denne modtages. I hvilket omfang sådanne faciliteter i praksis bliver udbudt, vil afhænge af efterspørgslen efter disse.

De omtalte nøglecentre vil oftest være kommercielle virksomheder, men også offentlige myndigheder, organiationer m.v., kan beslutte at etablere en nøglecenterfunktion. Der vil være forskel på, hvilke produkttyper, de enkelte nøglecentre udbyder. I den forbindelse vil nogle nøglecentre alene tilbyde udstedelse af certifikater, men vil forudsætte, at kunden anskaffer selve den elektroniske signatur (nøgleparret) andetsteds. Andre vil tilbyde begge dele. Nogle nøglecentre vil tilbyde tidsstemplingsfunktioner, men det vil formentlig ikke være alle nøglecentre, der tilbyder dette.

Der kan desuden være stor forskel på, hvordan nøglecentrene i praksis indrettes, herunder hvilke IT-løsninger og sikkerhedsprocedurer de anvender.

En virksomhed, der fungerer som nøglecenter, kan også udøve virksomhed på en række andre områder. Oplagte eksempler er virksomhed inden for kredit- og betalingskort-området, eller andre former for finansiel virksomhed, eller posthåndterings-virksomhed.

Det skal også understreges, at der er tale om et marked og nogle produkter, som først nu er under udvikling, og hvor den anvendte teknologi konstant ændrer sig. Det indebærer også, at beskrivelsen ovenfor af, hvordan en elektronisk signatur og elektroniske signatur certifikater fungerer i dag, alene er et øjebliksbillede, og ikke nødvendigvis vil have gyldighed om 1, 5 eller 10 år.

3. Bruger-interesser i forbindelse med anvendelse af elektronisk signatur og elektroniske signatur certifikater

Som nævnt indledningsvis er brugernes hovedinteresse, at man, når man kommunikerer gennem åbne digitale net som f.eks. Internettet, kan være sikker på, hvem det er, man kommunikerer med, og at indholdet af det kommunikerede ikke er blevet ændret undervejs eller efterfølgende. Det er som et element heri også afgørende efterfølgende at kunne dokumentere, hvad der er sket og hvornår.

Set fra en brugervinkel afhænger sikkerheden – både som afsender og modtager – af følgende forhold:

I) Hvordan og hvor omhyggeligt nøglecentret efterprøver underskriverens identitet forud for udstedelsen.

II) Hvor sikre og omhyggelige nøglecentrets procedurer er, når det gælder registrering af og information om, at et certifikat og en digital signatur er spærret eller udløbet, eller at certifikatet indeholder nogle anvendelsesbegrænsninger.

III) At certifikatets oplysninger om ovennævnte er korrekte og fyldestgørende.

IV) Hvordan nøglecentrets erstatningsansvar er i situationer, hvor der på et eller flere af de ovennævnte punkter er ukorrektheder i certifikatet eller på anden vis er sket fejl hos nøglecentret, og dette har ført til tab hos enten afsender eller modtager.

V) Kvaliteten af selve den elektroniske signatur, der anvendes i forbindelse med certifikatet, dvs. om det reelt er umuligt at bryde eller eftergøre signaturen, uden at det efterlader synlige spor.

Hvor betydningsfulde ovennævnte forhold er, afhænger af, hvad signaturen ønskes brugt til.

4. I hvilke sammenhænge vil elektroniske signaturer og elektroniske signatur certifikater blive anvendt ?

De seneste års hastige udvikling på det informationsteknologiske område, herunder sammensmeltningen af elektronisk databehandling (edb) og telekommunikation, har medført en øget udbredelse af digital kommunikation i samfundslivet. Brugen af elektronisk post, informationsudveksling og en række andre former for transaktioner via Internettet er kraftigt stigende.

I relation til offentlige myndigheder giver den elektroniske kommunikation mulighed for mere effektiv kommunikation mellem offentlige myndigheder og private borgere og virksomheder. Eksempelvis udvikles der i disse år stadig flere digitale selvbetjeningssystemer, der giver borgerne mulighed for at indgive deres selvangivelse, indsende SU-ansøgninger og -indberetninger, bestille et sygesikringsbevis, pas eller kørekort, indsende byggetilladelsesansøgninger eller flyttemeddelelser eller modtage en elektronisk recept fra lægen f.eks. som opfølgning på en telefonisk konsultation etc., fra en pc i hjemmet eller på arbejdspladsen, eller fra en offentlig info-kiosk.

Forskningsministeriets pilotprojekter med anvendelse af elektroniske signaturer i det offentlige indeholder en række praktiske eksempler på, hvordan elektroniske signaturer kan anvendes i kombination med f.eks. studiekort, SU-udbetaling og –indberetning, udveksling af patientoplysninger, patientjournaler og sygesikringsafregning mellem en række sundhedsinstitutioner. De erfaringer, der høstes i pilotprojekterne, er af stor betydning for opbygningen af en universel infrastruktur for elektroniske signaturer. Projekterne har afsløret mange af de problemstillinger, der opstår, når elektroniske signaturer skal anvendes i praksis.