

# Høringsnotat

Oktober 2019

---

## **Behandling af indkomne høringssvar i forbindelse med revision af certifikatpolitikker for Offentlige Certifikater til Elektronisk Service (OCES), samt offentlig certifikatpolitik for kvalificerede certifikater og offentlig politik for kvalificeret tidsstempling**

Digitaliseringsstyrelsen har ved høringsfristens udløb den 1. april 2019 modtaget en række høringssvar fra de organisationer og myndigheder, som har fået tilsendt høringen. Der er modtaget høringssvar fra i alt fire organisationer og myndigheder.

Høringsparternes bemærkninger er i dette høringsnotat indarbejdet i *ikke-redigeret form*. De følger strukturen i certifikatpolitikkerne og fremstår dermed ikke som samlede svar. Herved opnås et overblik over de samlede kommentarer til hvert punkt, for at give læseren en bedre fornemmelse af, hvad andre organisationer og myndigheder har bemærket til de samme punkter. Generelle kommentarer til certifikatpolitikkerne er medtaget under punkt 1. Der er overordnet set blevet taget godt i mod opdateringen af certifikatpolitikkerne.

Certifikatpolitikkerne er tilpasset dels som følge af de indkomne høringssvar og dels på baggrund af den analysefase som er gennemført i forbindelse med udbuddet af NemLog-in3.

De opdaterede certifikatpolitikker offentliggøres i 4. kvartal 2019 og kan indtil videre tilgås via Digitaliseringsstyrelsens hjemmeside ([digst.dk](http://digst.dk)) og på [Høringsportalen](#).

Digitaliseringsstyrelsen vil ibrugtage certifikatpolitikkerne i forbindelse med idriftsættelse af NemLog-in3, men andre parter kan basere udstedelse af certifikater og tidsstempler på certifikatpolitikkerne, når tilhørende revisionsinstrukser er offentliggjort. Disse forventes offentliggjort i løbet af 2019.

God læselyst.

## Indhold

<b>1. Generelle kommentarer.....</b>	<b>3</b>
<b>2. Certifikatpolitikker for Offentlige Certifikater til Elektronisk Service (OCES) (Bilag D1 og D2).....</b>	<b>9</b>
2.1 MOCES – Certifikatpolitikker for Offentlige Certifikater til Elektronisk Service (OCES) (Bilag D1) .....	9
2.2 VOCES – Certifikatpolitikker for Offentlige Certifikater til Elektronisk Service (OCES) (Bilag D2) .....	14
<b>3. Offentlig certifikatpolitik for kvalificerede certifikater (Bilag D3, D4 og D5) .....</b>	<b>17</b>
3.1 Kvalificeret person (Bilag D3).....	17
3.2 Kvalificeret medarbejder (Bilag D4).....	21
3.3 Kvalificeret virksomhed (Bilag D5).....	27
<b>4. Offentlig politik for kvalificeret tidsstempling (Bilag D6) .....</b>	<b>30</b>

## 1. Generelle kommentarer

<b>Afsnit</b>	Generelt
<b>Høringspart</b>	Datatilsynet
<b>Bemærkning</b>	<p>Datatilsynet har gennemgået det fremsendte materiale.</p> <p>Generelt skal Datatilsynet oplyse, at tilsynet alene har kompetence ved behandlinger af oplysninger om fysiske personer.</p> <p>Datatilsynet skal derfor anmode om, at der hvor der behandles denne type oplysninger, tages stilling eksplicit stilling til risikoen for den registreredes rettigheder. Dette er særligt, typerne af person og medarbejdersignaturer men også dele af virksomhedssignaturerne.</p> <p>Datatilsynet skal på baggrund af den dataansvarliges vurdering af denne risiko, særligt henlede opmærksomheden på de tiltag der er nødvendige, såfremt risikoen skønnes at være høj.</p> <p>Generelt fremstår materialet i øvrigt sammenhængende og gennemarbejdet.</p> <p>Datatilsynet har i øvrigt ingen bemærkninger til de rent processuelle dele og tekniske implementeringer af certifikaterne og den tiltænkte implementering af de pågældende politikker.</p> <p>Materialet er dog en central og væsentlig del, af hele grundlaget for fortrolighed, autentificering og uafviselighed, af samtlige transaktioner, der foretages ved hjælp af certifikaterne. på den baggrund opfordres der til, at dette finder udtryk ved vejledning om brugen og den efterfølgende implementering af udstedte certifikater.</p>
<b>Svar</b>	<p>Digitaliseringsstyrelsen finder det også væsentligt, at der er særlig opmærksomhed omkring databeskyttelse. Derfor er GDPR eksplicit nævnt i alle certifikatpolitikkerne (inklusive politikkerne for virksomhedscertifikater) som eksempel på regulering, der skal efterleves.</p> <p>På baggrund af Datatilsynets høringssvar tilføjes i øvrigt LOV nr. 502 af 23/05/2018, for at henlede udstederes opmærksomhed på disse supplerende bestemmelser.</p>

<b>Afsnit</b>	Generelt
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	Spørgsmål 1: Er der gjort nogle tanker og overvejelser omkring hensyn til og håndtering af udenlandske borgere brug af løsninger baseret på OCES, herunder identifikation og verifikation ved tilknytning af fysisk person til en elektronisk identitet?
<b>Svar</b>	Ja. I forhold til tidligere versioner af OCES-certifikatpolitikkerne er kravet om kontrol af CPR-nummer fjernet, og der er dermed åbnet op for, at brugeren kan være registreret uden CPR fx gennem eIDAS Gateway.

