Certifikatpolitik for OCES-medarbejdercertifikater (Offentlige Certifikater til Elektronisk Service)

Indholdsfortegnelse

Rettigheder

IT- og Telestyrelsen har alle rettigheder til denne certifikatpolitik (CP), OCES-navnet og OCES-OID. Brug af betegnelsen OCES-OID i certifikater og udstedelse af OCES certifikater er kun tilladt efter skriftlig aftale med IT- og Telestyrelsen.

Forord

Denne certifikatpolitik er udarbejdet af og administreres af IT- og Telestyrelsen i Danmark.

IT- og Telestyrelsen er den offentlige myndighed, som bemyndiger udstedelsen af OCES-medarbejdercertifikater til de udvalgte certificeringscentre (CA'ere), og som står for godkendelse af CA'erne i forhold til denne CP.

IT- og Telestyrelsen er tillige ansvarlig for indholdet af denne CP. Den gældende version af denne CP findes på www.signatursekretariatet.dk .
Henvendelse i øvrigt vedrørende digital signatur til IT- og Telestyrelsen. Se nærmere www.digitalsignatur.dk.

Introduktion

En digital signatur er en elektronisk underskrift, som bl.a. kan bruges, når det er væsentligt at vide, hvem man kommunikerer med elektronisk. Anvendelsen af digital signatur forudsætter, at der er etableret en offentlig nøgleinfrastruktur (PKI).

OCES udgør en sådan offentlig nøgleinfrastruktur. OCES er betegnelsen for Offentlige Certifikater til Elektronisk Service. IT- og Telestyrelsen har udarbejdet tre OCES-certifikatpolitikker (CP'er), en for henholdsvis person-, medarbejder- og virksomhedscertifikater. CP'erne udgør en fælles offentlig standard, der regulerer udstedelsen og anvendelsen af den digitale OCES signatur. CP'erne fastsætter således krav til nøgleinfrastrukturen og herigennem sikkerhedsniveauet for den digitale signatur.

Den digitale signatur kan anvendes, når en person er blevet identificeret og registreret hos et certificeringscenter (CA). CA tildeler et personligt elektronisk certifikat, indeholdende personens offentlige nøgle. Desuden sørger CA for, at den nødvendige software, herunder den private nøgle, kan installeres på personens PC. CP'en stiller krav til, hvorledes og under hvilke vilkår, CA skal udføre disse opgaver.

Herudover findes kvalificerede certifikater udstedt i medfør af lov nr. 417 af 31. maj 2000 om elektroniske signaturer. Et kvalificeret certifikat bygger ikke på den oven for nævnte fælles offentlige standard. Der kræves bl.a. personligt fremmøde i forbindelse med udstedelsen af et kvalificeret certifikat.

1 Oversigt og formål

Denne certifikatpolitik (CP) beskriver de retningslinjer, der gælder for udstedelsen af et OCES-medarbejdercertifikat, hvor OCES er en forkortelse for Offentlige Certifikater til Elektronisk Service.

CP'en er udarbejdet med udgangspunkt i de retningslinjer, som er angivet i ETSI TS 102 042 v 1.2.1. (2005-05): *"Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*.

Et medarbejdercertifikat garanterer, at certifikatholderen har den identitet og er tilknyttet den virksomhed, der fremgår af certifikatet.

Et certifikat er kun et OCES-certifikat, hvis det er udstedt efter en OCES CP og er udstedt af et certificeringscenter (CA), som er godkendt af IT- og Telestyrelsen som udsteder af OCES-medarbejdercertifikater.

En CP er en del af aftalegrundlaget mellem IT- og Telestyrelsen og det enkelte certificeringscenter (CA) om ret til udstedelse af OCES-certifikater.

CP'en angiver en række betingelser, som CA skal opfylde for at opnå og bevare retten til udstedelse af OCES-certifikater.

Hovedprincippet for CP'en er således, at den udarbejdes af den for området hovedansvarlige offentlige myndighed, IT- og Telestyrelsen, og angiver styrelsens minimumskrav til de systemer og aftaler, som certificeringscentrene (CA'erne), som de kommercielle udbydere af certifikater, skal opfylde i forhold til deres "kunder", certifikatindehavere og signaturmodtagere, idet formålet er, at certifikatpolitikken skal sikre, at signaturerne kan bruges på en for alle parter betryggende måde.

Denne CP stiller ikke krav om krydscertificering og uafhængig tidsstemplingstjeneste hos CA.

2 Referencer

Opmærksomheden henledes på de nuværende regler:

LOV nr. 417 af 31/05/2000: *Lov om elektroniske signaturer*

LOV nr. 429 af 31/05/2000: *Lov om behandling af personoplysninger*

CEN Workshop Agreement 14167-2:2002: *"Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – part 2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)*"

DS 2391:1995 *"Registrering af identifikatorer I datanetværk"*, del 1 og 3

DS 844: *"Specifikation for kvalificerede certifikater"*

ETSI TS 102 042 v 1.2.1. (2005-05): *"Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*

ETSI SR 002 176 v 1.1.1. (2003-03): *"Algorithms and Parameters for Secure Electronic Signatures"*

FIPS PUB 140-1: "*Security Requirements for Cryptographic Modules*"

ISO/IEC 15408 (del 1 til 3): "*Information technology - Security techniques - Evaluation criteria for IT security*"

ISO/IEC 9794-8/ITU-T Recommendation X.509: *"Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*"

Såfremt der måtte være uoverensstemmelse mellem tekniske dokumenter eller standarder og denne CP, finder CP'ens bestemmelser anvendelse for CA.

3 Definitioner og forkortelser

3.1 Definitioner

Dette afsnit giver en definition af de specielle termer, som anvendes i denne CP. Engelske termer er angivet i parentes.

bemyndiget: Person, der af en tegningsberettiget fra virksomhedens ledelse er valgt og godkendt som kontaktperson, og som har bemyndigelse til på virksomhedens vegne at godkende og indsende certifikatansøgninger, og/eller administrere virksomhedens certifikater.

certifikat ("public key certificate"): En elektronisk attest, som angiver certifikatindehaverens offentlige nøgle sammen med supplerende information, og som entydigt knytter den offentlige nøgle til identifikation af certifikatindehaveren. Et offentligt certifikat skal signeres af et certificeringscenter (CA), som derved bekræfter certifikatets gyldighed.

certifikatindehaver ("subscriber"): En fysisk eller juridisk person, der indgår aftale med det udstedende certificeringscenter (CA) for en eller flere certifikatholdere.

certifikatholder ("subject"): En fysisk person, som i certifikatet er identificeret som den rette anvender af den private nøgle, der er associeret med den offentlige nøgle, der er givet i certifikatet, og til hvem et OCES certifikat enten er under udstedelse eller er blevet udstedt.

certificeringscenter ("certification authority" – "CA"): En fysisk eller juridisk person, der er bemyndiget til at generere, signere og udstede certifikater[1].

certificeringspraksis ("Certification Practice Statement" – "CPS"): En specifikation af hvilke principper og procedurer, en CA anvender ved udstedelse af certifikater.

certifikatpolitik ("certificate policy"): Et sæt regler, der angiver krav til udstedelse og brug af certifikat i en eller flere specifikke sammenhæng, hvor der findes fælles sikkerhedskrav.

digital signatur: Data i en elektronisk form, som anvendes til autentificering af andre elektroniske data, som den digitale signatur er vedhæftet eller logisk tilknyttet.

kryptografisk modul: Hardwareenhed som uafhængigt af styresystemet kan generere og opbevare nøgler og anvende den digitale signatur.

Medarbejder: person tilknyttet den virksomhed, der fremgår af certifikatet.

[1] I lov om elektroniske signaturer benyttes betegnelsen nøglecenter for denne enhed. Det er dog fundet mest praktisk at ændre terminologien. Et certificeringscenter svarer til et nøglecenter i lov om elektroniske signaturer, bortset fra at certificeringscenteret ikke udsteder kvalificerede certifikater, men OCES-certifikater.

offentligt certifikat ("public-key certificate"): Se certifikat.

registreringsenhed ("registration authority" – ”RA”): Den fysiske eller juridiske person, der er ansvarlig for identifikation og autentifikation af en (kommende) certifikatholder.

rodcertifikat ("root certificate"): Et offentligt certifikat udstedt af en CA til brug for validering af andre certifikater. Et rodcertifikat er signeret med sin egen signeringsnøgle (egensignering ("self signing")).

rodnøgle: rodcertifikatets signeringsnøgle (private nøgle).

signaturmodtager ("verifier "): En fysisk eller juridisk person, der modtager en elektronisk signatur, som er dannet ved signering af data fra en certifikatholder.

spærreliste ("Certificate Revocation List"): En liste over certifikater, som ikke længere anses for gyldige, fordi de er permanent spærret.

3.2 Forkortelser

CA Certificeringscenter ("Certificate Authority")
CRL Spærreliste ("Certificate Revocation List")
CPS Certificeringspraksis ("Certification Practice Statement")
CP Certifikatpolitik ("Certificate Policy")
CVR Central Virksomhed Register
LDAP "Lightweight Directory Access Protocol"
OCES Offentlige Certifikater til Elektronisk Service
OCSP "Online Certificate Status Protocol"
PKI "Public Key Infrastructure"
RA "Registration Authority"
UTC Fælles tidsangivelse ("Universal Time Coordinate")

3.3 Notation

Kravene anført i denne CP omfatter:

1 Obligatoriske krav, der skal opfyldes. Disse krav er anført med "skal".
2 Krav, der bør opfyldes. Opfyldes kravene ikke, skal der gives begrundelse herfor. Disse krav er anført med ”bør”.
3 Krav, der kan opfyldes, hvis CA ønsker det. Disse krav er anført med "kan".

