Notat

om

anvendelsen af serverbaserede løsninger for kvalificerede elektroniske signaturer

---

1. Baggrund

DanID A/S har bedt mig vurdere, hvorvidt det er muligt efter lov om elektroniske signaturer, at private nøgler opbevares på en central server, således at den private nøgle hverken opbevares på signaturindehaverens computer eller på en anden hardwareenhed, som f.eks. et smart card, der er i signaturindehaverens besiddelse.

Notatet indeholder alene en vurdering af, om en central serverløsning er lovlig efter lov om elektroniske signatur. Det indebærer for det første, at notatet ikke forholder sig til anden lovgivning, og for det andet at notatet konklusioner ikke gælder for certifikater og løsninger, som ikke er omfattet af loven, herunder ikke-kvalificerede certifikater som f.eks. OCES-certifikater. Lov om elektronisk signaturer er ikke til hinder for, at sådanne løsninger baseres på en central serverløsning.

Der er ikke i notatet foretaget nogen undersøgelse af, hvordan direktivet er implementeret i andre medlemslande, herunder hvorvidt det efter lovgivningen i andre medlemslande udtrykkeligt er tilladt henholdsvis forbudt for udstedere af kvalificerede certifikater at opbevare signaturindehavernes private nøgler på centrale servere. Implementeringen af direktivet i de enkelte medlemslande vil dog heller ikke i sig selv være styrende for fortolkningen i direktivet.

2. Regelgrundlaget

Udgangspunktet for undersøgelsen er som nævnt lov om elektroniske signaturer (lov nr. 417 af 31. maj 2000).

Til loven hører to bekendtgørelser om henholdsvis nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen (bkg. 2000/922) og om sikkerhedskrav til nøglecentre (bkg. 2000/923). Ingen af disse bekendtgørelser er dog relevante i forhold til de her behandlede spørgsmål.

Loven er baseret på forslag til lov om elektroniske signaturer (lovforslag 229/2000). Dette lovforslag rummer en række fortolkningsbidrag til loven i form af almindelige bemærkninger og bemærkninger til de enkelte bestemmelser.

Loven implementerer direktivet om elektroniske signaturer (dir. 1999/93). Til direktivet hører fire bilag om henholdsvis krav til kvalificerede certifikater (bilag I), krav til certificeringstjenesteudbydere, der udsteder kvalificerede certifikater (bilag II), krav til sikre elektroniske signaturgenereringssystemer (bilag III) og anbefalinger vedrørende signaturverificering (bilag IV).

Efter direktivets art. 3, stk. 5, kan Kommissionen offentliggøre referencenumre på almindeligt anerkendte standarder for elektronisk signatur-produkter. Bestemmelsen fastslår endvidere, at der er en formodning for, at elektroniske signatur-produkter overholder kravene i direktivets bilag II, litra f) og bilag III, såfremt de overholder de offentliggjorte standarder. Kommissionen har ved beslutning 2003/511 af 14. juli 2003 offentliggjort, at tre dokumenter udarbejdet af en arbejdsgruppe under CEN (den europæiske standardiseringskomite) har karakter af almindelige anerkendte standarder efter direktivets art. 3, stk. 5. Disse tre dokumenter får derfor også en vis værdi som fortolkningskilde til direktivet. Dokumenterne er benævnt henholdsvis CWA (CEN Workshop Agreement) 14167-1, CWA 14167-2 og CWA 14169.

3. Problemstillingen

Lov om elektroniske signaturer opstiller tre centrale begreber: 1) avanceret elektronisk signatur, 2) kvalificeret certifikat og 3) sikkert signaturgenereringssystem. En avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat og som er fremstillet ved brug af et sikkert signaturgenereringssystem benævnes også en kvalificeret elektronisk signatur (et begreb der dog ikke anvendes i loven). Lovens § 13 tillægger en kvalificeret elektronisk signatur en særlig juridisk status, når lovgivningen kræver, at elektroniske meddelelser er forsynet med signatur.

