvorefter elektroniske meddelelser skal være forsynet med signatur, skal anses for opfyldt, hvis meddelelsen er forsynet med en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat, og som er fremstillet ved brug af et sikkert signaturgenereringssystem. Ved elektroniske meddelelser til og fra en offentlig myndighed gælder dette dog kun, såfremt andet ikke følger af lov eller bestemmelser fastsat i medfør af lov.

Kapitel 8

Sikre signaturgenereringssystemer

§ 14. Ved et sikkert signaturgenereringssystem forstås et signaturgenereringssystem, der ved hjælp af procedurer og tekniske midler sikrer, at signaturgenereringsdata, der anvendes til at skabe en elektronisk signatur,

1) i praksis kun kan fremtræde en gang,
2) med rimelig sikkerhed forbliver hemmelige og ikke kan udledes,
3) er beskyttet mod forfalskning og
4) på pålidelig vis kan beskyttes af underskriveren mod andres uretmæssige brug.

Stk. 2. Et sikkert signaturgenereringssystem må ikke indrettes således, at det ændrer de data, som en elektronisk signatur knyttes til, eller hindrer, at disse data forevises for underskriveren forud for signeringen.

Stk. 3. De i stk. 1 og 2 nævnte krav skal anses for opfyldt, såfremt et signaturgenereringssystem overholder almindeligt anerkendte standarder for sådanne systemer, som Kommissionen har fastsat og offentliggjort i EF-Tidende i overensstemmelse med proceduren i artikel 9 i Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer.

§ 15. Forskningsministeren udpeger et eller flere egnede organer eller myndigheder, som kan medvirke til at efterprøve, om signaturgenereringssystemer opfylder kravene til sikre signaturgenereringssystemer, jf. § 14, stk. 1 og 2, og fastsætter nærmere regler om procedurerne for denne efterprøvelse samt om betaling af gebyr for efterprøvelsen.

Stk. 2. Et signaturgenereringssystem, der betegnes som et sikkert signaturgenereringssystem, må først markedsføres eller anvendes til at fremstille avancerede elektroniske signaturer, der er baseret på et kvalificeret certifikat, når det er blevet efterprøvet, jf. stk. 1.

Stk. 3. Med en efterprøvelse efter stk. 1 ligestilles en efterprøvelse af et sikkert signaturgenereringssystem foretaget af et organ eller en myndighed i et andet land inden for Det Europæiske Økonomiske Samarbejde (EØS).

Kapitel 9

Tilsyn

§ 16. Nøglecentre skal senest samtidig med, at udstedelse af kvalificerede certifikater påbegyndes, foretage anmeldelse til Telestyrelsen.

Stk. 2. Anmeldelsen skal indeholde oplysning om

1) nøglecentrets navn og hjemsted,
2) selskabsform, såfremt nøglecentret drives som selskab,
3) nøglecentrets ledelse og systemrevisor.

Stk. 3. Ændringer i forhold, der er anmeldt i henhold til stk. 2, skal anmeldes inden 8 dage efter, at ændringen er sket.

Stk. 4. Telestyrelsen kan fastsætte nærmere regler om, hvilke yderligere oplysninger anmeldelsen skal indeholde.

§ 17. Nøglecentret skal samtidig med anmeldelse efter § 16 indsende en rapport til Telestyrelsen.

Stk. 2. Rapporten skal indeholde

1) en beskrivelse af nøglecentrets virksomhed og systemer,
2) en erklæring fra nøglecentrets ledelse om, hvorvidt nøglecentrets samlede data-, system- og driftssikkerhed må anses for betryggende og i overensstemmelse med denne lovs regler samt regler fastsat i medfør heraf, og
3) en erklæring fra systemrevisor, jf. § 5, stk. 2, om, hvorvidt nøglecentrets samlede data-, system- og driftssikkerhed efter systemrevisors opfattelse må anses for betryggende og i overensstemmelse med denne lovs regler samt regler fastsat i medfør heraf.

Stk. 3. Nøglecentret skal årligt udarbejde en opdateret rapport. Telestyrelsen fastsætter en

frist for, hvornår rapporten senest skal indsendes til Telestyrelsen.

Stk. 4. Telestyrelsen kan fastsætte nærmere regler vedrørende indholdet af nøglecentrets rapporter samt om systemrevisionens gennemførelse i nøglecentre.

§ 18. Telestyrelsen påser overholdelsen af denne lov og bestemmelser udstedt i medfør af loven.

Stk. 2. Telestyrelsen kan påbyde et nøglecenter at

1) foretage anmeldelse til Telestyrelsen, jf. § 16,
2) indsende rapporter til Telestyrelsen, jf. § 17,
3) bringe forhold vedrørende nøglecentrets virksomhed i overensstemmelse med loven eller bestemmelser udstedt i medfør af loven.

Stk. 3. Telestyrelsen fastsætter en tidsfrist for opfyldelse af påbud efter stk. 2.

Stk. 4. Telestyrelsen kan pålægge et nøglecenter tvangsbøder med henblik på at gennemtvinge påbud efter stk. 2, § 19, stk. 1, eller § 20.