4 Koncept

En Public Key Infrastruktur (PKI) benyttes til udveksling af information mellem to parter på internettet, hvor en fælles betroet tredjepart står inde for underskriverens identitet. En certifikatpolitik beskriver forholdet mellem disse tre parter.

Hovedprincippet for certifikatpolitikken er, som anført under pkt. 1, at den udarbejdes af den for området hovedansvarlige offentlige myndighed, IT- og Telestyrelsen. Certifikatpolitikken angiver styrelsens minimumskrav til de systemer og aftaler, certificeringscentrene (CA), som kommercielle udbydere af certifikater, skal opfylde i forhold til sine "kunder", certifikatindehavere og signaturmodtagere. Certifikatpolitikken skal sikre, at signaturerne kan bruges på en for alle parter betryggende måde. Certifikatindehavernes og signaturmodtagernes tillid skal således kunne baseres på IT- og Telestyrelsens godkendelse af CA'erne.

4.1 CA

En fysisk eller juridisk person, der er betroet af både certifikatindehavere og signaturmodtagere til at udstede, underskrive og administrere elektroniske certifikater, kaldes certificeringscenter (CA). CA har det overordnede ansvar for tilvejebringelsen af de tjenester, der er nødvendige for at udstede og vedligeholde certifikater. Det er CA's egne private nøgler, der benyttes til at underskrive udstedte certifikater, ligesom CA er identificeret i certifikatet som udsteder.

CA kan samarbejde med andre parter for at tilbyde de nødvendige tjenester, men CA har altid det overordnede ansvar for alle handlinger vedrørende håndtering af certifikater, ligesom CA er ansvarlig for, at kravene i denne CP til CA's tjenester altid er overholdt.

En OCES CA er øverst i tillidshierarkiet. Derfor vil OCES certifikater være signeret med en signeringsnøgle, som er selvsigneret, det vil sige rodnøglen i dette tillidshierarki.

4.2 CA-tjenester

De nødvendige tjenester for at udstede og vedligeholde certifikater kan opdeles i følgende:

- Registrering: Verificering af certifikatholderens identitet og eventuelle andre attributter. Resultatet af registreringen overgives til certifikatgenereringen
- Certifikatgenerering: Generering og elektronisk signering af certifikater baseret på den verificerede identitet og eventuelle andre attributter fra registreringen
- Certifikatdistribution: Distribution af certifikater til certifikatholdere
- Katalogtjeneste: Offentliggørelse af certifikater, så signaturmodtagere kan få adgang til certifikaterne
- Publikation af forretningsbetingelser: Offentliggørelse af betingelser og regler, herunder CP og CPS
- Spærring af certifikater: Modtagelse og behandling af anmodninger om spærring af certifikater

- Publikation af spærreinformation: Offentliggørelse af statusinformation for alle certifikater, specielt certifikater, der er spærret. Denne tjeneste skal være så realtidsnær som muligt

4.3 CP og CPS

4.3.1 Formål

Formålet med en CP som nærværende er at angive, hvilke krav der skal leves op til, mens formålet med en CPS er at angive, hvorledes der leves op til kravene hos den respektive CA. I certifikatet henvises til CP'en, således at en signaturmodtager kan tage stilling til, hvilke krav der som minimum er opfyldt gennem CA'ens CPS.

4.3.2 Specifikationsgrad

En CP er mindre specifik end en CPS, idet CPS'en angiver den detaljerede beskrivelse af forhold og betingelser, herunder forretnings- og driftsprocedurer for udstedelse og vedligeholdelse af certifikater.

CPS angiver, hvorledes en specifik CA opfylder de tekniske, organisatoriske og proceduremæssige krav identificeret i denne CP.

4.3.3 Forskelle

Indfaldsvinklen for CP og CPS er derfor ligeledes forskellig. En CP, som nærværende, er defineret uafhængig af specifikke detaljer i driftsmiljøerne hos CA'en, hvorimod CPS er skræddersyet til den organisatoriske struktur, driftsprocedurerne og IT-faciliteterne hos CA. Denne CP er udarbejdet af IT- og Telestyrelsen, mens CPS'en altid udarbejdes af en CA.

Da en CPS indeholder forretningsmæssige følsomme informationer, kan det ikke forventes, at hele CPS'en er offentligt tilgængelig. En uvildig tredjepart (systemrevisor) skal foretage en revision af CPS og skal erklære, at CPS overholder alle krav stillet i CP'en, samt at disse krav efterleves af CA.

4.3.4 Andre CA-betingelser

En CA vil typisk ud over CP og CPS'en have andre betingelser og vilkår. Dette vil normalt omfatte de kommercielle betingelser og vilkår, hvorunder CA udsteder certifikater og stiller statusinformation til rådighed.

4.4 Certifikatindehavere og certifikatholdere

Ved udstedelse af et medarbejdercertifikat indgår CA en aftale med certifikatindehaveren. Aftalen indgås mellem CA og virksomheden. I dette tilfælde vil certifikatindehaveren være virksomheden, mens medarbejderne, der får certifikaterne til brug, er certifikatholdere.

I denne CP benyttes begge termer for at skelne mellem den, der har indgået aftale med en CA, og den, der er identificeret som certifikatholder i certifikatet. Det er certifikatindehaveren, der har det endelige ansvar for brugen af certifikatet og de

tilhørende private nøgler, selvom det er certifikatholderen, der har kontrollen over den private nøgle.

Begrebet certifikatholder benyttes, hvor der eksplicit henvises til den, der er identificeret i certifikatet, mens begrebet certifikatindehaver benyttes i alle andre tilfælde, også hvor forskellen ikke klart fremgår af konteksten.

5 Introduktion til certifikatpolitik

5.1 Generelt

Dette dokument beskriver certifikatpolitik for OCES-medarbejdercertifikater.

5.2 Identifikation

Denne CP er identificeret ved den følgende "object identifier" (OID):

Medarbejdercertifikat:

{ 1 2 208 stat(169) pki(1) cp(1) nq(1) medarbejder(2) ver(4) }.

OID er registreret i Dansk Standard i overensstemmelse med DS 2391:1995, del 1 og 3.

Alle OCES-medarbejdercertifikater, der udstedes efter denne CP, skal referere til denne CP ved at angive den relevante OID i "certificate policy" – feltet i OCES-certifikatet. De nævnte OID'er må kun refereres i et certifikat efter skriftlig aftale med IT- og Telestyrelsen.

5.3 Anvendelsesområde

Et OCES-medarbejdercertifikat kan anvendes til sikring af afsender- og meddelelsesautencitet, herunder elektronisk signatur samt meddelelsesintegritet. Det kan også anvendes til at sikre hemmeligholdelse (kryptering).

OCES-medarbejdercertifikater er ikke kvalificerede certifikater, dvs. de må ikke bruges i situationer, hvor kvalificerede certifikater er påkrævet.

OCES-medarbejdercertifikater må ikke anvendes til signering af andre certifikater.

OCES-medarbejdercertifikater kan være gyldige i maksimum 4 år.

5.4 CA's ret til at udstede OCES-certifikater

CA kan udstede OCES-medarbejdercertifikater efter denne version af CP'en, hvis CA,

- har indgået skriftlig aftale med IT- og Telestyrelsen herom og
- har indsendt en rapport jf. 7.1. til IT- og Telestyrelsen, indeholdende en erklæring fra en ekstern systemrevisor. Revisionserklæringen skal godtgøre, at CA'en opfylder alle krav, der stilles i nærværende CP, samt har indført de kontroller, der er nødvendige for, at kravene til drift og sikkerhed til enhver tid kan overholdes og
- har modtaget en overensstemmelseserklæring fra IT- og Telestyrelsen, der bekræfter, at IT- og Telestyrelsen har godkendt den indsendte rapport og betragter kravene i nærværende CP som værende opfyldt.

6 Forpligtigelser og ansvar

6.1 CA's forpligtelser

CA skal sikre, at alle krav som er specificeret i afsnit 7, er implementeret.

Certificeringscentre (CA'er), der må udstede certifikater ifølge denne CP (OCES-medarbejdercertifikater), er offentliggjort på IT- og Telestyrelsens hjemmeside: https://www.signatursekretariatet.dk.

Der er ikke krav om krydscertificering mellem disse centre.

CA skal sikre varetagelsen af alle aspekter i forbindelse med:

- distribution af rodcertifikater
- anvisning af, hvorledes nøgler genereres og opbevares
- udsendelse af OCES-medarbejdercertifikater til certifikatindehavere
- spærring af OCES-medarbejdercertifikater efter anmodning
- publikation af spærrelister
- underretning af certifikatindehavere om snarligt udløb af gyldighed for certifikat og evt. fornyelse af nøglepar
- fornyelse af OCES-medarbejdercertifikater

CA skal opretholde et teknisk driftsmiljø, der overholder sikkerhedskravene i denne CP.