Loven opstiller en lang række krav, der skal være opfyldt, før en elektronisk signatur har status af avanceret elektronisk signatur, et certifikat har status af kvalificeret certifikat og et signaturgenereringssystem har karakter af et sikkert signaturgenereringssystem. Disse krav skal være opfyldt, før der foreligger en kvalificeret elektronisk signatur, og signaturen dermed får den særlige juridiske status, som følger af lovens § 13.

Vurderingen af om en kvalificeret elektronisk signatur kan være baseret på en central nøgleserverløsning, hvor brugernes private nøgler er lagret på en central server, afhænger derfor af, om de krav, loven opstiller, kan opfyldes med en sådan central serverløsning.

Det er særligt to af lovens krav, der påkalder sig interesse i denne vurdering.

For det første følger det af definitionen af en avanceret elektronisk signatur, lovens § 3, nr. 2, litra c, at signaturen skal skabes med midler, som kun underskriveren har kontrol over. Dette er en implementering af det tilsvarende krav i direktivets art. 2, nr. 2, litra c, hvoref-

ter signaturen skal genereres med midler, som underskriveren kan bevare den fulde kontrol over. Dette rejser spørgsmålet, om denne enekontrol skal være en fysisk kontrol, eller om en logisk kontrol er tilstrækkeligt.

For det andet følger det af lovens § 10, stk. 3, at "nøglecentre ikke må opbevare eller kopiere de personers signaturgenereringsdata, som nøglecentret gennem udstedelsen af certifikater måtte have fået kendskab til". Dette er en implementering af det tilsvarende krav i direktivets bilag II, litra j, hvorefter certificeringstjenesteudbyderen (benævnt "nøglecenter" i den danske lov) ikke må "opbevare eller kopiere de personers signaturgenereringsdata, som certificeringstjenesteyderen har tilbudt nøglehåndteringstjenester". Begrebet "signaturgenereringsdata" svarer til den private nøgle i en digital signatur-løsning. Dette rejser spørgsmålet, om denne bestemmelse hindrer en løsning med en central nøgleserver ejet af certifikatudstederen.

Disse to spørgsmål behandles i det følgende. Først behandles forbuddet mod nøglecentrets opbevaring af private nøgler, dernæst kravet om brugerens egenkontrol.

4. Forbuddet mod nøglecentrets opbevaring og kopiering af private nøgler, lovens § 10, stk. 3

Forbuddet mod nøglecentrets opbevaring og kopiering af private nøgler i lovens § 10, stk. 3, kan forstås på to måder.

Det kan for det første forstås som et ubetinget forbud mod, at nøglecentret er i besiddelse af brugernes private nøgle. Med denne forståelse vil det ikke være muligt at etablere en central serverløsning, hvor brugernes private nøgler er lagret på en central server i nøglecentres besiddelse. Derimod vil bestemmelsen efter sin ordlyd ikke være til hinder for, at brugernes private nøgler lagres på en central server hos en tredjepart, som ikke er certifikatudsteder. Forbuddet i § 10, stk. 3, omfatter alene udstederen af kvalificerede certifikater.

Bestemmelsen kan for det andet forstås således, at forbuddet kun gælder, når brugeren selv er i besiddelse af den private nøgle (forstået således at brugeren er i besiddelse af et fysisk medium, hvorpå den private nøgle er lagret). Med denne forståelse vil bestemmelsen ikke være til hinder for, at der kan etableres en ordning, hvor brugernes private nøgle lagres på en central server i certifikatudstederens besiddelse.

Bestemmelsen ordlyd taler umiddelbart for den førstnævnte fortolkning. Ordlyden indeholder ikke nogen forudsætning om, at forbuddet kun gælder, hvis brugeren selv er i besiddelse af den private nøgle. Man kan dog omvendt også læses ordlyden således, at certifikatudstederen ikke er i "besiddelse" af den private nøgle, hvis ikke udstederen har adgang til den, og at der ikke foreligger en "kopi", hvis der kun foreligger ét eksemplar af den private nøgle (på den centrale nøgleserver). Fortolkningen kan dog under alle omstændigheder ik-

ke i sig selv afgøres ved bestemmelsens ordlyd; også det bagvedliggende formål med bestemmelsen vil have betydning for fortolkningen.