<b>Afsnit</b>	Generelt
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	Spørgsmål 2: Er der gjort nogle overvejelser omkring udskiftning af rodcertifikat(er) for CA(?er) i en givent PKI-struktur og betydning for dette hos brugerne og tilhørende klienter?
<b>Svar</b>	Der er i certifikatpolitikkerne ikke stillet eksplicitte krav til skift af rodcertifikat(er), men CA skal sikre at der genereres nye nøglepar, herunder nyt rodnøglepar inden udløb jf. afsnit 5.6.  Da rodnøglepar har en planlagt lang levetid, kan teknologien og standarder for skift af CA nøglepar ændres over tid. Derfor stilles der ikke eksplicitte krav.

<b>Afsnit</b>	Generelt
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	Spørgsmål 3: Er der gjort nogle overvejelser omkring krydscertificering mellem CA'er i det tilfælde at der påtænkes at blive anvendt flere CA'er og evt. anvendelse af en virtuel rod?
<b>Svar</b>	Jf. afsnit 1.3.1 i certifikatpolitikkerne forhindres krydscertificering ikke, men der stilles ikke eksplicitte krav om krydscertificering. Det

	er således op til den konkrete implementering af et PKI, der benytter en af certifikatpolitikkerne, at vurdere om et givet CA skal krydscertificeres.
--	---

<b>Afsnit</b>	Generelt
<b>Høringspart</b>	Danske Regioner
<b>Bemærkning</b>	<p>Vi vil gerne kvittere for god tid til kommentering. Vi finder certifikatpolitikkerne fornuftige og afbalancerede og godt strukturerede. Det har gjort læsningen lettere.</p> <p>Vi har overordnet ikke mange kommentarer. Nedenstående er primært detaljer, vi har bemærket – eller forhold, der har været vanskelige at forstå.</p>
<b>Svar</b>	-

<b>Afsnit</b>	Generelt
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Høringspart skal anmode om, at det tydeliggøres enten direkte i CP'erne eller i en tilhørende vejledning, hvornår et krav rettet mod CA henfører udelukkende til Digitaliseringsstyrelsen, eller hvornår dette krav kan henføres videre til underleverandøren. Det er nødvendigt med en entydig definition, så man som underleverandør helt specifikt kan se hvilke krav der kun vedrører DIGST og hvilke der kan videreføres til underleverandøren.
<b>Svar</b>	Grundlæggende er krav rettet mod CA og det er CA's ansvar at sikre at eventuelle underleverandører efterlever relevante krav i certifikatpolitikkerne.

<b>Afsnit</b>	Generelt
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Der er flere krav i MOCES og VOCES CP'er, som ikke er gengivet i Kvalificeret medarbejder, Kvalificeret virksomhed og Kvalificeret person, hvorfor der synes at være strengere krav til MOCES og

	VOCES. Høringsparten anmoder derfor om at disse krav udgår eller tilpasses.
<b>Svar</b>	Det er særligt i forhold til revision og rapportering at OCES certifikatpolitikkerne har eksplicitte krav. Dette skyldes primært at revision og rapportering for kvalificerede tillidstjenesteudbydere i modsætning til OCES tillidstjenesteudbydere er reguleret gennem eIDAS, hvorfor det ikke er nødvendigt at have eksplicitte krav i certifikatpolitikkerne.

<b>Afsnit</b>	Generelt
<b>Krav</b>	5.1.1-01, 5.1.1-02, 5.1.1-03, 5.1.1-04
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>Høringsparten anmoder om at begreberne “CA driftslokaler” i KRAV 5.1.1-01, “lokaler” i KRAV 5.1.1-02 samt “driftslokaler” i KRAV 5.1.1-03 og KRAV 5.1.1-04, rettes således at det er tydeligt hvornår der menes almindelige kontorlokaler, datacenter og lokaler, hvor udstyr til nøgle-generering er placeret.</p> <p>Det formodes endvidere, at lokaler, hvor udstyr til nøglegenerering er placeret skal være defineret som særligt sikkerhedsområde i henhold til ISO 27001 A.11.1, og ikke som angivet i KRAV 5.1.1-02 alle lokaler, der benyttes af medarbejdere hos CA.</p>
<b>Svar</b>	Certifikatpolitikkerne er tilrettet en ensartet brug af betegnelsen "CA driftslokaler".

<b>Afsnit</b>	Generelt
<b>Krav</b>	5.1.1-04
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>Høringsparten anmoder om at:</p> <p>[KRAV 5.1.1-04] CA skal segmentere sine driftslokaler i zoner i forhold til en risikovurdering under hensyntagen til kritikaliteten af de enkelte delsystemer. Zoneopdelingen skal følge den logiske segmentering i netværk.</p>

	Bør omformuleres til at være i overensstemmelse med:  ETSI 319, 401 REQ-7.8-02: The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.
<b>Svar</b>	Certifikatpolitikkerne er tilrettet en bedre oversættelse af ETSI-kravet.

<b>Afsnit</b>	Generelt
<b>Krav</b>	5.5.4-02
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Høringspart anmoder om at:  [KRAV 5.5.4-02] Der skal tages regelmæssige sikkerhedskopier af kritiske data og software i overensstemmelse med ISO 27002, clause 12.3.  Ændres til:  [KRAV 5.5.4-02] Der skal tages regelmæssige sikkerhedskopier af kritiske data og software i overensstemmelse med ISO 27001 A.12.3.
<b>Svar</b>	Henvisning til ISO 27002 er identisk med krav i ETSI EN 411 del 1 krav OVR-6.4.8-03. Kravet fastholdes i sin nuværende form.

<b>Afsnit</b>	Generelt
<b>Krav</b>	6.1.1-03
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Høringspart anmoder om henvisningen til at CA skal følge relevante og officielle anbefalinger fra ENISA:  [KRAV 6.1.1-03] For kritiske dele af CA's infrastruktur, skal CA følge relevante og officielle anbefalinger fra ENISA vedr. anvendelsen af tidssvarende algoritmer og nøglelængder.