CA skal udfærdige en CPS, der adresserer alle krav i denne CP. CPS'en skal være i overensstemmelse med denne CP.

CA skal underkaste sig revisionskrav jf. denne CP.

Registreringsenheden (RA) kan enten være nøje knyttet til CA'en, eller den kan være en selvstændig funktion. CA hæfter under alle omstændigheder for RA's opfyldelse af de stillede krav og forpligtelser på ganske samme måde som for sine egne forhold.

CA skal sikre, at den eller de tilknyttede RA følger de bestemmelser, som er fastlagt i denne CP.

CA skal desuden sikre, at RA:

- etablerer en Web-adgang for registreringsprocedurer (kan være en del af CA'ens Web-tjeneste)
- verificerer ansøgerens identitet og oplysninger
- opretholder et teknisk driftsmiljø i overensstemmelse med kravene i denne CP

6.2 Certifikatindehaverens forpligtelser

CA skal ved aftale forpligte certifikatindehaveren til at sikre, at certifikatholder opfylder følgende betingelser:

- at give fyldestgørende og korrekte svar på alle anmodninger fra CA (eller RA) om information i ansøgningsprocessen
- at generere, opbevare og anvende nøglepar som anvist af CA. Den private nøgle kan opbevares på harddisk, diskette eller lignende
- at tage rimelige forholdsregler for at beskytte den private nøgle mod kompromittering, ændring, tab og uautoriseret brug
- at beskytte den private nøgle med en aktiveringskode, der mindst består af 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal
- anvendelse af anden aktiveringskode – f.eks. biometrisk – skal have en kompleksitet på mindst 128 bit
- aktiveringskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan dog være minimum fire cifre
- at beskytte aktiveringskoden, så andre ikke får kendskab til den
- at en evt. sikkerhedskopi af den private nøgle skal opbevares i krypteret form på betryggende vis
- ved modtagelse af OCES-certifikatet at sikre sig, at indholdet af OCES-certifikatet er i overensstemmelse med de faktiske forhold
- alene at benytte OCES-certifikatet og de tilhørende private nøgler i henhold til bestemmelserne i denne CP
- omgående at anmode den udstedende CA om spærring af OCES-certifikatet i tilfælde af kompromittering eller mistanke om kompromittering af den private nøgle
- omgående at anmode om fornyelse af certifikatet, hvis indholdet af OCES-certifikatet ikke længere er i overensstemmelse med de faktiske forhold

For så vidt angår private nøgler til brug for sikring af fortrolighed (krypteringsnøgler) kan certifikatindehaveren anvise certifikatholderen alternative procedurer til sikring af en fælles kontrol og anvendelse af nøgler. Certifikatindehaveren skal i givet fald informere certifikatholderen om konsekvenserne i forhold til fortrolighed.

Såfremt certifikatholder ikke længere har tilknytning til certifikatindehaver, skal certifikatindehaver omgående meddele CA dette og anmode om spærring af certifikatholderens certifikat.

CA skal desuden orientere certifikatindehaver og certifikatholder om, at den private nøgle anses for kompromitteret og skal spærres, hvis andre får kendskab til aktiveringskoden.

6.3 Information til signaturmodtagere

CA skal - bl.a. via sin hjemmeside - orientere signaturmodtagere om vilkår og betingelser for anvendelsen af digital signatur, herunder at tillid til et certifikat kræver, at signaturmodtager sikrer sig:

- at et modtaget certifikat er gyldigt og ikke spærret - dvs. ikke opført på CA's spærreliste
- at det formål, et certifikat søges anvendt til, er passende i forhold til anvendelsesbegrænsninger på OCES-certifikatet samt
- at anvendelsen af certifikatet i øvrigt er passende i forhold til niveauet af sikkerhed, som er beskrevet i denne CP.

6.4 Ansvar

CA skal, i forhold til den der med rimelighed forlader sig på certifikatet, påtage sig erstatningsansvar efter dansk rets almindelige regler.

CA skal desuden påtage sig erstatningsansvar for tab hos certifikatindehavere og signaturmodtagere, der med rimelighed forlader sig på certifikatet, såfremt tabet skyldes:

- at oplysningerne angivet i certifikatet ikke var korrekte på tidspunktet for udstedelsen af certifikatet
- at certifikatet ikke indeholder alle oplysninger som krævet i henhold til 7.3.3
- manglende spærring af certifikatet, jf. 7.3.6
- manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. 7.3.3 og 7.3.6, eller
- tilsidesættelse af 7.3.1,

medmindre CA kan godtgøre, at CA ikke har handlet uagtsomt eller forsætligt.

CA udformer selv sine aftaler m.v. med sine medkontrahenter. CA er berettiget til at søge at begrænse sit ansvar i forholdet mellem sig og sine medkontrahenter i det omfang disse medkontrahenter er erhvervsdrivende eller offentlige myndigheder. CA er således ikke berettiget til at søge at begrænse sit ansvar i forhold til private borgere som medkontrahenter.

CA er desuden berettiget til at fraskrive sig ansvar over for medkontrahenter, som er erhvervsdrivende og offentlige myndigheder, for tab af den i § 11, stk. 3, i lov nr. 417 af 31. maj 2000 beskrevne art.

Forsikring

CA skal tegne og opretholde en forsikring til dækning af eventuelle erstatningskrav mod CA og RA fra såvel alle medkontrahenter (certifikatindehavere og signaturmodtagere) som IT- og Telestyrelsen. Forsikringen skal som minimum have en dækning på kr. 2 millioner pr. år.

7 Krav til CA-praksis

7.1 Certificeringspraksis (CPS)

CA skal udarbejde en certificeringspraksis (CPS), der i detaljer beskriver, hvorledes kravene i denne CP opfyldes, herunder:

- CA's administrative og ledelsesmæssige procedurer
- kvalifikationer, erfaring, m.v. hos CA's personale
- de systemer og produkter, som CA anvender
- CA's sikkerhedsforanstaltninger og arbejdsproces i forbindelse hermed, herunder oplysninger om hvilke foranstaltninger, der gælder med hensyn til at opretholde og beskytte certifikaterne, så længe de eksisterer
- CA's procedurer vedrørende registrering (identitetskontrol), udstedelse af certifikater, katalog- og tilbagekaldelsestjeneste samt registrering og opbevaring af oplysninger vedrørende certifikater, herunder vedrørende identitetsoplysninger
- CA's økonomiske ressourcer
- CA's procedurer vedrørende indgåelse af aftaler om udstedelse af certifikater og dets oplysningsforpligtelser
- I det omfang CA har udliciteret CA-opgaver til andre virksomheder eller myndigheder, skal CPS'en ligeledes omfatte udførelsen af disse opgaver

CA-praksis skal til enhver tid være i overensstemmelse med det i CPS'en beskrevne.

Godkendelse og løbende revision

En CA, der ønsker at udstede OCES-medarbejdercertifikater, skal indgå skriftlig aftale med IT- og Telestyrelsen.

CA skal efter underskrivelsen af aftalen udarbejde og indsende en rapport til IT- og Telestyrelsen. Rapporten skal godkendes af IT- og Telestyrelsen og indeholde:

- CA's CPS
- revisionsprotokollen
- en erklæring fra CA's ledelse om, hvorvidt CA's samlede data-, system- og driftssikkerhed må anses for betryggende samt om, at CA opfylder sin egen CPS
- en erklæring fra systemrevisor om, hvorvidt CA's samlede data-, system- og driftssikkerhed efter systemrevisors opfattelse må anses for betryggende, samt at CA opfylder sin egen CPS
- Dokumentation for ansvarsforsikring, der dækker CA's ansvar

Rapporten skal efterfølgende indsendes årligt til IT- og Telestyrelsen. Dette skal ske senest tre måneder efter afslutningen af CA's regnskabsår. Rapportens tidsperiode skal følge regnskabsåret for CA.

Systemrevision

Der skal gennemføres systemrevision hos CA. Ved systemrevision forstås revision af:

- generelle edb-kontroller i virksomheden
- edb-baserede brugersystemer m.v. til generering af nøgler og nøglekomponenter samt registrering, udstedelse, verificering, opbevaring og spærring af certifikater og
- edb-systemer til udveksling af data med andre

Valg af systemrevisor - dennes beføjelser og pligter
CA skal vælge en ekstern statsautoriseret revisor til varetagelse af systemrevisionen hos CA. IT- og Telestyrelsen kan i særlige tilfælde dispensere fra kravet om, at systemrevisor skal være statsautoriseret revisor. CA skal senest en måned efter valg af systemrevisor anmelde dette til IT- og Telestyrelsen.

CA skal udlevere de oplysninger, som er nødvendige for systemrevisionen i CA. Herunder skal CA give den valgte systemrevisor adgang til ledelsesprotokollen.

CA skal give den valgte systemrevisor adgang til ledelsesmøder under behandling af sager, der har betydning for systemrevisionen. Ved ledelse forstås den øverste ledelse af CA, dvs. bestyrelse eller tilsvarende ledelsesorgan afhængigt af, hvorledes CA er organiseret. Ved et ledelsesmøde forstås et møde mellem den øverste ledelse af CA, i praksis ofte et bestyrelsesmøde. CA skal sikre, at den valgte systemrevisor deltager i ledelsens behandling af pågældende sager, såfremt det ønskes af blot ét ledelsesmedlem.

