

Inden for erhvervslivet ser man især en stigende udnyttelse af teknologien i forbindelse med elektronisk handel, dvs. aftaleindgåelse og betalingsoverførsel via elektroniske medier, herunder til automatisk udveksling af forretningsdokumenter som f.eks. ordrer og fakturaer (eksempelvis via EDI - Electronic Data Interchange).

Elektronisk udveksling af data mellem erhvervsvirksomheder foregår i dag i en række situationer i såkaldte lukkede systemer, hvor parterne på forhånd har indgået aftale om sikkerhedsaspekter, udvekslingsformater m.v. De fælles standarder for elektronisk dataudveksling er et eksempel på et sæt spilleregler, der kan anvendes i sådanne lukkede systemer. Handler man ofte med hinanden, så kan det give mening at indgå sådanne rammeaftaler. Men den løsningsmodel er ikke anvendelig, hvis ønsket er, at principielt alle virksomheder, myndigheder og privatpersoner på nettet indbyrdes skal kunne foretage juridisk bindende dispositioner, f.eks. foretage en enkelt bestilling eller indgå en enkeltstående aftale, uanset om de tidligere har været i kontakt med hinanden eller ej.

Der er derfor en stigende efterspørgsel fra erhvervs-side efter en regulering, der kan sikre betryggende rammer for, at man kan foretage juridisk bindende dispositioner via åbne net som f.eks. Internettet uden først at skulle aftale med modtageren, hvordan man gør.

Det er imidlertid ikke kun dansk erhvervsliv, der er interesseret i elektronisk kommunikation. Også private borgere ønsker i stigende omfang at bruge Internettet i kommercielle sammenhænge, dvs. ved bestilling og køb af varer og tjenesteydelser.

I nogle situationer foregår den nævnte kommunikation allerede i dag helt uden brug af en elektronisk signatur. Dette gælder navnlig mindre omfattende dispositioner. Også i de situationer, hvor man ønsker at anvende en elektronisk signatur, er der forskel på den økonomiske risiko, som man løber, og de eventuelle tab der kan opstå m.v.

Tendensen er derfor også, at der udvikles en række elektronisk signaturer og tilhørende certifikater med et gradueret sikkerhedsniveau, som er skræddersyet til forskellige typer anvendelse.

Som borger er det derfor også sandsynligt, at man vil råde over forskellige digitale certifikater og signaturgenereringsdata til forskellige formål, herunder f.eks. til private »små-indkøb«, til kommunikation med det offentlige, eller i arbejdsammenhæng.

Det bør i vidt omfang overlades til markedet selv at sørge for, at der etableres nøglecentre, og at de løsninger, de udbyder, er tilstrækkelig sikre set i relation til

de situationer, hvori de tænkes anvendt. Når dette er udgangspunktet, skyldes det ikke mindst, at der fortsat er tale om et marked, som er inde i en rivende udvikling, og hvor en for intensiv offentlig regulering med stor sikkerhed vil hæmme og bremse produktudviklingen. Der vil desuden være stort behov for i givet fald at skulle opdatere denne regulering i takt med de seneste tekniske landvindinger.

Samtidig er der imidlertid tale om et nyt marked med produkter af en sådan teknisk kompleksitet, at det er særdeles vanskeligt for den enkelte private bruger at gennemskue, om man får et produkt med den fornødne sikkerhed.

Der findes på nuværende tidspunkt ingen regulering af virksomheder, der ønsker at udbyde certifikater og elektroniske signaturer.

##### *5. Lovreguleringens rolle i forhold til elektroniske signatur certifikater*

Lovforslagets primære sigte er at etablere en fleksibel tilsyns- og kontrolordning for nøglecentre, der ønsker at udbyde certifikater med betegnelsen kvalificerede certifikater, og i tilknytning hertil at regulere de pågældende nøglecentres erstatningsansvar overfor henholdsvis underskrivere og modtagere af kvalificerede certifikater.

Tilsynsordningen indebærer, at de omfattede nøglecentre løbende skal dokumentere, at deres virksomhed og de certifikater, de udsteder, overholder en række minimumskrav, der kan sikre et udbud af løsninger af fornøden kvalitet på det danske marked. De minimumskrav, der opstilles, vedrører punkt I-III i afsnit 2 ovenfor, dvs. sikring af kvaliteten af elektronisk signatur certifikaterne. Overholdes reglerne ikke, vil et nøglecenter kunne miste retten til at anvende det offentligt anerkendte begreb kvalificerede certifikater om deres certifikatprodukter.

For så vidt angår reguleringen af, i hvilket omfang nøglecenteret er ansvarlig i forbindelse med fejl, der opstår på grund af manglende overholdelse af de fastsatte minimumskrav (punkt IV i afsnit 2), er sigtet et culpaansvar med omvendt bevisbyrde.

Tilsynsordningen og ansvarsreguleringen vil ikke omfatte alle de certifikater, der udbydes, eller alle nøglecentre på markedet, men omfatter kun certifikater, som et nøglecenter vælger at benævne »kvalificerede certifikater«. Et nøglecenter vil som led i sin samlede virksomhed kunne udbyde både kvalificerede certifikater, og andre certifikater, herunder også certifikater, som i praksis opfylder lovens minimumskrav, men ikke benævnes kvalificerede certifikater.