	<p>Ændres til:</p> <p>[KRAV 6.1.1-03] For kritiske dele af CA's infrastruktur, skal CA følge relevante og officielle anbefalinger vedr. anvendelsen af tidssvarende algoritmer og nøglelængder.</p> <p>Hvor ENISA ikke fremgår eksplicit, da Høringspart mener at relevante og officielle anbefalinger også kan komme fra fx nationale myndigheder.</p>
<b>Svar</b>	Digitaliseringsstyrelsen vurderer, at ENISA er den rigtige kilde til anbefalinger om anvendelse af tidssvarende algoritmer og nøglelængder. Formuleringen fastholdes.

<b>Afsnit</b>	Generelt
<b>Krav</b>	8.4-01
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>Høringspart anmoder om at SANS CIS udgår af følgende krav:</p> <p>[KRAV 8.4-01] Der skal gennemføres systemrevision hos CA. Ved systemrevision forstås revision af:</p> <ul style="list-style-type: none"> <li>• generelle it-kontroller i virksomheden, der er baseret på verificeret dokumentation som gennemføres ud fra internationale anerkendte standarder og rammeværk for sikkerhedskontroller fx SANS CIS</li> </ul>
<b>Svar</b>	<p>Kravet er ændret til at henvise til en revisionsinstruks som Digitaliseringsstyrelsen udarbejder til brug for revision af alle de 5 certifikatpolitikker.</p> <p>I forbindelse med udarbejdelse af disse instrukser vil Digitaliseringsstyrelsen inddrage denne kommentering.</p>



## 2. Certifikatpolitikker for Offentlige Certifikater til Elektronisk Service (OCES) (Bilag D1 og D2)

### 2.1 MOCES – Certifikatpolitikker for Offentlige Certifikater til Elektronisk Service (OCES) (Bilag D1)

<b>Afsnit</b>	MOCES (og VOCES)
<b>Krav</b>	8.4
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>Gælder for både MOCES og VOCES.</p> <p>Kravet specificerer at der skal foretages en sårbarhedsvurdering af logningsproceduren i forbindelse med systemrevision. Kravet giver ikke mening. Høringspart anmoder om, at kravet udgår eller omformuleres. Kravet ser ud til at stamme fra RFC3647, hvor kravet omfatter en sårbarhedsvurdering, som kan indebære, at audit data bliver analyseret ved brug af dedikeret software med henblik på at identificere mulige forsøg på brud på sikkerheden af systemet.</p> <p>I RFC3647 afsnit 4.5.4 “Audit Logging Procedure” står der nederst:</p> <p>“Vulnerability assessments, for example, where audit data is run through a tool that identifies potential attempts to breach the security of the system.”</p>
<b>Svar</b>	<p>Digitaliseringsstyrelsen er enige i denne betragtning. Kravet følger implicit af generelle krav til risikostyring (KRAV 5-01 - KRAV 5-08) og krav til fortrolighed og integritet af logdata (KRAV 5.4.4-01).</p> <p>Krav 8.4-02 slettes.</p>

<b>Afsnit</b>	MOCES (4.6)
<b>Krav</b>	-
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	Er det muligt og tilladt at genanvende nøglepar ved genudstedelse af nyt certifikat?
<b>Svar</b>	Jf. definition af genudstedelse i afsnit 4.6 vil nøglepar blive genanvendt ved genudstedelse. Bemærk at certifikatpolitikkerne også

	understøtter begreberne certifikatfornyelse (afsnit 4.7) og certifikatopdatering (afsnit 4.8).
--	--

<b>Afsnit</b>	MOCES (4.9)
<b>Krav</b>	-
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	Kunne det være en idé at nedsætte tidsintervallet på p.t. 12 timer til eksempelvis 6 timer eller lavere for herved at øge sikkerheden?
<b>Svar</b>	Udgangspunktet er, at spærringen skal ske hurtigst muligt. De 12 timer er en øvre grænse, der kan benyttes til eventuelle afklaringer for at sikre at en af årsagerne til spærring (pkt. a-h) er indtruffet. Digitaliseringsstyrelsen vurderer, at der kan være situationer, hvor denne afklaring vil kunne tage mere end 6 timer og har derfor fastholdt en øvre grænse på 12 timer.

<b>Afsnit</b>	MOCES (4.9)
<b>Krav</b>	-
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	Kunne det være en idé at anvende straks opdatering af tilbagetrækningsliste til brug for bl.a. it-løsninger som anvender OCSP-løsning for at reducere risici?
<b>Svar</b>	Jf. afsnit 4.9.8 skal CA offentliggøre spærrelister senest 1 minut efter gennemført spærring (dog længere frist for rod-CA grundet, at rod-CA skal være offline). Der er således tale om straks-opdatering af spærrelister i forbindelse med en spærring.

<b>Afsnit</b>	MOCES (4.9.1)
<b>Krav</b>	4.9.1-01
<b>Høringspart</b>	Region Midtjylland - Danske Regioner

<b>Bemærkning</b>	Det forekommer at være meget langt tid til spærring af certifikater. Vi regner med, at der her regnes i minutter, da en spærring kan være kritisk.
<b>Svar</b>	Udgangspunktet er, at spærringen skal ske hurtigst muligt. De 12 timer er en øvre grænse, der kan benyttes til eventuelle afklaringer for at sikre at en af årsagerne til spærring (pkt. a-h) er indtruffet. Digitaliseringsstyrelsen vurderer, at der kan være situationer, hvor denne afklaring vil kunne tage mere end 6 timer og har derfor fastholdt en øvre grænse på 12 timer.