I CA'er, hvor der afholdes generalforsamling, finder årsregnskabslovens bestemmelser om revisionens pligt til at besvare spørgsmål på et selskabs generalforsamling tilsvarende anvendelse for den valgte systemrevisor.

CA skal gøre den valgte systemrevisor bekendt med, at denne i overensstemmelse med god revisionsskik skal foretage den nedenfor nævnte systemrevision, herunder at påse, at:

- CA's systemer er i overensstemmelse med kravene i denne CP
- CA's sikkerheds-, kontrol- og revisionsbehov tilgodeses i tilstrækkeligt omfang ved udvikling, vedligeholdelse og drift af CA's systemer
- CA's forretningsgange såvel de edb-baserede som de manuelle er betryggende i sikkerheds- og kontrolmæssig henseende og i overensstemmelse med CA's certificeringspraksis (CPS)

CA skal sikre, at der i forbindelse med systemrevisionen foretages en sårbarheds-vurdering af logningsproceduren.

Den valgte systemrevisor kan samarbejde med den interne revision hos CA, såfremt en sådan eksisterer.

I det omfang den valgte systemrevisor konstaterer væsentlige svagheder eller uregelmæssigheder, skal CA’s ledelse behandle sagen på næstkommende ledelsesmøde.

CA skal gøre den valgte systemrevisor bekendt med, at denne har pligt til at indberette forholdet eller forholdene til IT- og Telestyrelsen, såfremt systemrevisoren fortsat

mener, at der forekommer væsentlige svagheder eller uregelmæssigheder. CA skal desuden gøre systemrevisor bekendt med, at denne ved forespørgsler fra IT- og Telestyrelsen er forpligtet til at give oplysninger om CA's forhold, der har eller kan have indflydelse på CA's forvaltning af opgaven som udsteder af OCES-certifikater, uden forudgående accept fra CA. Systemrevisor er dog forpligtet til at orientere CA om henvendelsen.

CA og systemrevisor skal straks oplyse IT- og Telestyrelsen om forhold, der er af afgørende betydning for CA's fortsatte virksomhed.

Revisionsprotokol
CA skal gøre den valgte systemrevisor bekendt med, at denne løbende skal føre en særskilt revisionsprotokol, der skal fremlægges på ethvert ledelsesmøde, samt at enhver protokoltilførsel skal underskrives af CA's ledelse og den valgte systemrevisor.

CA skal desuden gøre systemrevisor bekendt med, at indholdet i protokollen skal være som anført nedenfor i dette afsnit.

I den valgte systemrevisors protokol skal der afgives beretning om den gennemførte systemrevision samt konklusionerne herpå. Der skal desuden redegøres for alle forhold, der har givet anledning til væsentlige bemærkninger.

I den valgte systemrevisors protokol skal det endvidere oplyses, hvorvidt denne under sit arbejde har modtaget alle de oplysninger, der er anmodet om.

Ved afslutningen af CA's regnskabsår udarbejder den valgte systemrevisor et protokollat til CA's ledelse.

Protokollatet skal indeholde erklæringer om, hvorvidt

- systemrevisionen er blevet udført i overensstemmelse med god revisionsskik
- den valgte systemrevisor opfylder de i lovgivningen indeholdte habilitetsbetingelser
- den valgte systemrevisor har fået alle de oplysninger, som den valgte systemrevisor har anmodet om
- de anførte systemrevisionsopgaver er udført ifølge denne CP's krav
- den samlede data-, system- og driftssikkerhed må anses for betryggende

IT- og Telestyrelsen kan pålægge CA inden for en fastsat frist at vælge en ny systemrevisor, såfremt den fungerende systemrevisor findes åbenbart uegnet til sit hverv.

Ved revisorskifte skal CA og den eller de fratrådte systemrevisorer hver især give IT- og Telestyrelsen en redegørelse.

Udgifter i forbindelse med systemrevision
CA skal afholde alle udgifter i forbindelse med systemrevision, herunder tillige systemrevision pålagt af IT- og Telestyrelsen.

7.2 Nøglehåndtering

CA's nøglehåndtering skal være i overensstemmelse med ETSI SR 002 176 v 1.1.1. (2003-03): *"Algorithms and Parameters for Secure Electronic Signatures"*, der definerer en liste over anerkendte kryptografiske algoritmer samt krav til deres parametre.

7.2.1 CA nøglegenerering

Generering af CA's rodnøgler og andre private nøgler skal ske under overvågning af to personer med hver sin betroede funktion i CA.

Generering af CA's private nøgler skal ske i kryptografisk modul, der opfylder kravene i FIPS 140-1 level 3, CWA 14167-2, eller højere. Det kryptografiske modul skal opbevares i henhold til kravene i 7.4.4.

Hvis CA's rodnøgler eller andre private nøgler skal overføres fra kryptografisk modul, skal dette ske i krypteret form og under medvirken af mindst to personer med forskellige betroede funktioner i CA.

Certifikatudsteders rodnøgler skal være RSA-nøgler af en længde på mindst 2048 bit eller tilsvarende. Certifikatudsteders rodnøgler skal være gyldige i mindst 5 år.

Betegnelsen "OCES" skal indgå i rodcertifikatets Common Name.

7.2.2 CA-nøglelagring, backup og genskabelse

CA skal sikre, at CA's rodnøgler ikke kompromitteres og til stadighed bevarer deres integritet.

Lagring, sikkerhedskopiering og transport af CA's rodnøgler og andre private nøgler skal ske under overvågning af to personer med hver sin betroede funktion i CA.

CA's rodnøgler og andre private nøgler skal opbevares og bruges i kryptografiske moduler, der opfylder FIPS140-1 level 3, CWA 14167-2, eller højere.

Sikkerhedskopier af CA's private nøgler skal opbevares i kryptografisk modul, der opfylder kravene i FIPS 140-1 level 3, CWA 14167-2, eller højere. Det kryptografiske modul skal opbevares i henhold til kravene i 7.4.4.

7.2.3 CA's publicering af den offentlige nøgle

CA's rodcertifikat skal gøres tilgængelig for signaturmodtagere ved Web-adgang med SSL-kommunikation. Verifikation af rodcertifikatets fingerprint (en kontrolværdi) skal ske via anden kanal.

7.2.4 Nøgleopbevaring og -genskabelse

CA skal sikre, at certifikatholderes private nøgler til afsender- og meddelelses-autencitet, herunder elektronisk signatur samt meddelelsesintegritet, ikke opbevares eller kan genskabes hos CA.

CA skal sikre, at certifikatholders private nøgler til sikring af hemmeligholdelse (kryptering) ikke opbevares eller kan genskabes hos CA uden certifikatindehaverens godkendelse.

CA skal sikre, at der ikke kræves en sådan godkendelse fra certifikatindehaverens side som forudsætning for udstedelse af OCES-medarbejdercertifikater.

CA skal sikre, at proceduren for udlevering af opbevarede eller genskabte nøgler aftales samtidig med, at certifikatindehaveren giver sin godkendelse til opbevaring og/eller genskabelse.

7.2.5 CA's brug af nøgler

CA skal sikre, at CA's private nøgler ikke bliver benyttet til andet formål end signering af certifikater og statusinformation om certifikater.

CA skal sikre, at certifikatsigneringsnøgler kun benyttes i fysisk sikrede lokaler i henhold til 7.4.4.

7.2.6 CA's afslutning af nøglebrug

CA's private nøgle skal have en fast gyldighedsperiode. Efter udløb skal den private nøgle enten destrueres på en sådan måde, at den ikke kan genskabes eller opbevares sådan, at den ikke kan tages i brug igen.

CA skal sikre, at der, inden udløb af den private nøgle, genereres et nyt CA-nøglepar, der benyttes til udstedelse af efterfølgende certifikater.

7.2.7 Håndtering af kryptografiske moduler

CA skal håndtere og opbevare kryptografiske moduler i henhold til kravene i 7.4 i hele de kryptografiske modulers levetid.

CA skal sikre sig, at kryptografiske moduler til certifikat og signering af statusinformation ikke er blevet kompromitteret inden installation.

CA skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering ikke bliver kompromitteret under brug.

CA skal sikre sig, at al håndtering af kryptografiske moduler til certifikat- og statusinformationssignering sker under medvirken af mindst to personer med hver sin betroede funktion i CA.

CA skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering altid fungerer korrekt.

CA skal sikre sig, at nøgler, opbevaret i et kryptografisk modul til certifikat- og statusinformationssignering, destrueres i forbindelse med, at modulet kasseres.

7.2.8 Generering af certifikatholders nøgler hos CA

CA skal sikre, at certifikatholders nøgler, som genereres af CA, genereres sikkert, og at hemmeligholdelsen af certifikatholderens private nøgler er sikret.