Hverken lovens forarbejde eller direktivet giver noget sikkert svar på, hvad formålet med bestemmelsen har været. Bestemmelsen kan tjene forskellige formål.

Formålet kunne for det første være en sikring mod, at der gives certifikatudstederen adgang til at etablere bagdøre til brugernes private nøgle, som f.eks. vil kunne udnyttes af politiet og efterretningstjenesterne. Risikoen for etablering af bagdøre i krypteringsværktøjer har været et ganske omdiskuteret emne. Er dette formålet med bestemmelsen, vil den ikke give adgang til, at der etableres en central serverløsning hos certifikatudstederen. Loven, dennes forarbejder og direktivet peger dog i retning af, at dette ikke har været formålet med bestemmelsen.

Beskyttelsen mod sådanne bagdøre har navnlig betydning, når krypteringsværktøjer anvendes til hemmelighedskryptering. Det er i denne situation, at efterretningstjenester og andre kan have en interesse i at kunne skaffe sig adgang til den private nøgle og dermed til indholdet af den krypterede tekst, hvorimod det ikke forekommer sandsynligt, at certifikatudstederen, efterretningstjenester eller tilsvarende enheder skulle have samme interesse i at kunne afgive en borgers elektroniske signatur. Der er imidlertid intet i loven, dens forarbejder eller direktivet, der peger i retning af, at lovgiver også havde hemmelighedskryptering for øje ved reglernes tilblivelse. Der omtales alene kryptering i forbindelse med afgivelse af elektroniske signaturer, og det forekommer derfor ikke sandsynligt, at bestemmelsen i § 10, stk. 3, og den tilsvarende bestemmelse i direktivets bilag II, litra j, har haft beskyttelse mod bagdøre, der kunne give adgang til en krypteret tekst, for øje.

Herudover gælder forbuddet som nævnt kun for udstedere af kvalificerede certifikater. Det vil således ikke være i strid med reglerne, at én part udsteder certifikaterne, og en anden part etablere en central nøgleserver. Risikoen for etablering af bagdøre eller nøgleserverindehaverens eget misbrug vil imidlertid være det samme, hvad enten nøgleserverindehaveren er certifikatudstederen eller ej. Havde man fra lovgivers side ønsket at beskytte mod etableringen af bagdøre, ville det være nødvendigt at udforme reglen som et generelt forbud mod brug af centrale nøgleservere. Når reglen alene forbyder certifikatudstedere at etablere centrale nøgleservere, har det derfor formodningen mod sig, at formålet har været at beskytte mod bagdøre.

Et andet formål med bestemmelsen kunne være en beskyttelse mod, at der med centrale nøgleservere blev etableret et single point of failure/attack, som kunne udgøre en sikkerhedsrisiko i systemet. Dette rammes dog af samme indvending som netop er gjort ovenfor: Reglen forbyder ikke andre end certifikatudstederen at etablere en central nøgleserve og single point of attack-risikoen vil være helt den samme, hvad enten nøgleserveren besiddes af certifikatudstederen eller en anden. Forbuddet kan derfor næppe hellere antages at være en sikring mod et single point of attack.

Et tredje formål med bestemmelsen kunne være en sikring af, at certifikatudstederen ikke beholder eller i øvrigt kopierer de private nøgler, som udstederen får kendskab til i forbindelse med certifikatudstedelsen, når brugeren selv er i besiddelse af den private nøgle. I denne situation vil der ikke være behov for, at certifikatudstederen ligger inde med den private nøgle, og de ekstra kopier vil blot udgøre en ekstra og unødvendig sikkerhedsrisiko. Forstået på denne måde regulerer bestemmelsen den situation, hvor brugeren selv er i besiddelse af den private nøgle, og hvor certifikatudstederen får en (ubeskyttet) kopi af nøglen i sin besiddelse i forbindelse med certifikatudstedelsen.