<b>Afsnit</b>	MOCES (4.9.3)
<b>Krav</b>	4.9.3-02
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	<p>Vi finder indrapporteringsmulighederne ikke relevante.</p> <ul style="list-style-type: none"> <li>- Vi forventer, at der med "Fysisk post" menes et papirbrev formidlet og fragtet af en eller anden virksomhed til dette. Det mener vi ikke er relevant – bare af hensyn til tidsfaktoren.</li> <li>- Vi forstår Web, som indrapportering via en dedikeret web-portal med brug af relevant certifikatet og signering – eller brug af webservice med anvendelse af relevant certifikat.</li> <li>- Vi finder ikke, at telefonisk henvendelse kan give den rette sikkerhed – det vil kræve særlige procedurer for tilbageringning m.v. Vi finder ikke, denne mulighed relevant endsige sikker nok.</li> <li>- Brugen af offentlig Digital Post skal være en metode</li> </ul>
<b>Svar</b>	<p>"Fysisk post" er inkluderet, så et CA ikke kan afvise at behandle en anmodning på baggrund af, at den er sendt som fysisk brev, men at det næppe i praksis være en særlig hyppig mekanisme.</p> <p>"Web" er tænkt som et browserbaseret interface.</p> <p>"Telefonisk" er inkluderet, efter samme argument som for fysisk post. Det er CA ansvar at sikre sig at anmodningen sendes af en autoriseret anmoder jf. KRAV 4.9.3-01.</p> <p>Under forudsætning af, at en anmodning kan valideres til at komme fra en autoriseret anmoder, kan CA tilbyde andre kanaler inklusiv</p>

	"Digital Post" og e-mail. "Digital Post" vil ikke være et krav, da Certifikatpolitikkerne også skal kunne anvendes af CA'er, der er en fysisk person eller privat virksomhed.
--	---

<b>Afsnit</b>	MOCES (4.9.8)
<b>Krav</b>	-
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Der anmodes om en længere frist (end 10 min) for offentliggørelse af spærreliste for rod-CA efter en spærring. Høringspart finder 30 min som en rimelig frist. Her skal dog bemærkes at en offentliggørelse vil finde sted så hurtigt som muligt. Denne bemærkning gælder for de CP'er hvor kravet fremgår.
<b>Svar</b>	Digitaliseringsstyrelsen anerkender at der er særlige forhold i forbindelse med offentliggørelse af spærrelister fra rod-CA som skal være offline jf. KRAV 5.1.2-12. Det vurderes at de særlige sikkerhedsforanstaltninger omkring rod-CA kan betyde at 30 minutter er en rimelig frist.  Certifikatpolitikkerne vil blive tilrettet så "10 min." ændres til "30 min."

<b>Afsnit</b>	MOCES (4.10.2)
<b>Krav</b>	4.10.2-02
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	Vi er enige i performancemålet 95% mindre end 1 sekund. Men vi vil også have mål for de resterende 5%; f.eks. 95% af de restende 5% mindre end 2 sekunder og ingen over 4 sekunder.
<b>Svar</b>	Digitaliseringsstyrelsen er delvist enige i denne betragtning. Performancemål er udvidet, så mindst 99% af svarene skal være mindre end 1 sekund.

<b>Afsnit</b>	MOCES (5.1.1)
<b>Krav</b>	-
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	Kunne det være en idé, at henvise til ISO 27002 i stedet for ISO 27001 alternativt benytte principperne fra Forsikring og Pension evt. suppleret med oplysninger i FKOBST 358-1 omkring fysisk sikkerhed?
<b>Svar</b>	Henvisningen er indført for at være i overensstemmelse med den europæiske standard ETSI EN 319 411 del 1, krav OVR-6.4.8-03. Henvisningen fastholdes.

<b>Afsnit</b>	MOCES (5.1.1)
<b>Krav</b>	-
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	Kunne det være en idé, at stille krav om at efterleve standarden: ANSI/TIA-942 på et niveau svarende til: Tier 3?
<b>Svar</b>	Krav i certifikatpolitikkerne er rettet mod en europæisk harmonisering og derfor anvendes ETSI-standarder som udgangspunkt for kravsætningen.

## 2.2 VOCES – Certifikatpolitikker for Offentlige Certifikater til Elektronisk Service (OCES) (Bilag D2)

<b>Afsnit</b>	VOCES (1.6.1)
<b>Krav</b>	
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>Vedrørende definitionen af ISO27001: Gældende version af “ISO/IEC 27001 - Information technology -- Security techniques -- Information security management systems”.</p> <p>Høringspart anmoder om, at der angives en rimelig frist til at implementere og efterleve eventuelle fremtidige nye version af ISO 27001.</p>
<b>Svar</b>	Definitionen af ISO 27001 er ændret til at henvise til en specifik version af standarden. I forbindelse med opdatering af ISO 27001 vil certifikatpolitikkerne vil blive opdateret i en styret proces, der giver mulighed for at CA'er kan have en overgangsordning.

<b>Afsnit</b>	VOCES (4.9.1)
<b>Krav</b>	4.9.1-01
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	<p>Det forekommer at være meget langt tid til spærring af certifikater. Vi regner med, at der her regnes i minutter, da en spærring kan være kritisk.</p>
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	VOCES (4.9.3)
<b>Krav</b>	4.9.3-02
<b>Høringspart</b>	Region Midtjylland - Danske Regioner

<b>Bemærkning</b>	<p>Vi finder indrapporteringsmulighederne ikke relevante.</p> <ul style="list-style-type: none"> <li>- Vi forventer, at der med "Fysisk post" menes et papirbrev formidlet og fragtet af en eller anden virksomhed til dette. Det mener vi ikke er relevant – bare af hensyn til tidsfaktoren.</li> <li>- Vi forstår Web, som indrapportering via en dedikeret web-portal med brug af relevant certifikatet og signering – eller brug af webservice med anvendelse af relevant certifikat.</li> <li>- Vi finder ikke, at telefonisk henvendelse kan give den rette sikkerhed – det vil kræve særlige procedurer for tilbageringning m.v. Vi finder ikke, denne mulighed relevant endsige sikker nok.</li> <li>- Brugen af offentlig Digital Post skal være en metode</li> </ul>
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	VOCES (4.10.2)
<b>Krav</b>	4.10.2-02
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	Vi er enige i performancemålet 95% mindre end 1 sekund. Men vi vil også have mål for de resterende 5%; f.eks. 95% af de restende 5% mindre end 2 sekunder og ingen over 4 sekunder.
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	VOCES (9.4)
<b>Krav</b>	-
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Høringspart anmoder om, at definitionerne for persondata følger gældende lovgivning, Databeskyttelsesforordningen (GDPR artikel 6 og 9) og Databeskyttelsesloven i stedet for anvendelsen af uklare definitioner for private og fortrolige oplysninger.
<b>Svar</b>	Definitionerne var videreført fra eksisterende OCES certifikatpolitikker. Digitaliseringsstyrelsen har revurderet

	nødvendigheden på baggrund af kravene i forhold til at GDPR og supplerende dansk lovgivning er trådt i kraft. På den baggrund er kravene fjernet i alle certifikatpolitikkerne.
--	---