- Nøgler genereret af CA skal være RSA-nøgler med en længde på mindst 1024 bit eller tilsvarende
- CA genererede nøgler skal genereres og opbevares sikkert før leverance til certifikatholderen
- Certifikatholderens nøgler skal leveres på en sådan måde, at fortroligheden af nøglerne ikke kompromitteres
- Hvis der ikke skal opbevares en kopi af certifikatholderens nøgler hos CA, jf. 7.2.4, skal det ved leverance af nøglerne til certifikatholderen kun være certifikatholderen selv, som har adgang til den private nøgle. Alle kopier af certifikatholderens nøgler hos CA skal i så fald destrueres

7.3 Certifikathåndtering

7.3.1 Registrering af certifikatindehaver og certifikatholder

Registrering af certifikatindehaver

CA skal sikre, at certifikatindehaver, inden et OCES-medarbejdercertifikat tages i brug, gøres opmærksom på og accepterer vilkår og betingelser for anvendelsen af certifikatet.

Der er ikke krav om personligt fremmøde i forbindelse med udstedelsen af et OCES-medarbejdercertifikat.

CA skal etablere en procedure for verifikation af ansøgers identitet, der sikrer, at

- certifikatindehaveren angiver virksomhedens CVR-nr.
- OCES-certifikatindehaverens CVR-postadresse indhentes ved online opslag i CVR registeret i tilmeldingsprocessen
- den bemyndigedes engangskode fremsendes via pinkodebrev til virksomhedens ledelse på virksomhedens CVR-postadresse
- processen sker gennem en af virksomheden bemyndiget person, eller efter godkendelse fra en af virksomheden bemyndiget person
- bemyndiget er udpeget og godkendt af virksomhedens ledelse

Det er tilstrækkeligt, at CVR-postadressen verificeres én gang. Hvis virksomhedens adresse ændrer sig, skal CVR-postadressen verificeres på ny.

Såfremt CA på forhånd har kendskab til certifikatindehaverens identitet eller anvender andre betryggende procedurer til at foretage identitetskontrol, kan ovennævnte procedure for certifikatansøgning helt eller delvist fraviges.

Registrering af certifikatholder

CA skal etablere og opretholde en funktion, hvorigennem den bemyndigede kan foretage ansøgning om og udstedelse af medarbejdercertifikater. CA skal sikre, at registreringsprocessen sker gennem en af virksomheden bemyndiget person. Certifikatindehaver skal etablere en procedure for verifikation af certifikatholders identitet. CA skal etablere en procedure for verifikation af ansøgers identitet, der sikrer, at

- den bemyndigede angiver virksomhedens CVR nr.
- den bemyndigede angiver certifikatholders navn eller pseudonym
- OCES-certifikatholderen udstyres med en engangskode fremsendt via pinkodebrev til installation af den private nøgle og tilhørende certifikat eller
- OCES-certifikatholderen udstyres med en engangskode udleveret via den bemyndigede til installation af den private nøgle og tilhørende certifikat

Såfremt engangskoden udleveres til certifikatholderen af den bemyndigede, har certifikatindehaveren ansvaret for, at etablere en procedure, der sikrer,

- at udleveringen sker på betryggende vis,
- at certifikatholderen fysisk kvitterer for modtagelsen af engangskoden
- overfor udstederen at dokumentere at denne procedure følges
- og at der foretages audits heraf.

Såfremt CA på forhånd har kendskab til certifikatindehaverens identitet eller anvender andre betryggende procedurer til at foretage identitetskontrol, kan ovennævnte procedure for certifikatansøgning helt eller delvist fraviges.

Generering og installation af certifikatholders nøgler

Såfremt certifikatholders nøgler genereres hos certifikatholderen, skal CA etablere en installationsprocedure, der teknisk sikrer, at

- certifikatholder skal angive sin engangskode for at starte installation af den private nøgle og tilhørende certifikat
- nøglepar genereres hos certifikatholder
- certifikatholders nøgler er RSA-nøgler med en længde på mindst 1024 bit eller tilsvarende
- den offentlige nøgle overføres til CA sammen med oplysninger i en meddelelse signeret med den private nøgle
- den private nøgle er krypteret og beskyttet af aktiveringskode
- aktiveringskode til aktivering af den private nøgle genereres og indtastes i forbindelse med nøglegenereringen
- den private nøgle er aktiveret, når certifikatholderen har angivet aktiveringskode, der består af mindst 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal

- anvendelse af anden aktiveringskode – f.eks. biometrisk – skal have en kompleksitet på mindst 128 bit
- aktiveringskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan dog være minimum fire cifre
- rodcertifikatet er installeret hos OCES-certifikatholder
- rodcertifikatet kan verificeres via anden kanal
- tidspunkt og dato for udstedelsen af certifikatet efterfølgende kan fastlægges

Såfremt certifikatholders nøgler genereres af CA, jf. 7.2.8, skal CA etablere en procedure for overførsel og installation, som teknisk sikrer, at

- den private nøgle er krypteret og beskyttet af aktiveringskode
- den private nøgle og aktiveringskode leveres til certifikatholder i to forskellige forsendelser
- den private nøgle først aktiveres, når certifikatholderen har angivet aktiveringskode, der består af mindst 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal
- anvendelse af anden aktiveringskode – f.eks. biometrisk – skal have en kompleksitet på mindst 128 bit
- aktiveringskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan dog være minimum fire cifre
- rodcertifikatet kan verificeres via anden kanal
- tidspunkt og dato for udstedelsen af certifikatet efterfølgende kan fastlægges

CA skal understøtte, at generering og lagring af nøgler kan foregå ved brug af hardware. CA skal over for certifikatholdere anvise kryptografiske moduler til dette formål. Der er ikke angivet specifikke krav til OCES-certifikatindehaveres kryptografiske moduler.

CA skal efter anmodning om muligt anvise metode for certifikatindehaver til at lave evt. sikkerhedskopi af den private nøgle, således at den opbevares i krypteret form på betryggende vis.

RA skal godkende en certifikatansøgning, hvis:

- proceduren gennemføres som anvist
- ansøgeren kan verificeres via bemyndigede, og
- ansøgeren giver korrekt engangskode i højst 5 forsøg

CA skal sikre, at der fra det tidspunkt, RA har modtaget en certifikatansøgning og til nødvendig information for udstedelse af et certifikat er afsendt til certifikatansøgeren, over en løbende måned i gennemsnit maksimalt må gå en arbejdsdag, dog max. tre arbejdsdage.

7.3.2 Certifikatfornyelse og nøglefornyelse

Fornyelse af et OCES-certifikat betyder udstedelse af et nyt certifikat til den samme certifikatholder som i det eksisterende certifikat, men med en ny nøgle, ny

gyldighedsperiode, et nyt certifikat-serienummer og det gældende OID. Et OCES-certifikat må fornyes for fire år ad gangen.

Et certifikat kan efter anmodning fra certifikatholder og mod behørig identifikation kun blive fornyet, hvis certifikatholders nøglers gyldighedsperiode ikke er udløbet, og den private nøgle ikke er kompromitteret.

CA skal sikre, at anmodningen om fornyelse signeres med certifikatholderens private nøgle. Såfremt den bemyndigede gør indsigelse mod fornyelsen, må certifikatet ikke fornys.

CA skal godkende bevis for besiddelsen af den private nøgle tilhørende det eksisterende certifikat som værende tilstrækkelig autentifikation i det tilfælde, hvor et certifikat skal fornyes.
RA skal således sikre, at certifikatholder besidder den private nøgle, som svarer til den offentlige nøgle, som præsenteres i certifikatansøgningen. Det er tilstrækkeligt, at verifikationen sker ved, at den bemyndigede signerer certifikatansøgningen med sin private nøgle. Den verificerende RA skal validere signaturen vha. den offentlige nøgle givet i certifikatansøgningen.

Certifikatansøgning og -udstedelse skal opfylde kravene i afsnit 7.3.1 om generering og installation af certifikatholders nøgler, dog med undtagelse af udsendelse af engangskode, som ved fornyelse erstattes af validering med det eksisterende certifikat.

Efter spærring eller udløb, eller hvis den private nøgle er blevet kompromitteret, kan et certifikat ikke fornyes. CA skal i disse tilfælde sikre, at der kan ske udstedelse af nyt certifikat med ny nøgle, og at behandlingen af anmodning om nyt OCES-certifikat i dette tilfælde sker som ny udstedelse efter samme retningslinjer, som angivet i 7.3.1.

CA skal senest 14 dage før udløb notificere certifikatholderen via e-post til den i certifikatet angivne e-postadresse. Desuden skal CA samtidig hermed notificere den bemyndigede om udløb via e-post eller til virksomhedens CVR-postadresse.

CA skal sikre, at anmodning om og udstedelse af fornyet OCES-certifikat kan ske on-line.

7.3.3 Certifikatgenerering

OCES-medarbejdercertifikater skal benytte DS 844: Specifikation for kvalificerede certifikater, idet dog QcStatements ikke må angive, at der er tale om et kvalificeret certifikat.

