Der er ikke fundet behov for at give Telestyrelsen adgang til at foretage inspektioner af nøglecentrets forretningslokaler.

Nøglecentre, som ikke ønsker at udstede kvalificerede certifikater vil kunne oprettes frit og drive deres virksomhed i henhold til kvalitetskrav og standarder, som de selv vælger. Telestyrelsen fører dog også et tilsyn med, om de danske nøglecentre overholder bestemmelsen i § 12 vedrørende behandling af personoplysninger.

Ved at lade markedet for elektroniske signaturer være åbent for aktører, som ikke opfylder bestemte krav om at være under tilsyn, etc., sikres det, at en eventuel markedsudvikling, hvor private autorisationsordninger eller lignende ordninger måtte blive fremherskende, ikke bremses af en ufleksibel lovgivning.

Baggrunden for at indrette tilsynet som et revisionsbaseret system, hvor en vigtig del af det praktiske tilsyn udføres af den eksterne revision i nøglecentrene, er for det første at udnytte den erfaring og kompetence, som allerede findes i revisionsbranchen med at udføre systemrevision. Det kræver specialistviden at kunne overskue og bedømme den avancerede teknologi, som anvendes i et nøglecenter, og denne viden findes ikke i dag i Telestyrelsen.

For det andet vil opbygning af et større statsligt tilsyn kræve mange ressourcer, som forudsættes betalt af de tilsynsbelagte virksomheder. Dette kunne afholde nøglecentre fra at udstede kvalificerede certifikater, og på den måde risikeres det, at der ikke opstår et marked for elektroniske signaturer af en kvalitet, som forbrugere, myndigheder og virksomheder kan have tilstrækkelig tiltro til. Det vurderes, at de udgifter til revision, som med forslaget pålægges nøglecentrene, i højere grad kommer nøglecentret selv til gode i form af viden, kontrol og erfaringsudveksling med revisionen, end det ville være muligt under en statslig ordning.

Det foreslås, at udgifterne ved tilsynet på kort sigt finansieres af det offentligt, men at udgifterne på længere sigt bør afholdes af de nøglecentre, der udsteder kvalificerede certifikater.

6. Ansvarsregler

I lovforslagets § 11 fastlægges særlige ansvarsregler for nøglecentre, der udsteder kvalificerede certifikater.

Bestemmelsen fastlægger ansvaret i visse tilfælde, hvor en person, der med rimelighed forlader sig på et certifikat, lider tab på grund af nøglecentret. Det drejer sig om tab opstået som følge af fejl og mangler i oplysningerne i et certifikat, manglende spærring af et certifikat, manglende eller fejlagtige oplysninger vedrørende udløbsdatoen eller gældende anvendelsesbegrænsninger for certifikatet samt fejl i nøglecentrets kontrol af, at underskriveren er i besiddelse af de signaturgenereringsdata, som korresponderer med de signaturverificeringsdata, der er indeholdt i certifikatet.

Det er ifølge bestemmelserne pålagt nøglecentret at bevise, at der ikke er sket fejl, som kan tilregnes nøglecentret i forbindelse med udstedelsen af et kvalificeret certifikat til en elektronisk signatur, samt at oplysningerne i certifikatet er korrekte.

Nøglecentret er ligeledes ansvarligt for, at der stilles oplysninger til rådighed om certifikatets udløbsdato, spærring, begrænsninger af hvilke formål certifikatet kan anvendes til eller beløbsmæssige begrænsninger for certifikatet, og at disse oplysninger er korrekte.

Der er således tale om et culpaansvar med omvendt bevisbyrde eller et såkaldt præsumptionsansvar. Begrundelsen for at indføre dette skærpede ansvar for visse nøglecentre er områdets meget tekniske og komplicerede karakter. Det vil for den almindelige bruger af elektroniske signaturer være svært at påvise, at der er sket fejl i forbindelse med håndteringen af signaturtjenesterne. Reglerne har derved et forbrugerbeskyttende sigte. For at der kan pålægges nøglecentret et erstatningsansvar for tab lidt hos underskriveren eller tredjemand efter bestemmelserne i dette lovforslag, skal de øvrige betingelser for at pålægge et erstatningsansvar også være tilstede.

Forhold, som ikke er omfattet af det særlige skærpede ansvar i loven, vil fortsat skulle bedømmes efter dansk rets almindelige bestemmelser.

7. Beskyttelse af peronsoplysninger

Lovforslaget indeholder enkelte supplerende bestemmelser til den gældende lovgivning om beskyttelse af personoplysninger.

Bestemmelserne i lovforslaget angående beskyttelse af persondata gælder for alle nøglecentre etableret i Danmark.

Ifølge forslaget må et nøglecenter kun indhente persondata i forbindelse med nøglecentervirksomheden direkte fra den registrerede eller med den registreredes udtrykkelige samtykke og kun i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat.

Nøglecentret må ikke behandle eller videregive data til andet formål end i det omfang, det er nødvendigt for udstedelsen eller opretholdelsen af et certifikat uden den registreredes udtrykkelige samtykke.