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-