Læser man de kortfattede bemærkninger i forarbejderne til lovens § 10, stk. 3, synes de at støtte denne fortolkning: "Det er ifølge stk. 3 forbudt for et nøglecenter, der udsteder kvalificerede certifikater, at opbevare eller kopiere de personers signaturgenereringsdata, som det har udstedt et certifikat til. Opbevaring og kopiering af signaturgenereringsdata vil kunne udgøre en alvorlig trussel mod den juridiske anerkendelse af elektroniske signaturer. Der bør være sikkerhed for, at det alene er underskriveren, der har adgang til signaturgenereringsdataene, og dermed, at det kun er underskriveren, der har haft mulighed for at benytte sin elektroniske signatur".

Bemærkningerne synes at forudsætte, at certifikatudstederen får en ubeskyttet adgang til de private nøgler, og at underskriveren selv er i besiddelse af den private nøgle. Generelt synes lovbemærkningerne at forudsætte, at den private nøgle kun kan opbevares på et fysisk medium i signaturindehaverens besiddelse. Muligheden for en løsning med en central nøgleserver nævnes ingen steder i lovbemærkningerne, ligesom det heller ikke nævnes i direktivet.

Dette taler for, at formålet med bestemmelsen alene har været at forbyde certifikatudstederens opbevaring og kopiering af den private nøgle, når signaturindehaveren selv er i besiddelse af den.

En tilsvarende forståelse af direktivets bestemmelse synes lagt til grund i dokumentet CEN Workshop Agreement (CWA) 14355:2004 – Guidelines for the implementation of Secure Signature-Creation Devices. I dokumentet knyttes nogle bemærkninger til direktivets betragtning 18, der er udgangspunktet for bestemmelsen i direktivets bilag II, litra j. Betragtning 18 har følgende ordlyd: "Opbevaring og kopiering af signaturgenereringsdata vil kunne udgøre en alvorlig trussel mod elektroniske signaturers juridiske gyldighed". Formuleringen om opbevaring og kopiering af signaturgenereringsdata genfindes i bestemmelsen i bilag II, litra j, og er ligeledes gentaget i de ovenfor citerede bemærkninger til lovens § 10, stk. 3. Om betragtning 18 bemærker dokumentet følgende: "SCD [Signature-Creation Data, dvs. den private nøgle] shall not be backed up or escrowed. For qualified signatures no duplicates of the SCD shall exist even with the consent of the signatory. If SCD is transferred, the source copy shall be reliable destroyed ... Thus, regardless of whether such duplicates of SCD are created with or without the consent or knowledge of the signatory, the interests of both the signatory and of the relying party would be jeopardized by such duplicate

SCD". Også her forudsættes således tilsyneladende, at bestemmelsen omhandler yderligere kopier (duplicates) af de private nøgler.

Dokumentet forudsætter også mere generelt, at der kan etableres en løsning med en central nøgleserver, se dokumentets afsnit 12, Signing Services: "It is quite possible to design a Signing Service system where the SCD of all users are held in large SSCD to which many users can connect. One instance would be an Internet sit that signs messages for the signatory when presented with the message and proper user authentication. This design is not prohibited by the Directive and is technically possible".

Dokumentet, der er udarbejdet af en undergruppe i regi af CEN, har ikke autoritativ karakter i forhold til fortolkningen af direktivet, men har dog alligevel en vis status i denne henseende.

Dette skyldes, at dokumentet er udarbejdet i forlængelse af en anden CEN Workshop Agreement, det ovennævnte CWA 14169. Som beskrevet ovenfor har CWA 14169 efter Kommissionens meddelelse 2003/511 karakter af en almindelig anerkendt standard i direktivets art. 3.5's forstand. CWA 14169 indeholder forskellige krav til sikre signaturgenereringssystemer i direktivets bilag III og skaber en formodning for, at disse krav er opfyldt, når kravene i CWA 14169 er opfyldt.

Ifølge forordet til CWA 14355 var CWA 14169 baseret på et princip om teknologineutralitet, hvorfor CWA 14169 ikke adresserede krav til specifikke teknologiplatforme og miljøer. Formålet med CWA 14355 er at udbygge CWA 14169 med angivelse af krav til sådanne specifikke teknologier ("The purpose of CWA 14355 is therefore to extend the previous work towards defining guidelines on implementing SSCDs in specific platforms (such as smart cards, PCs PDAs and mobile phones) and in specific environments (such as public terminals or secured environments").