OCES-medarbejdercertifikater skal indeholde:	***Løsning***
Den udstedende CA's identifikation og det land som certificeringscenteret er etableret i	Issuer-information indeholder den krævede information. Dvs. min. entydigt Navn og landekode
Certifikatholderens navn eller pseudonym; i sidstnævnte tilfælde skal det fremgå, at der er tale om et pseudonym	Common Name indeholder Navn og/eller pseudonym. Hvis der benyttes pseudonym, lægges pseudonymet tillige i Pseudonym-feltet.
Særlige oplysninger om certifikatholderen, der tilføjes, hvis det er relevant, afhængigt af formålet med certifikatet	Subject serialNumber og andre attributter indeholder informationen med passende kvalifikatorer. Se uddybning i ETSI TS 101 862 og RFC 3039. Formatet for Subject SerialNumber skal følge anvisningerne for medarbejdercertifikater i DS 844, pkt. 4.3
De signaturverificerings-data, som svarer til de signaturgenereringsdata, som er under underskriverens kontrol	X.509.v3.
Certifikatets ikrafttrædelses- og udløbsdato	X.509.v3 og RFC 2459.
Certifikatets identifikationskode	CA tildeler certifikatet et for CA'en unikt løbenummer. Sammen med CA's identifikation er nummeret totalt unikt. X.509.v3 og RFC 2459.
Den udstedende CA's avancerede elektroniske signatur	X.509.v3 og RFC 2459.
Eventuelle begrænsninger i certifikatets anvendelsesområde	KeyUsage, CertificatePolicies og Extended Key Usage.

Certifikatfeltet subject

I kolonnen "Krav" benyttes M for Mandatory (=krav) og O for Optional(=frivilligt).

Attribut	**Krav**	**Kommentarer**
countryName:	M	Landekode
organizationName:	M	Virksomhedens fulde navn, evt. inkl. CVR-nummer
organizationalUnitName:	O	Afdelingsbetegnelse
serialNumber:	M	CVR:cvrnummer-RID:medarbejderId.
postalAddress	O	Virksomhedens CVR-adresse
givenName:	O	Medarbejderens fornavne
surname:	O	Medarbejderens efternavn
commonName	M	Medarbejderens fulde navn eller registrerede pseudonym, evt. inkl. titel.
title	O	Medarbejderens stillingsbetegnelse
emailAddress	O	Medarbejderens e-postadresse
pseudonym	O	Medarbejderens pseudonym

Eksempel:
countryName=DK,
organizationName= ABC // CVR:12345678,
emailAddress=testesen@gyldigtdnsdomæne.dk,
serialNumber=CVR:12345678-RID:medarbejderId,
commonName= Projektleder Jens Madsen,
title="Projektleder"

Regler:
CountryName=DK, organizationName, organizationalUnitName, serialNumber, givenName, surname, commonName og **pseudonym** skal tilsammen entydigt udpege personen, der er holder af certifikatet. CVR-nummer skal være indeholdt i **serialNumber**.

Øvrige felter (extensions)

Versionsnummer skal være ”v3”.

Ved et kombineret certifikat, som skal anvendes til signering, autentifikation samt kryptering, skal **keyUsage** "extension" have de følgende specifikationer sat:

digitalSignature (0)
keyEnchipherment (2)
dataEncipherment (3)
keyAgreement (4)

contentCommitment specifikationen (**contentCommitment(1)**) kan, efter aftale med certifikatindehaver, sættes for, at certifikatet kan anvendes til at verificere signaturer, som har til hensigt at styrke uafviselighed og de som ikke har det.

Certifikater, der anvendes til autentifikation og signatur, skal have følgende specifikationer sat til:

digitalSignature (0)

contentCommitment specifikationen (**contentCommitment (1)**) kan, efter aftale med certifikatindehaver, sættes for, at certifikatet kan anvendes til at verificere signaturer, som har til hensigt at styrke uafviselighed og de som ikke har det.

Ved certifikater, der udelukkende anvendes til kryptering, skal følgende specifikationer sættes til:

keyEnchipherment (2)
dataEncipherment (3)
keyAgreement (4)

I alle tilfælde skal denne ekstension defineres som kritisk.

I de følgende oversigter anvendes disse koder:
O: Valgfri.("Optional")
C: Ekstension skal markeres kritisk ("Critical").
X: Ekstension må ikke markeres kritisk.
(C): Valgfrit for CA at markere ekstension som kritisk ("Critical").
R: Ekstension er krævet ("Required").
M: Håndtering af ekstension skal være tilstede ("Mandatory").
- : Ekstension har ingen mening.

Ekstension		Generering		
		Signatur		4. Key Man.
	1. Anvendelse	2. CA	3. Slut bruger	
AuthorityKeyIdentifier	O	O	O	O
SubjectKeyIdentifier	O	O	O	O
KeyUsage	CM	CMR	CMR	CMR
ExtendedKeyUsage	O	O	O	O
PrivateKeyUsagePeriod	O	O	O	O
CertificatePolicies	M	(C)MR	(C)MR	(C)MR
PolicyMappings	O	O	-	-
SubjectAltName	O	O	O	O
IssuerAltName	O	O	O	O
SubjectDirectoryAttributes	O	O	O	O
BasicConstraints	M	CMR	O	O
NameConstraints	O	O	-	-
PolicyConstraints	O	O	-	-
CRLDistributionPoints	M	R	R	R
QcStatements	O	O	O	O

Kommentarer til skemaet:
Håndtering af "extensions" er delt i 4 kolonner:
1. Software, der anvender udstedte certifikater.
2. Generering af certifikater til CA-software.
3. Generering af certifikater til slutbruger til brug for elektronisk signatur.
4. Generering af certifikater til slutbruger til brug for nøgle håndtering/udveksling, f.eks. i forbindelse med autentifikation / kontrol af adgangsrettigheder.

CertificatePolicies skal i det mindste angive de relevante "object identifiers" for denne CP.

Når CA har udstedt et certifikat, kan certifikatindehaveren notificeres ad anden kanal end benyttet i udstedelsesproceduren.

7.3.4 Publicering af vilkår og betingelser

CA skal orientere certifikatindehaver om, at OCES-medarbejdercertifikater ikke kan anvendes til signering af andre certifikater.

CA skal orientere certifikatindehaver om, at den private nøgle ikke må benyttes, førend OCES-certifikatet er modtaget af certifikatholderen, bortset fra den brug, der sker ved certifikatansøgningen.

CA skal orientere certifikatindehaver om, at den private nøgle ikke må benyttes til signering efter anmodning om spærring, notifikation om spærring eller efter udløb.

Desuden skal CA orientere certifikatindehaver om, at ved mistanke om at den private nøgle er kompromitteret, må denne kun anvendes til anmodning om spærring.

I begge tilfælde må den private nøgle dog stadig benyttes til dekryptering af data, der er krypteret med den tilhørende offentlige nøgle før spærring/mistanken om kompromittering.

I forbindelse med udstedelse af nye nøgler, herunder ved fornyelse, skal CA orientere certifikatindehaver om, at data krypteret med en offentlig nøgle, kun kan dekrypteres med den tilhørende private nøgle.

CA skal orientere certifikatindehaver om gyldighedsperioden for et OCES-medarbejdercertifikat og om, at et OCES-medarbejdercertifikat kan fornyes, hvis det gøres inden certifikatet udløber.

7.3.5 Publicering af certifikater

CA skal gøre følgende typer af information tilgængelig for alle:

- det rodcertifikat, der anvendes for udstedelse af certifikater ifølge denne CP, samt rodcertifikatets "fingerprint" ad anden kanal
- andre certifikater, der anvendes for signering af information mellem CA og certifikatindehavere og signaturmodtagere
- denne CP, så længe der er gyldige certifikater udstedt efter denne CP og så længe, der er certifikater på spærrelisten for denne CP
- den af systemrevisor godkendte CPS, med undtagelse af forretningshemmeligheder
- alle OCES-medarbejdercertifikater i mindst to måneder efter udløb af gyldighedsperiode, undtagen de certifikater, som skal holdes hemmelige
- spærreliste for OCES-medarbejdercertifikater udstedt efter denne CP.

Spærrelisteinformation skal være tilgængelig for læsning uden nogen form for adgangskontrol.

CA skal sikre, at de krav, CA stiller til certifikatindehaver og signaturmodtager på baggrund af denne CP uddrages og dokumenteres, jf. afsnit 6.2 og 6.3.

7.3.6 Certifikatspærring

CA skal omgående spærre et OCES-certifikat, hvis CA får kendskab til, at:

- der er vished eller mistanke om, at certifikatholderens private nøgle er kompromitteret
- den private nøgle er ødelagt
- certifikatholder ikke længere har tilknytning til certifikatindehaveren
- der er konstateret unøjagtighed i certifikatets indhold eller anden information knyttet til certifikatindehaveren/holderen
- certifikatholderen ønsker at afslutte brugen af OCES-certifikatet
- certifikatindehaveren ønsker at afslutte brugen af OCES-certifikatet
- certifikatindehaveren er gået konkurs

CA bør spærre et certifikat, hvis CA får kendskab til, at:

- certifikatholderen har mistet adgang til den private nøgle, f.eks. som følge af bortkommen aktiverings-kode

CA's misligholdelse af CP giver ikke CA ret til at spærre et certifikat.

CA skal sikre, at en anmodning om spærring af certifikat i videst mulig omfang sker ved angivelse af specifik tilbagetrækningskode tildelt af CA'en ved udstedelsen eller ved signering med certifikatholderens private nøgle.

Er tilbagetrækningskoden eller den private nøgle bortkommet eller ikke tilgængelig, skal CA sikre, at identifikationen sker på en måde, der sikrer identiteten bedst muligt f.eks. ved en kombination af navn, CVR-postadresse og e-postadresse.

