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).