

troniske signaturprodukter, der overholder direktivets bestemmelser. Dette krav er gennemført i lovens § 13, hvorefter bestemmelser i lovgivning, der kræver, at en elektronisk meddelelse er forsynet med signatur, skal anses for opfyldt, hvis meddelelsen er forsynet med en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat.

Ministeriet for Videnskab, Teknologi og Udvikling fastsatte i 2002 den såkaldte OCES-standard (Offentlige Certifikater til Elektroniske Services) for at skabe et større marked for digitale signaturer på et højt sikkerhedsniveau, idet udbredelsen af kvalificerede certifikater var meget begrænset.

OCES-standardens er ikke omfattet af lov om elektroniske signaturer, men standarden afspejler i videst muligt omfang kravene i lov om elektroniske signaturer. OCES-certifikater adskiller sig således ikke rent teknisk fra kvalificerede certifikater, og de giver dermed også sikkerhed for identiteten på certifikatindehaveren (autenticitet) samt for, at et signeret dokument ikke kan ændres, uden at det senere vil kunne konstateres (integritet).

Fra 2003 har der via en statslig aftale med TDC A/S været mulighed for, at alle borgere gratis kan erhverve og over for offentlige myndigheder bruge en digital OCES-signatur. Denne aftale udløber i juni 2008. En OCES-signatur kan anskaffes ved på TDC's hjemmeside at udfylde en elektronisk ansøgningsblanket.

Ved certifikatudstedelsen foretages en række kontroller, der skal sikre, at certifikatet udstedes til den rette. På baggrund af det indtastede personnummer og postnummer indhentes ansøgerens navn og adresse i Det Centrale Personregister, og den pågældendes alder kontrolleres. Den angivne e-postadresse benyttes til fremsendelse af installationsvejledning og installationslink til certifikatet. I tillæg til disse kontroller sendes et postbesørgt brev til ansøgeren på dennes folkeregisteradresse med en pinkode, der skal benyttes, når certifikatet installeres. Ved udstedelse af en OCES-signatur benyttes således to forskellige kommunikationskanaler, der skal sikre, at det er den rette person, der erhverver signaturen, og at signaturen kun kan benyttes af den person, som den er udstedt til.

Ved bestilling af virksomheds- og medarbejdercertifikater skal der angives oplysninger om virksomhedens CVR-nummer og navn på en tegningsberettiget person fra virksomhedens ledelse. Udstedelse af virksomhedscertifikater forudsætter endvidere angivelse af navn og e-postadresse på en kontaktperson. Ved udstedelse af medarbejdercertifikater skal opgives navn på en person, som skal være ansvarlig i forbin-

delse med udstedelsen af de enkelte medarbejdercertifikater.

Der er også etableret alternative muligheder for at få udstedt en OCES-signatur. Personer med navne- og adressebeskyttelse kan således få udleveret brevet med pinkoden hos bopælskommunen efter at have identificeret sig med billedlegitimation i form af sygesikringsbevis og pas eller dansk kørekort, og danske, der har bopæl i udlandet, kan afhente pinkoden personligt enten hos Københavns Kommune eller en dansk repræsentation i udlandet efter at have identificeret sig med dansk pas.

Der henvises i øvrigt til betænkningen side 108 ff.

4.2.2. Lovforslagets udformning

Det er udvalgets opfattelse, at digitale signaturer vil være egnede til at erstatte traditionelle underskrifter på tinglysningsdokumenter, idet digitale signaturer giver en høj grad af sikkerhed for identiteten på underskriveren af et digitalt dokument og sikrer, at indholdet af dokumentet ikke kan ændres efter signeringen, uden at det senere vil kunne konstateres.

Reglerne om retsvirkningerne af underskrifter er teknologineutrale, og det er således muligt at gøre brug af digitale signaturer, uden at det er nødvendigt at indføre særlige regler.

Udvalget anbefaler på den baggrund, at der i tinglysningsloven indsættes en bestemmelse, hvorefter digitale dokumenter, der anmeldes til tinglysning, skal være forsynet med udstederens digitale signatur.

For så vidt angår de tekniske krav, der stilles til digitale signaturer, foreslår udvalget en bemyndigelsesbestemmelse, hvorefter justitsministeren efter forhandling med ministeren for videnskab, teknologi og udvikling kan fastsætte nærmere regler herom. Det vil gøre det muligt at justere kravene til digitale signaturer, såfremt den teknologiske udvikling nødvendiggør det.

Udvalget anbefaler i den forbindelse, at den digitale signatur som udgangspunkt bør baseres på OCES-standardens eller på digitale signaturer med et sikkerhedsniveau, der som minimum er på niveau med OCES, og som er teknisk kompatible med OCES. Baggrunden for, at udvalget ikke anbefaler en egentlig kvalificeret signatur er for det første, at OCES-standardens i videst mulig omfang afspejler kravene i lov om elektroniske signaturer, og at OCES-signaturer således ikke rent teknisk adskiller sig fra kvalificerede signaturer. Det betyder, at en OCES-signatur på samme måde som et kvalificeret certifikat giver en høj grad af sikkerhed for identiteten på underskriveren af et digitalt dokument og sikrer, at indholdet af doku-