De følgende kan anmode om spærring af certifikat:

- certifikatholder mod behørig dokumentation
- bemyndigede mod behørig dokumentation
- CA, hvis reglerne i denne CP ikke er overholdt, eller hvor forholdene i øvrigt tilsiger dette
- tegningsberettigede i virksomheden mod behørig dokumentation
- tilsyn eller kurator, såfremt certifikatindehaver har anmeldt betalingsstandsning eller tages under konkursbehandling

CA skal sikre, at proceduren for anmodning om spærring så vidt muligt ikke tillader, at der foretages uautoriserede spærringer samtidig med, at autoriserede spærringer tilgodeses via telefonisk henvendelse, via e-post eller via Web-adgang.

CA skal sikre, at der ved telefonisk spærring angives information som angivet ovenfor plus årsag til spærring. CA skal kvittere for spærring via signeret e-post til den oplyste e-postadresse. Certifikatholder kan kræve, at kvitteringen sendes med almindelig post.

CA skal ved anmodning via e-post sikre sig, at e-posten er signeret med den private nøgle. CA skal kvittere for spærring via signeret e-post. Certifikatholder kan kræve, at kvitteringen sendes med almindelig post.

CA skal sikre, at der ved anmodning via Web angives årsag til spærring, og at web-formularen signeres med den private nøgle eller angivelse af tildelt spærringskode.

CA skal kvittere for spærring via signeret e-post, om muligt sendt til den e-postadresse som er angivet i certifikatet, og ellers med almindelig post. Certifikatholder kan kræve at kvitteringen sendes med almindelig post.

Hvis CA foretager spærring uden at være anmodet om det, skal CA sende meddelelse med angivelse af årsag til spærring via signeret e-post til certifikatholder og til den bemyndigede. Samtidig skal CA sende meddelelse til den officielle postadresse som anført i CVR-registeret.

I tilfælde af konkurs kan anmodningen om spærring ske af skifteret eller kurator. Ovennævnte metoder kan ligeledes anvendes. CA skal dog ligeledes sende kvittering for spærring til den af skifteretten hhv. kuratoren angivne postadresse.

CA skal sikre, at der, efter at en anledning til spærring er konstateret, anmodes om spærring uden ugrundet forsinkelse.

CA skal sikre, at spærring sker umiddelbart efter anmodning er modtaget og eventuelt bekræftelse for anmoderens identitet er sket.

CA skal offentliggøre opdateret spærreliste samtidig med, at der udsendes kvittering for spærring af certifikat. Dette skal ske senest 1 minut efter, spærring er sket.

CA skal sikre, at der er en separat spærreliste for OCES-certifikater.

CA skal som minimum offentliggøre en ny spærreliste hver 12. time.

CA skal gøre spærrelister tilgængelige for download via LDAP og HTTP som CRL-fil samt for manuelt opslag fra Web browser.

Et OCES-certifikat kan ikke suspenderes. Ved mistanke om kompromittering af den private nøgle, skal CA sikre, at certifikatet spærres.

CA skal sikre spærrelister mod kompromittering, og at spærrelisterne og OCSP-tjenester er tilgængelige via internet daglig mellem klokken 0 og 24. Tjenesterne skal have en gennemsnitlig svartid, der ikke overstiger 1 sekund målt på serverindgang – dvs. fra serveren har registreret forespørgslen, til den returnerer et svar.

For Spærrelister skal CA benytte en profil som angivet i IETF RFC 3280. **thisUpdate** og **nextUpdate** skal angives i **UTCTime** format YYMMDDHHMMSSz.

Versionsnummer skal være angivet og sættes til "v2". Der er ikke krav om benyttelse af CRL-extensions.

En CA kan tillige tilbyde online (F.eks. via Online Certificate Status Protocol, OCSP) kontrol af status.

CA skal sikre, at svaret er elektronisk signeret og indeholder OCES-certifikatets unikke identifikationsnummer, status for certifikatet samt tidspunktet for svaret angivet i UTC-format med en nøjagtighed på 1 sekund.

For OCSP skal CA benytte en profil i overensstemmelse med IETF RFC 2560.

thisUpdate feltet må højst være 1 minut ældre end **producedAt** feltet. Begge felter angives i **generalizedTime.**

Version 1 skal understøttes. Der er ikke krav om benyttelse af OCSP-extension.

OCSP-tjenester og spærrelister skal være tilgængelige via internet dagligt mellem klokken 0 og 24. Tjenesterne skal have en gennemsnitlig svartid på Internet, der ikke overstiger 1 sekund målt på serverindgang – dvs. fra serveren har registreret forespørgslen til, den returnerer et svar.

7.4 CA styring og drift

7.4.1 Sikkerhedsimplementering

CA skal sikre, at dens administrative og ledelsesmæssige procedurer er tilstrækkelige og lever op til anerkendte standarder.

CA skal gennemføre en risikoanalyse af de forretningsmæssige risici og indføre de nødvendige sikkerhedstiltag samt driftsmæssige procedurer.

CA skal påtage sig det fulde ansvar for alle tjenester, der stilles direkte eller indirekte til rådighed for håndteringen af certifikatudstedelsen og statusinformationen.

CA skal implementere en IT-sikkerhedsorganisation, der til enhver tid skal have ansvaret for en sikkerhedsmæssig korrekt drift af CA's funktioner.

CA skal sikre, at personer med auditørfunktioner hos CA ikke personalemæssigt refererer til samme ledelse som driftsansvarlige og administratorer.

IT-sikkerheden i CA skal defineres i henhold til internationalt anerkendte standarder og være underlagt IT sikkerhedsorganisationens tilsyn.

De sikkerhedskontroller og driftsprocedurer, der gælder for CA’s lokaliteter, systemer og data vedrørende certificeringstjenester, skal være dokumenteret, implementeret og skal løbende vedligeholdes.

I tilfælde, hvor ansvaret for CA’ens certificeringsfunktioner outsources til en anden organisation eller enhed, skal CA sikre, at informationssikkerheden opretholdes tilsvarende.

7.4.2 Identifikation og klassifikation af IT-aktiver

CA skal gennemføre en risikoanalyse af alle IT-aktiver, hvor sårbarheder listes.

De enkelte IT aktiver skal klassificeres i henhold til deres betydning for driften af CA's primære funktioner og i overensstemmelse med den gennemførte risikoanalyse.

7.4.3 Personalesikkerhed

Krav til kvalifikationer, erfaring og sikkerhedsklassifikation
Personer med betroede funktioner hos CA, herunder også systemrevisor, skal have verificerede kvalifikationer inden for deres ansvarsområde og mindst 1 års erfaring.

Alle personer med ledelsesfunktioner hos CA skal være bekendte med sikkerhedsprocedurer for ansatte med sikkerhedsansvar samt have erfaring i IT-sikkerhed og risikovurdering.

Procedurer for sikkerhedsklassifikation
CA skal kontrollere, at ledere og medarbejdere, der skal udføre betroede opgaver i eller for CA, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv.

Krav til uddannelse
Alle personer med betroede funktioner hos CA skal have en for deres arbejdsområde relevant uddannelse eller træning. CA's ledelse er ansvarlig for, at hver medarbejder er egnet til det pågældende hverv.

Krav om og hyppighed af opdatering af kvalifikationer
Generelt
Relevante kvalifikationer hos medarbejdere i CA skal opdateres, hvis de ikke har været anvendt i de seneste fire år.

CA-driftspersonale
CA-driftspersonale skal opdatere deres viden en gang årligt.

Procedure for håndtering af uautoriserede handlinger
Der skal etableres klare procedurer for håndtering af enhver form for uautoriserede handlinger. Procedurerne skal være udmeldt til alle personer med betroede funktioner hos CA.

Kontrol af underleverandører
CA skal sikre, at personale hos underleverandører opfylder samme krav til uddannelse, erfaring og sikkerhedsklassifikation som CA's egne medarbejdere i de funktioner, underleverandørens personale varetager.

CA skal ved adgangsprocedurerne sikre, at personale hos underleverandører ikke kan arbejde uovervåget noget sted hos CA.

Dokumentation til brug for personale
CA skal dokumentere og gøre alle procedurer, regler og sanktioner tilgængelige for personalet i CA. CA's ledelse skal kunne dokumentere, at alt personale er blevet gjort bekendt med procedurer, regler og sanktioner.

7.4.4 Fysisk sikkerhed

Generelt
CA skal beskrive klart, på hvilken lokalitet man har placeret medarbejdere og datacentre i forbindelse med CA's virke. De lokaler, hvor udstyr til nøglegenerering er placeret, benævnes CA driftslokaler.

Alle lokaler, der benyttes til medarbejdere i CA, skal være defineret som særligt sikkerhedsområde i henhold til DS 484:2005.

CA driftslokaler
CA driftslokaler skal defineres til et sikkerhedsniveau og overholde kravene i DS 484:2005.

CA driftslokalet skal være fysisk adskilt fra CA's øvrige lokaler

I tilfælde af evakuering skal CA's driftslokaler kunne fungere med uændret drift via fjernbetjening. Ved fjernbetjening forstås mulighed for f.eks. via en PC at betjene CA-funktionerne fra et fra CA-driften fysisk adskilt lokale, f.eks. hvor CA har etableret reservesystem.

CA's driftslokaler skal beskyttes mod indtrængende luftforurening, røg og radioaktivt nedfald.