<b>Afsnit</b>	VOCES (9.4.4)
<b>Krav</b>	9.4.4-03
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	Det er ikke helt klart, hvorfor der her sættes regler for MOCES certifikater?
<b>Svar</b>	Der er tale om en fejl fra copy-paste. Dette vil blive rettet.



### 3. Offentlig certifikatpolitik for kvalificerede certifikater (Bilag D3, D4 og D5)

#### 3.1 Kvalificeret person (Bilag D3)

<b>Afsnit</b>	Kvalificeret person (1.3.3)
<b>Krav</b>	-
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Helt generelt bør man vurdere om der er behov for at inkludere distinktionen mellem certifikatindehaver og certifikatholder, når det i denne CP er en og samme person.
<b>Svar</b>	<p>Digitaliseringsstyrelsen har vurderet om man med fordel kan nøjes med at anvende én af termene certifikatindehaver eller certifikatholder.</p> <p>Det er valgt at fastholde begge termer, dels for at have samme terminologi på tværs af certifikatpolitikker og dels for at indikere, hvornår der er tale om aftaleforhold og hvornår der er tale om praktisk anvendelse.</p> <p>Det er tydeliggjort i afsnit 1.3.3, at certifikatindehaver og certifikaterholder er samme fysiske person.</p>

<b>Afsnit</b>	Kvalificeret person (2.1)
<b>Krav</b>	2.1-06
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Vilkår og betingelser skal stilles til rådighed via et varigt kommunikationsmiddel. Et kommunikationsmiddel er per definition ikke varigt. Derimod kan man tale om et varigt medium, som der er givet definition på i Informationsordbogen og af hhv. Forbrugerombudsmanden og Finanstilsynet.
<b>Svar</b>	Digitaliseringsstyrelsen tilretter og anvender termen "varigt kommunikationsmedie" i alle certifikatpolitikkerne. Dette er rettet i både afsnit 2.1 og 4.4.1.

<b>Afsnit</b>	Kvalificeret person (3.1.2)
<b>Krav</b>	3.1.2-03
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>”Hvis certifikatholder er registreret med pseudonym, må pseudonym ikke være af en art, der kan give anledning til oplagte misforståelser og må ikke krænke varemærker.”</p> <p>Det kan være vanskeligt at afgøre, hvornår et varemærke er krænket. I stedet kunne man skrive ”må ikke være identisk eller forveksleligt med et varemærke”. Endvidere kunne det være hensigtsmæssigt, at CA havde mulighed for at afvise krænkende eller uetiske pseudonymer som fx ”Luder”, ”ILOVEISIS” o.l.</p>
<b>Svar</b>	Digitaliseringsstyrelsen er enig i betragtningen og tilretter alle certifikatpolitikkerne.

<b>Afsnit</b>	Kvalificeret person (4.1.2)
<b>Krav</b>	4.1.2-01, 4.1.2-02
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>[krav 4.1.2-01] Certifikatanmodning skal ske gennem en betroet RA. Det er mere relevant, at det er en ”autoriseret” RA (autoriseret af CA).</p> <p>[krav 4.1.2-02] ”Hvis eksterne registreringstjenesteudbydere anvendes, skal registreringsdata udveksles sikkert og kun hos anerkendte RA’ere, hvis identitet er autentificeret”.</p> <p>Registreringstjeneste er defineret, men ikke registreringstjenesteudbyder, i øvrigt er forkortelsen RA anvendt alle andre steder. Hvad menes med en anerkendt RA, og hvem skal anerkende?</p>
<b>Svar</b>	Alle RA skal være betroet og anerkendt, for at CA kan være betroet og dermed er det ikke nødvendigt sprogbrug. Alle certifikatpolitikkerne er tilrettet til udelukkende at anvende termen RA.

<b>Afsnit</b>	Kvalificeret person (4.3.1)
<b>Krav</b>	4.3.1-08
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>[krav 4.3.1-08] Et navn, der anvendes til at angive én certifikatholder i et certifikat, må ikke anvendes til at angive en anden certifikatholder i et certifikats i løbet af CA's livstid".</p> <p>Bør tydeliggøres. Der kan være mange, der hedder Peter Hansen.</p>
<b>Svar</b>	Digitaliseringsstyrelsen tilføjer note der tydeliggør, at det er det samlede navn inklusiv <i>subject serialNumber</i> .

<b>Afsnit</b>	Kvalificeret person (4.3.2)
<b>Krav</b>	4.3.2-01
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>Her vælger man at anvende begge begreber i overskriften, mens certifikatindehaver anvendes i krav 4.3.2-01 og certifikatholder anvendes i overskriften til punkt 4.4.1</p> <p>Denne bemærkning understøtter den generelle kommentar om, at det giver problemer for læsbarheden at anvende 2 begreber for den samme person.</p>
<b>Svar</b>	Se tidligere besvarelse vedrørende kvalificeret person (afsnit 1.3.3).

<b>Afsnit</b>	Kvalificeret person (4.7)
<b>Krav</b>	4.7.1-02, 4.7.2-01
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	Krav 4.7.1-02 og krav 4.7.2-01 bør skrives sammen, da det er samme krav. "CA skal sikre at certifikatholder kan forny certifikat on-line.

