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