til bindende juridiske dispositioner forudsætter, at der kan kommunikeres med sikkerhed for afsenders identitet og for, at indholdet ikke er blevet ændret.

Formålet med direktivet er at lette anvendelsen af elektroniske signaturer samt at medvirke til deres juridiske anerkendelse. Direktivet tilvejebringer en ramme for elektroniske signaturer og de tilknyttede certificeringstjenester m.v. med henblik på at sikre det indre marked med hensyn til elektroniske signaturer.

Anvendelsesområde

Direktivets anvendelsesområde er elektroniske signaturer. Direktivet opererer med en meget bred definition af en elektronisk signatur, idet det definerer en elektronisk signatur som data i elektronisk form, der er vedhæftet eller logisk tilknyttet andre elektroniske data, og som anvendes til autentifikation.

Samtidig opererer direktivet med begrebet »en avanceret elektronisk signatur«, som er en elektronisk signatur, der skal 1) være entydigt knyttet til underskriveren, 2) kunne identificere underskriveren, 3) tilvejebringes med midler, som underskriveren kan bevare den fulde kontrol med, og 4) være knyttet til de data, som den vedrører på en sådan måde, at enhver efterfølgende ændring i disse data kan opdages.

Sondringen mellem en elektronisk signatur og en avanceret elektronisk signatur har betydning for direktivets bestemmelser om retsvirkninger (se nedenfor).

Det er overladt til medlemsstaterne at bestemme på hvilke retsområder, man i lovgivningen vil tillade brugen af elektronisk kommunikation og elektroniske signaturer.

Elektronisk kommunikation i lukkede systemer er ikke omfattet af direktivets generelle regulering. I de tilfælde, hvor parterne på forhånd har indgået en kommunikationsaftale, har denne aftale forrang. Elektroniske signaturer afgivet inden for sådanne systemer må dog ikke udelukkes fra at opnå de retsvirkninger, der fastlægges i direktivet.

Fastlæggelse af en række krav til nøglecentrene og elektroniske signaturer

Med henblik på at skabe et marked for elektroniske signaturer af høj kvalitet og med samme sikkerhedsniveau i hele EU, er der i direktivet fastlagt en række krav til udbyderne (nøglecentre er i direktivet kaldet certificeringstjenesteudbydere) af såkaldte kvalificerede certifikater til elektroniske signaturer. I den efterfølgende gennemgang af direktivet bruges direktivets betegnelse for disse certifikater.

Nøglecentre er ifølge direktivet en person eller et organ, der udsteder certifikater eller leverer andre tjenesteydelser i forbindelse med elektronisk signatur til offentligheden. Dette betyder bl.a., at tjenesteudbydere, som ikke tilbyder certificering, alligevel bliver omfattet af visse af direktivets regler, hvis de tilbyder »tilknyttede« tjenester, f.eks. tidsstempling af elektronisk post. Direktivet angiver i bilag II en række grundlæggende krav til sådanne udbydere.

Et certifikat til en elektronisk signatur er ifølge direktivet en digital attestering, som knytter et signaturverificeringssystem til en person og bekræfter denne persons identitet.

Et kvalificeret certifikat er ifølge direktivet et certifikat, der opfylder kravene til kvalificerede certifikater i bilag I, og som udstedes af et nøglecenter, der opfylder kravene i bilag II.

Direktivet fastlægger regler for nøglecentrets ansvar over for »enhver person, som med rimelighed forlader sig på certifikatet«. Europa-Kommissionen har præciseret, at denne personkreds også omfatter underskriveren.

Ansvarsreglerne omfatter alene de tilfælde, hvor et nøglecenter har udstedt et certifikat som et kvalificeret certifikat, eller hvor udbyderen indestår for en anden udbyders certifikat.

Nøglecentret skal være ansvarlig for 1) korrektheden af alle oplysningerne i certifikatet regnet fra udstedelsesdagen, 2) sikkerheden for, at den i det kvalificerede certifikat identificerede person på udstedelsesdagen var i besiddelse af de signaturgenereringsdata (den private nøgle), der svarer til det i certifikatet indeholdte eller omhandlede signaturverificeringsdata (den offentlige nøgle) og 3) sikkerheden for, at signaturgenereringsdataene og signaturverificeringsdataene fungerer komplementært med hinanden i de tilfælde, hvor det er nøglecentret, der genererer de to systemer.

Ansvarsreglerne skal bygge på et princip om, at nøglecentret i det mindste skal have handlet uagtsomt for at ifalde erstatningsansvar i de tre ovennævnte tilfælde. Ifølge direktivet er bevisbyrden for at bevise, at der ikke er handlet uagtsomt, pålagt nøglecentret.

Medlemsstaterne skal herudover sikre, at nøglecentre, der udsteder kvalificerede certifikater, er erstatningsansvarlige for tab, der opstår som følge af manglende spærring af certifikatet, medmindre nøglecentret kan bevise, at der ikke er handlet uagtsomt.

Direktivet indeholder ingen regulering af ansvarsforholdet mellem underskriver og modtager af en elektronisk signatur.

Medlemsstaterne skal sikre, at certificeringstjenesteudbydere samt nationale akkrediterings- og tilsynsorganer opfylder det generelle EF-direktiv 97/46/EF