<b>Svar</b>	Første krav sætter en øvre grænse for hvor lang tid, der kan fornyes, mens andet krav angiver, at det er tilladt for CA eller certifikatindehaver, at der ikke skal kunne fornyes. Dette kan fx være relevant for "korttidscertifikater", som ikke persisteres.
-------------	---

<b>Afsnit</b>	Kvalificeret person (4.9.3)
<b>Krav</b>	4.9.3-03, 4.9.3-05
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>Krav 4.9.3-03 "CA skal orientere om gennemført til certifikatindehaver via..."</p> <p>Hvad skal CA orientere om? I MOCES står "om spærring.."</p> <p>Krav 4.9.3-05 "kvittering sendes til den af skifteretten hhv. bobestyrer angivne postadresse".</p> <p>Anvendelse af Digital Post bør overvejes?</p>
<b>Svar</b>	<p>"spærring" er tilføjet krav 4.9.3-03.</p> <p>Krav 4.9.3-05 er generaliseret, så der ikke stilles specifikke krav til kommunikationskanal.</p>

<b>Afsnit</b>	Kvalificeret person (9.17)
<b>Krav</b>	9.17-03
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>9.17-03 Særlig skal CA's øverste ledelse, andre ledende medarbejdere og medarbejdere i betroede roller, der beskæftiger sig med certifikatgenerering og spærring være fri for ethvert kommercielt, finansielt og andet pres"</p> <p>Kravet er upræcist, og derfor ikke muligt at overholde ift. medarbejdere. Der kan fx stilles konkrete krav til medarbejderes økonomi.</p>
<b>Svar</b>	Kravet kommer fra ETSI EN 319 411-1 og kravet afsluttes med "... som kan have negativ indflydelse på tilliden til de leverede

	<p>ydelser".</p> <p>Digitaliseringsstyrelsen mener, at det vil være problematisk hvis de omtalte personer IKKE er fri af et kommercielt, finansielt eller lignende pres, som kan have negativ indflydelse på tilliden til de leverede ydelser. Den valgte formulering fastholdes.</p>
--	---

### 3.2 Kvalificeret medarbejder (Bilag D4)

<b>Afsnit</b>	Kvalificeret medarbejder (1.6.1)
<b>Krav</b>	-
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>"Sikringsniveau ("Level of Assurance (LoA)")": Sikringsniveau afspejler graden af tillid til, at et elektronisk identifikationsmiddel kan fastslå identiteten på en fysisk eller juridisk person".</p> <p>Stemmer ikke med definitionen i NSIS. Sikringsniveau er graden af tillid til en autentificeret Identitet – ikke et identifikationsmiddel.</p>
<b>Svar</b>	Definitionen af "Sikringsniveau" tilrettes, så den stemmer overens med definition i NSIS.

<b>Afsnit</b>	Kvalificeret medarbejder (4.10.1)
<b>Krav</b>	4.10.1-12, 4.10.1-13
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>[KRAV 4.10.1-12] Levetiden for OCSP responder-certifikater for CA'er, der udsteder certifikater til certifikatholdere, skal være maksimal 72 timer og de tilhørende nøgler skal beskyttes af kryptografiske moduler på linje med øvrige CA nøgler, som angivet i afsnit 6.2.</p> <p>[KRAV 4.10.1-13] Levetiden for OCSP responder-certifikater for rod-CA skal være maksimalt 3 måneder og de tilhørende nøgler skal</p>

	<p>beskyttes af kryptografiske moduler på linje med øvrige CA nøgler, som angivet i afsnit 6.2.</p> <p>Høringspart anmoder om at kravet om at OCSP responderens nøgler beskyttes på samme niveau som CA'ens nøgler blødes op. De i markedet almindelige tilgængelige produkter for OCSP funktionalitet ligger på et lidt lavere niveau fx FIPS 140-3 level 2.</p>
<b>Svar</b>	<p>Grundet OCSP-servers mere online karakteristika er "på linje med øvrige CA nøgler" slettet for de to krav for alle certifikatpolitikker.</p> <p>Desuden tillades anvendelse af FIPS 140-2 level 3 til beskyttelse af OCSP-servers nøgler.</p>

<b>Afsnit</b>	Kvalificeret medarbejder (3.2.2)
<b>Krav</b>	3.2.2-02
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>KRAV 3.2.3-02] Certifikatholderens tilknytning til certifikatindehaver skal være sikret på NSIS sikringsniveau "betydelig" eller "høj" eller eIDAS sikringsniveau "betydelig" eller "høj".</p> <p>Det forekommer uhensigtsmæssigt at man kan vælge mellem NSIS og eIDAS, da der bør være overensstemmelse mellem disse.</p>
<b>Svar</b>	<p>NSIS er en dansk specifikation af sikringsniveauer som tager udgangspunkt i eIDAS sikringsniveauer, men ikke kun er rettet mod nationalt notificerede identitetssystemer.</p> <p>Digitaliseringsstyrelsen har et ønske om i videst muligt omfang at sikre interoperabilitet på tværs af EØS-lande, og derfor tillades både NSIS certificerede løsninger og nationale eIDAS-notificerede identitetssystemer.</p>

<b>Afsnit</b>	Kvalificeret medarbejder (4.4.1)
<b>Krav</b>	4.4.1-07
<b>Høringspart</b>	Nets

<b>Bemærkning</b>	<p>KRAV 4.4.1-07] CA skal registrere aftalen med certifikatindehaveren. Hvis certifikatindehaver og certifikatholder er forskellige fysiske eller juridiske personer, skal aftalen med certifikatholder også registreres.</p> <p>Skal der også indgås en formel aftale med certifikatholder? Normalt vil man vel blot have en aftale med certifikatindehaver som underretter certifikatholder om sine forpligtelser?</p>
<b>Svar</b>	Certifikatholder skal acceptere vilkår. Dette kan fx ske gennem en aktiv handling (klik i en checkboks) på en hjemmeside. Det er denne handling, der skal registreres.