Læser man CWA 14355 i sammenhæng med CWA 14169 peger dette således i retning af, at et sikkert signaturgenereringssystem i direktivets forstand kan udgøres af en central nøgleserver.

Dette er ikke i sig selv ensbetydende med, at bestemmelsen i bilag II, litra j, og lovens § 10, stk. 3, skal fortolkes således, at den ikke forbyder en central serverløsning, da CWA 14355 og CWA 14169 kun forholder sig til kravene i bilag III, men det understøtter formodningen for dette resultat.

Sammenfattende giver hverken loven, lovens forarbejder eller direktivet noget sikkert svar på, hvordan forbuddet mod certifikatudstederens opbevaring af private nøgler skal forstås. Spørgsmålet er heller ikke behandlet i retspraksis fra EF-domstolen eller fra danske domstole. Selvom der således ikke kan gives et sikkert svar på spørgsmålet, er det ud fra det ovenstående min vurdering, at lovens § 10, stk. 3, ikke forbyder brug af centrale nøgleservere i certifikatudstederens besiddelse.

5. Kravet om egenkontrol med den private nøgle i lovens § 3, nr. 2, litra c

Kravet om, at en avanceret elektronisk signatur skal være skabt med et middel, som kun underskriveren har kontrol over, kan dels forstås således, at underskriveren skal have kontrollen over et fysisk medium, hvorpå den private nøgle er lagret, dels således, at kun underskriveren må kunne skaffe sig adgang til den private nøgle.

I den første forståelse indeholder bestemmelsen et krav om *fysisk* egenkontrol, mens den i den anden forståelse også kan opfyldes ved en *logisk* egenkontrol.

Såfremt meningen havde været at kræve kontrol med et fysisk medium, forekommer det nærliggende at have angivet det eksplicit i teksten, og bestemmelsens ordlyd kan derfor umiddelbart peget i retning af, at en logisk egenkontrol vil kunne opfylde kravet, men svaret kan ikke med sikkerhed udledes af ordlyden, og det vil også være nødvendigt at se på bestemmelsens bagvedliggende formål.

Det kan overvejes, om bestemmelsen baggrund er et ideologisk funderet ønske om at markere, at den elektroniske signatur i lighed med den håndskrevne signatur er tæt knyttet til den enkeltes personlighed. Dette kunne tale for, at bestemmelsen skal forstås som et krav om fysisk kontrol (på sammen måde som den håndskrevne underskrift er fysisk knyttet til personen).

Der er imidlertid intet i forarbejderne, der antyder, at dette skulle være formålet med bestemmelsen. Tværtimod angives det i den kortfattede bemærkning til bestemmelsen, at den er indsat "af hensyn til sikkerheden omkring den elektroniske signatur". Det synes således at være mere konkrete sikkerhedsovervejelser, der har ført til bestemmelsen. Dette stemmer også overens med lovens opbygning i øvrigt, idet loven i vidt omfang har karakter af en sikkerhedsstandard.

Spørgsmålet er herefter hvilke sikkerhedsrisici, lovgiver har ønsket at imødegå ved kravet om underskriverens egenkontrol.

Det er åbenbart, at bestemmelsen skal sikre, at tredjeparter ikke har adgang til den private nøgle og dermed afgive underskriverens elektroniske signatur. Dette kan principielt sikres både ved logisk og fysisk egenkontrol.

Det kan overvejes, om bestemmelsen herudover har haft til hensigt sikre mod risici, som særligt er relevante i løsninger, hvor underskriveren ikke har fysisk kontrol over lagringsmedier, dvs. i de centraliserede serverløsninger. Dette vil tale for, at bestemmelsen skal fortolkes således, at den indeholder et krav om fysisk kontrol.

Det kan overvejes, om bestemmelsen skal imødegå muligheden for at serverindehaveren gennem bagdøre o.lign. skaffer sig adgang til private nøgler, som i øvrigt er logisk beskyttet. Der er dog intet i forarbejderne som tyder på, at dette har været hensigten med bestemmelsen. Bagdøre vil typisk særligt have relevans i forhold til hemmelighedskryptering, og loven kan ikke antages at have haft til hensigt at regulere hemmelighedskryptering, jf. herom ovenfor i afsnit 4.