Stk. 5. Telestyrelsen kan kræve, at der gennemføres en ekstraordinær systemrevision af et nøglecenter. Telestyrelsen udpeger den systemrevisor, som skal udføre den ekstraordinære systemrevision. Nøglecentret kan pålægges at betale for den ekstraordinære systemrevisions udførelse.

Stk. 6. Telestyrelsen kan fratage et nøglecenter retten til at anvende betegnelsen kvalificerede certifikater, jf. § 4, hvis nøglecentret

1) trods pålæg af tvangsbøder undlader at efterkomme Telestyrelsens påbud efter stk. 2, § 19, stk. 1, eller § 20,
2) groft eller i gentagne tilfælde har overtrådt lovens regler eller regler fastsat i medfør heraf eller
3) anmelder betalingsstandsning eller kommer under konkurs.

Stk. 7. Telestyrelsens afgørelse efter stk. 6 kan af nøglecentret forlanges indbragt for domstolene. Anmodning herom skal være modtaget i Telestyrelsen senest 4 uger efter, at afgørelsen er blevet meddelt nøglecentret. Telestyrelsen anlægger sag mod nøglecentret efter reglerne i den borgerlige retsplejes former.

Stk. 8. Anmodning om sagsanlæg har ikke opsættende virkning, men retten kan ved kendelse bestemme, at det pågældende nøglecenter under sagens behandling skal have adgang til at udstede kvalificerede certifikater. Ankes en dom, hvorved fratagelsen af adgangen til at udstede kvalificerede certifikater ikke findes lovlig, kan den ret, der har afsagt dommen, eller den ret, hvortil sagen er indbragt, bestemme, at nøglecentret ikke må udstede kvalificerede certifikater under ankesagens behandling.

§ 19. Telestyrelsen kan af nøglecentre kræve meddelt alle oplysninger, som findes nødvendige for tilsynet efter § 18, herunder til afgørelse af, om en fysisk eller juridisk person er omfattet af dette tilsyn.

Stk. 2. Nøglecentret og systemrevisor skal straks meddele Telestyrelsen oplysning om forhold, der er af afgørende betydning for nøglecentrets fortsatte virksomhed.

§ 20. Telestyrelsen kan pålægge nøglecentret inden for en fastsat frist at vælge en ny systemrevisor, jf. § 5, stk. 2, såfremt den fungerende systemrevisor findes åbenbart uegnet til sit hverv.

Stk. 2. Telestyrelsen kan pålægge systemrevisor at give oplysninger om nøglecentrets forhold uden accept fra nøglecentret.

Stk. 3. Ved revisorskifte skal nøglecentret og den eller de fratrådte systemrevisorer hver især give Telestyrelsen en redegørelse. Telestyrelsen kan give påbud om at efterkomme 1. pkt.

§ 21. Telestyrelsens afgørelser efter denne lov eller bestemmelser, der er fastsat i medfør heraf, kan ikke indbringes for anden administrativ myndighed.

§ 22. Forskningsministeren kan fastsætte regler om, at udgifterne ved Telestyrelsens tilsyn afholdes af de nøglecentre, der udsteder kvalificerede certifikater.

Kapitel 10

Internationale forhold

§ 23. Kvalificerede certifikater udstedt af et nøglecenter etableret i et land uden for Det Europæiske Økonomiske Samarbejde (EØS), skal anerkendes på samme måde som kvalificerede certifikater udstedt af nøglecentre etableret i et land inden for Det Europæiske Økonomiske Samarbejde (EØS) såfremt

1) nøglecentret opfylder kravene i denne lov og er tilsluttet en frivillig akkrediteringsordning i en medlemsstat eller

2) et nøglecenter etableret i en medlemsstat, der opfylder kravene i denne lov, indestår for certifikater udstedt af det pågældende nøglecenter eller
3) certifikatet eller nøglecentret er anerkendt i henhold til en bilateral eller multilateral aftale mellem Fællesskabet og tredjelande eller internationale organisationer.

Kapitel 11

Strafansvar

§ 24. Medmindre strengere straf er forskyldt efter anden lovgivning, straffes med bøde den, der
1) overtræder § 9, stk. 4, § 10, stk. 3, § 12 eller § 15, stk. 2,
2) afgiver urigtige eller vildledende oplysninger til Telestyrelsen eller
3) overtræder påbud eller afgørelser fra Telestyrelsen i medfør af § 18, stk. 2 og 6, og § 19, stk. 1.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Stk. 3. Forældelsesfristen for strafansvar efter stk. 1 og 2 er 5 år.

Kapitel 12

Ikrafttrædelse m.v.

§ 25. Loven træder i kraft den 1. oktober 2000.

§ 26. Loven gælder ikke for Grønland og Færøerne, men kan ved kongelig anordning sættes i kraft for disse landsdele med de afvigelser, som de særlige grønlandske og færøske forhold tilsiger.

Givet på Christiansborg Slot, den 31. maj 2000

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Birte Weiss