<b>Afsnit</b>	Kvalificeret medarbejder (4.9.1)
<b>Krav</b>	4.9.1-01, 4.9.1-02
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>[KRAV 4.9.1-01] CA skal omgående og senest indenfor 12 timer spærre et kvalificeret certifikat udstedt under denne CP, hvis CA får kendskab til et eller flere af følgende forhold: h) Certifikatindehaverens virksomhed ophører.</p> <p>[KRAV 4.9.1-02] Hvis certifikatindehaver ændrer navn, skal CA omgående notificere certifikatindehaver om, at certifikatet skal fornyes inden for 30 dage. Sker dette ikke, skal CA spærre certifikatet.</p> <p>Der kan være behov for en overgangsperiode i disse situationer.</p>
<b>Svar</b>	<p>I forhold til KRAV 4.9.1-01 vurderer Digitaliseringsstyrelsen at certifikater for en ophørt virksomhed skal spærres og formulering i litra h) fastholdes.</p> <p>I forhold til KRAV 4.9.1-02 eksisterer certifikatholder stadig og certifikatet indeholder en entydig identifikation af certifikatindehaveren, der ikke er afhængig af certifikatindehaverens navn. Derfor vurderes det, at de 30 dages reaktionstid kan sættes op og formuleringen er ændret til 120 dage for alle erhvervsrelaterede certifikatpolitikker, hvilket bør give selv store organisationer tid til at planlægge og gennemføre en opdatering. Desuden er tilføjet en note vedrørende situationer, hvor certifikatindehaver beholder sit navn som binavn, hvilket betyder, at kravet ikke kommer i anvendelse jf. KRAV 3.1.2-01.</p>

<b>Afsnit</b>	Kvalificeret medarbejder (4.9.1)
<b>Krav</b>	4.9.1-01
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	Det forekommer at være meget langt tid til spærring af certifikater. Vi regner med, at der her regnes i minutter, da en spærring kan være kritisk.
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	Kvalificeret medarbejder (4.9.3)
<b>Krav</b>	4.9.3-02
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	<p>Vi finder indrapporteringsmulighederne ikke relevante.</p> <ul style="list-style-type: none"> <li>- Vi forventer, at der med "Fysisk post" menes et papirbrev formidlet og fragtet af en eller anden virksomhed til dette. Det mener vi ikke er relevant – bare af hensyn til tidsfaktoren.</li> <li>- Vi forstår Web, som indrapportering via en dedikeret web-portal med brug af relevant certifikatet og signering – eller brug af webservice med anvendelse af relevant certifikat.</li> <li>- Vi finder ikke, at telefonisk henvendelse kan give den rette sikkerhed – det vil kræve særlige procedurer for tilbageringning m.v. Vi finder ikke, denne mulighed relevant endsige sikker nok.</li> <li>- Brugen af offentlig Digital Post skal være en metode</li> </ul>
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	Kvalificeret medarbejder (4.10.2)
<b>Krav</b>	4.10.2-02



<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	Vi er enige i performancemålet 95% mindre end 1 sekund. Men vi vil også have mål for de resterende 5%; f.eks. 95% af de restende 5% mindre end 2 sekunder og ingen over 4 sekunder.
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	Kvalificeret medarbejder (5.1.1)
<b>Krav</b>	5.1.1-01
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>KRAV 5.1.1-01] CA skal tydeligt beskrive, på hvilke lokaliteter medarbejdere og datacentre i forbindelse med CA's virke er placeret. De lokaler, hvor udstyr til nøglegenerering er placeret, benævnes CA driftslokaler.</p> <p>Det bør defineres hvad de forskellige lokaliteter betyder.</p>
<b>Svar</b>	Der er foretaget en generel omskrivning i forhold til "lokaler", "driftslokaler" og "CA driftslokaler".

<b>Afsnit</b>	Kvalificeret medarbejder (5.4.3)
<b>Krav</b>	5.4.3-01, 5.4.3-02
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>KRAV 5.4.3-01] CA skal lagre log over alle livscyklushændelser relateret til CA's håndtering af nøgler, inklusiv eventuel håndtering af certifikatholderes nøgler i mindst syv år efter gyldighedsophør af ethvert certifikat relateret til loggen.</p> <p>[KRAV 5.4.3-02] CA skal lagre alle øvrige auditlogs i mindst løbende kalenderår + 5 år.</p> <p>Alle opbevaringstider bør ensrettes.</p>
<b>Svar</b>	Digitaliseringsstyrelsen har ensrettet alle opbevaringstider til mindst 7 år.

<b>Afsnit</b>	Kvalificeret medarbejder (8.2)
<b>Krav</b>	8.2-01
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	<p>[KRAV 8.2-01] CA skal vælge et eksternt overensstemmelsesvurderingsorgan til varetagelse af systemrevisionen hos CA. Overensstemmelsesvurderingsorganet skal enten være et overensstemmelsesvurderingsorgan defineret i eIDAS artikel 3 litra 18).</p> <p>Der mangler noget til denne beskrivelse og det er uvist om det ”bare” er en fejl fra copy-paste fra bilag D1?</p>
<b>Svar</b>	Der er tale om en fejl fra copy-paste. Dette vil blive rettet.

<b>Afsnit</b>	Kvalificeret medarbejder (8.3)
<b>Krav</b>	8.3-01
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	<p>[KRAV 8.3-01] Det valgte overensstemmelsesvurderingsorgan kan samarbejde med den interne revision hos CA'en.</p> <p>Organet skal vel samarbejde?</p>
<b>Svar</b>	Kravet er ændret til, at overensstemmelsesvurderingsorganet skal samarbejde med den interne revision.