Det kan endvidere overvejes, om man med bestemmelsen har ønsket, at de private nøgler fysisk skal være placeret decentralt hos brugerne for at sikre mod et single point of failure/attack. Forarbejderne er tavse herom, og noget sikkert svar kan ikke gives, men hvis formålet var at beskytte mod et single point of failure/attack havde det været nærliggende, at dette var nævnt i forarbejderne.

På denne baggrund er det efter min opfattelse mest nærliggende, at formålet med bestemmelsen alene er at sikre, at ikke andre end underskriveren har adgang til den private nøgle og dermed adgang til at udvirke signaturen.

Denne forståelse af bestemmelsen understøttes også af, at et sikkert signaturgenereringssystem må antages at kunne være baseret på en central serverløsning, jf. afsnit 4.

Som nævnt rummer direktivet og loven tre centrale begreber (avanceret elektronisk signatur, kvalificeret certifikat og sikkert signaturgenereringssystem), som alle skal foreligge, før de særlige retsvirkninger efter direktivet og loven udløses. Det vil derfor være uden praktisk betydning om et sikkert signaturgenereringssystem kunne være baseret på en central serverløsning, hvis denne samme løsning skulle indebærer, at der ikke foreligger en avanceret elektronisk signatur.

At kravet om egenkontrol ikke forudsætter en fysisk besiddelse af lagringsmediet synes også forudsat i det ovennævnte dokument CWA 14355:2004, se s. 15, og ligeledes af Forum of European Supervisory Authorities for Electronic Signatures (FESA) i dokumentet Public Statement on Server Based Signature Services. FESA har ingen særlig autoritet i forhold til fortolkningen af direktivet, men medlemmerne er de nationale tilsynsmyndigheder og har dermed typisk været involveret i udformningen af direktivet og i udarbejdelsen af de nationale implementeringslove.

Sammenfattende giver forarbejderne til direktivet og loven heller ingen sikre svar på, hvorvidt kravet om egenkontrol skal forstås som fysisk egenkontrol, og der foreligger heller ingen praksis herom fra EF-domstolen eller danske domstole. Det er derfor heller ikke muligt at give et sikkert svar på dette spørgsmål. På baggrund af det ovenstående må bestemmelsen om egenkontrol i lovens § 3, nr. 2, litra c, dog efter min vurdering antages ikke at indeholde et krav om fysisk egenkontrol og dermed heller ikke hindre, at en avanceret elektronisk signatur baseres på en central serverløsning.

6. Konklusion

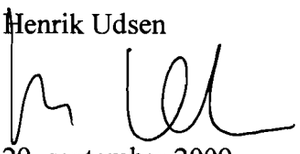
I det ovenstående er det vurderet, om loven om elektroniske signaturer hindrer brug af centrale nøgleserver-løsninger.

Det er for det første vurderet, hvorvidt lovens forbud mod, at udstedere af kvalificerede certifikater besidder og kopierer brugernes private nøgler, indebærer, at disse certifikatudstedere ikke må drive centrale nøgleservere. Hverken direktivets eller lovens forarbejder gør det muligt at give et sikkert svar, men det er min vurdering, at bestemmelsen ikke hindrer udstedere af kvalificerede certifikater i at drive centrale nøgleservere.

Det er for det andet vurderet, hvorvidt lovens krav om, at en avanceret elektronisk signatur skal skabes med midler, som kun underskriveren har kontrol over, indebærer, at en avanceret elektronisk signatur ikke kan være baseret på en central nøgleserver-løsning. Det er min vurdering, at dette ikke kan antages at være tilfældet. Heller ikke her giver forarbejderne dog et sikkert svar.

Der er efter min vurdering ikke andre bestemmelser i loven som hindrer brugen af centrale serverløsninger. En sådan brug forudsætter dog, at den konkrete løsning kan leve op til de sikkerhedskrav, der i øvrigt gælder for kvalificerede elektroniske signaturer.

Henrik Udsen



29. september 2009