<b>Afsnit</b>	Kvalificeret medarbejder (8.4)
<b>Krav</b>	8.4-02
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	[KRAV 8.4-02] CA skal kunne dokumentere opfyldelse af gældende lovgivning. Særligt i forhold til eIDAS og GDPR.

	Det [undrer (red.)] Skatteforvaltningen, at der ikke stilles krav til IT-kontroller med anerkendte standarder og rammeværk for sikkerhedskontroller fx SANS CIS?
<b>Svar</b>	Der stilles færre direkte krav til revision i de kvalificerede certifikatpolitikker end for de tilsvarende OCES certifikatpolitikker, da revision af kvalificerede tillidstjenester er reguleret gennem eIDAS (artikel 20).

### 3.3 Kvalificeret virksomhed (Bilag D5)

<b>Afsnit</b>	Kvalificeret virksomhed (4.9.1)
<b>Krav</b>	4.9.1-01
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	Det forekommer at være meget langt tid til spærring af certifikater. Vi regner med, at der her regnes i minutter, da en spærring kan være kritisk.
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	Kvalificeret virksomhed (4.9.3)
<b>Krav</b>	4.9.3-02
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	<p>Vi finder indrapporteringsmulighederne ikke relevante.</p> <ul style="list-style-type: none"> <li>- Vi forventer, at der med "Fysisk post" menes et papirbrev formidlet og fragtet af en eller anden virksomhed til dette. Det mener vi ikke er relevant – bare af hensyn til tidsfaktoren.</li> <li>- Vi forstår Web, som indrapportering via en dedikeret web-portal med</li> </ul> <p>brug af relevant certifikatet og signering – eller brug af webservice med anvendelse af relevant certifikat.</p>

	<p>- Vi finder ikke, at telefonisk henvendelse kan give den rette sikkerhed – det vil kræve særlige procedurer for tilbageringning m.v. Vi finder ikke, denne mulighed relevant endsige sikker nok.</p> <p>- Brugen af offentlig Digital Post skal være en metode</p>
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	Kvalificeret virksomhed (4.10.2)
<b>Krav</b>	4.10.2-02
<b>Høringspart</b>	Region Midtjylland - Danske Regioner
<b>Bemærkning</b>	Vi er enige i performancemålet 95% mindre end 1 sekund. Men vi vil også have mål for de resterende 5%; f.eks. 95% af de restende 5% mindre end 2 sekunder og ingen over 4 sekunder.
<b>Svar</b>	Se tidligere svar for MOCES.

<b>Afsnit</b>	Kvalificeret virksomhed (8.2)
<b>Krav</b>	8.2-01
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	<p>[KRAV 8.2-01] CA skal vælge et eksternt overensstemmelsesvurderingsorgan til varetagelse af systemrevisionen hos CA. Overensstemmelsesvurderingsorganet skal enten være et overensstemmelsesvurderingsorgan defineret i eIDAS artikel 3 litra 18).</p> <p>Der mangler noget til denne beskrivelse og det er uvist om det ”bare” er en fejl fra copy-paste fra bilag D1?</p>
<b>Svar</b>	Der er tale om en fejl fra copy-paste. Dette vil blive rettet.

<b>Afsnit</b>	Kvalificeret virksomhed (8.3)
---------------	-------------------------------

<b>Krav</b>	8.3-01
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	[KRAV 8.3-01] Det valgte overensstemmelsesvurderingsorgan kan samarbejde med den interne revision hos CA'en.  Organet skal vel samarbejde?
<b>Svar</b>	Se tidligere svar for Kvalificeret medarbejderpolitik.

<b>Afsnit</b>	Kvalificeret virksomhed (8.4)
<b>Krav</b>	8.4-02
<b>Høringspart</b>	Udviklings -og Forenklingsstyrelsen (UFST)
<b>Bemærkning</b>	[KRAV 8.4-02] CA skal kunne dokumentere opfyldelse af gældende lovgivning. Særligt i forhold til eIDAS og GDPR.  Det underer Skatteforvaltningen, at der ikke stilles krav til IT-kontroller med anerkendte standarder og rammeværk for sikkerhedskontroller fx SANS CIS?
<b>Svar</b>	Se tidligere svar for Kvalificeret medarbejderpolitik.

#### 4. Offentlig politik for kvalificeret tidsstempling (Bilag D6)

<b>Afsnit</b>	Offentlig politik for kvalificeret tidsstempling (7.2)
<b>Krav</b>	7.2-03
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>[KRAV 7.2-03] TSA bør gøre sine tjenester tilgængelige for alle, hvis aktiviteter falder inden for det angivne driftsområde og overholder deres forpligtelser som angivet i TSA's vilkår og betingelser.</p> <p>Denne bestemmelse bør præciseres yderligere.</p>
<b>Svar</b>	<p>Kravet bliver suppleret med en præciserende note:</p> <p>"TSA har mulighed for at begrænse driftsområdet for sine tjenester og TSA bør offentliggøre sit driftsområde i sin praksis. Eksempelvis kan TSA angive, at tidsstempler udelukkende udstedes til én angivet abonnent, men at tidsstempler fra TSA kan verificeres af alle modtagerparter."</p>

<b>Afsnit</b>	Offentlig politik for kvalificeret tidsstempling (7.6.7)
<b>Krav</b>	7.6.7-08
<b>Høringspart</b>	Nets
<b>Bemærkning</b>	<p>a) [KRAV 7.6.7-08] TSU's signeringsnøgler og enhver nøgledel, herunder eventuelle kopier, skal destrueres, så nøglerne ikke kan genskabes.</p> <p>Det bør angives hvor lang tid efter udløb at nøgler skal destrueres.</p>
<b>Svar</b>	<p>Digitaliseringsstyrelsen finder det ikke nødvendigt, at specificere, hvor lang tid efter udløb at nøgler skal destrueres, da det skal ske ved udløb. I praksis vurderes det, at dette sker som led i overgang til nye nøgler og dermed ofte inden nøglerne faktisk er udløbet.</p>