Fysisk adgang
Generelt
CA skal sikre, at alle lokaler har en perimeterbeskyttelse svarende til DS 471 eller bedre.

CA skal sikre, at adgang til og ophold i centrale driftslokaler er begrænset til specifikke personalekategorier ved elektronisk adgangskontrol.

CA skal sikre, at der etableres vagt 24 timer i døgnet.

CA-driftslokaler
CA skal sikre, at adgang til og ophold i de centrale driftslokaler videoovervåges.

Elforsyning og luftkonditionering
CA skal beskytte elforsyningen mod udfald. Beskyttelsen skal dække alle driftssystemer samt alt telekommunikationsudstyr placeret hos CA.

CA-driftslokaler

CA skal dublere og beskytte luftkonditionering i CA-driftslokaler mod elforsyningsudfald.

CA skal beskytte luftkonditionering mod forurening, røg og radioaktivt nedfald via luftindtaget.

Vandtryk
Generelt
CA skal foretage sikring mod vandindtrængning og rørlækager.

CA-driftslokaler
CA skal sikre, at der ikke forekommer vandinstallationer i CA-driftslokaler, ej heller må vandinstallationer føres gennem CA-driftslokaler.

CA skal implementere detektering af vand i CA-driftslokaler og alarmering i forbindelse hermed.

Forebyggelse af og beskyttelse mod brand
Generelt
CA skal installere automatisk brandalarmeringsanlæg

CA-driftslokaler
CA skal etablere de enkelte funktionsrum som separate brandceller.

CA skal endvidere installere automatisk brandslukningsanlæg.

Opbevaring af lagringsmedie
CA skal etablere arkiver for opbevaring af lagringsmedier med sikkerhedskopierede data og programmer i separate, funktionsadskilte celler.

Affaldshåndtering
Generelt
CA skal sikre, at affald, der indeholder fortrolig information, betragtes som fortroligt materiale og destrueres på forsvarlig vis.

CA-driftslokaler
CA skal sikre, at affald fra CA-driftslokaler behandles særskilt og destrueres, inden det fjernes fra området.

Reservesystem på anden lokalitet
Etablerer CA evt. reservesystemer på anden lokalitet, skal CA sikre, at disse opfylder samme krav som hovedsystemer. Såfremt reservesystemer etableres skal CA sikre, at det sker fysisk så langt fra hovedsystemet, at risikoen for kumulative nedbrud er minimeret.

7.4.5 Styring af IT-systemers og netværks drift

CA skal definere hvilke betroede funktioner der haves, og der skal udarbejdes en beskrivelse af hver betroede funktions ansvarsområde i CA.

Generelt

CA skal sikre, at der medvirker mindst to personer med forskellige betroede funktioner hos CA ved alle opgaver, hvor der er mulighed for ændring i opsætninger og funktionalitet.

CA skal sikre, at alt IT-udstyr og data sikres mod vira, fejlbehæftet og uautoriseret software.

CA skal søge at minimere skader som følge af sikkerhedsbrud og fejl ved hjælp af hændelsesrapportering og procedurer for umiddelbar opfølgning.

CA skal sikre, at alle benyttede medier beskyttes mod skade, tyveri og uautoriseret brug.

CA skal sikre, at følsomme data ikke kan genskabes via kasserede medier.

CA-driftslokaler

CA skal sikre, at der medvirker mindst to personer med forskellige betroede funktioner hos CA ved alle opgaver i CA-driftslokaler.

CA skal sikre, at medarbejdere i hver betroet funktion kan identificeres entydigt ved tydelig billeddokumentation.

CA skal sikre, at adgang til systemer knyttes til hver enkelt betroet funktion. Hvor der er krav om flere personers adgang til systemer, skal CA sikre, at dette understøttes teknisk i størst mulig omfang.

7.4.6 Kontrol af adgang til systemer, data og netværk

CA skal sikre, at alt benyttet IT-udstyr er sikkert og driftes korrekt med et minimum af fejlmuligheder.

CA skal gennem opstillede regler og ved tekniske foranstaltninger begrænse adgangen til CA-systemerne til et absolut minimum.

CA skal begrænse eksterne personers adgang til CA-systemerne mest muligt.

CA's interne netværk skal være beskyttet mod andre netværk med korrekt konfigurerede firewalls.

CA skal sikre, at følsomme data beskyttes, når de udveksles over netværk. Normalt ved brug af kryptering.

CA skal sikre, at administration af brugerrettigheder til systemerne er beskrevet i skriftlige instrukser, at alle ændringer i rettigheder skal logges, og der skal føres kontrol med disse logs.

CA skal sikre, at alle systemer understøtter en stringent kontrol med adgang til data og forhindrer utilsigtet udveksling på tværs af betroede funktioner hos CA.

CA skal sikre, at adgang til systemer kun opnås efter korrekt identifikation fra den enkelte ansatte.

CA skal sikre, at der udpeges en ansvarlig for tildeling af adgange til ethvert system. CA skal desuden sikre, at tiltag i tilfælde af uregelmæssigheder er klargjort for den enkelte ansatte.

Driftslokaler
CA skal sikre, at alle netværks komponenter er placeret i fysisk sikrede lokaler i henhold til 7.4.4, samt at netværkskomponenternes konfiguration revideres periodisk.

CA skal sikre, at alle IT-komponenter i driftslokaler konstant er overvåget, og at der er alarmer for alle forsøg på adgang til og ændring af konfigurationer og data.

CA skal sikre, at der er alarmer for alle uautoriserede ændringer i data vedrørende certifikater og tilhørende information samt statusinformation.

7.4.7 Udvikling, anskaffelse og vedligeholdelse af IT-systemer
CA skal benytte anerkendte systemer og produkter, som er beskyttet mod ændringer. Produkterne skal overholde en tilstrækkelig beskyttelsesprofil i henhold til ISO/IEC 15408 eller tilsvarende.

Ved egen udvikling skal CA sikre, at der foreligger en ledelsesgodkendt plan for indbygning af sikkerhed i systemerne. Dette gælder også ved bestilt udviklingsarbejde.

CA skal sikre, at der etableres kontrolprocedurer for nye versioner, ændringer og reservesystemer

7.4.8 Beredskabsplanlægning
Følgende hændelser skal betragtes som alvorlige:

- Kompromittering af CA's private nøgle
- Mistanke om kompromittering af CA's private nøgle
- Nedbrud og kritiske fejl på CA-driftskomponenter (spærrelister etc.)
- Stop af CA-driftsmiljøet som følge brand, elforsyningssvigt osv.

CA skal sikre, at der foreligger en beredskabsplan, der kan bringe CA's drift tilbage til normal hurtigst muligt, efter at en alvorlig hændelse er indtrådt. Beredskabsplanen skal herefter revideres med henblik på at undgå, at lignende hændelser gentages.

CA skal i tilfælde af kompromittering af CA’s private nøgle eller mistanke herom informere alle certifikatindehavere og IT- og Telestyrelsen herom. I det omfang, det

er muligt, skal signaturmodtagere informeres. Det kan for eksempel ske igennem offentlige medier og ved annoncering i dagspressen.

CA skal i tilfælde af alvorlige hændelser på databehandlingsudstyr, programmel og/eller data orientere certifikatindehavere herom i det omfang, det er relevant for deres brug af CA-tjenesterne. Så vidt muligt skal signaturmodtagere informeres. Det kan for eksempel ske igennem offentlige medier og ved annoncering i dagspressen.

CA skal sikre, at alle procedurer omkring spærrelister, herunder anmodning om spærring, har højeste prioritet i forbindelse med retablering af forretningsgange.

7.4.9 Ophør af CA

CA skal sikre, at al udstedelse og fornyelse af certifikater straks stoppes, når en CA-funktion vil ophøre med at fungere.

CA skal sikre den fortsatte operationelle drift af spærrelister og anmodninger om spærringer, indtil alle certifikater udstedt af denne CA er udløbet eller eventuelt overdraget til anden CA, der opfylder kravene i denne CP.

CA skal sikre, at arkiver er tilgængelige i mindst 6 år efter udløb af sidste certifikat udstedt af denne CA.

7.4.10 Overensstemmelse med lovgivningen

CA skal sikre overensstemmelse med lovgivningsmæssige krav særligt i relation til persondata.

Særlige forpligtelser med henblik på beskyttelse af fortrolig information

Information, som indgår i certifikater, anses som ikke fortrolig.

Personrelateret information, som ikke indgår i certifikatet, anses som privat information.

Information, som indgår i certifikater, anses som værende ikke privat.

CA skal sikre, at fortrolig information er beskyttet mod kompromittering og må ikke benytte fortrolig information til andet, end hvad der er påkrævet for driften af CA'en.

CA skal sikre, at privat information er beskyttet mod kompromittering og må ikke benytte privat information udover, hvad der er påkrævet for drift af CA'en.

CA skal sikre, at statistiske oplysninger om anvendelse af OCES-medarbejdercertifikater ikke kan henføres til det enkelte OCES-certifikat (jf. persondataloven).

I tilfælde af tvistigheder, som ikke kan løses ved forhandling mellem parterne, er almindelig dansk ret gældende.

7.4.11 Opbevaring af certifikatinformation

CA er ansvarlig for etablering af et datalagringssystem, der skal indeholde alle data, der er nødvendige for sikker drift af CA i overensstemmelse med denne CP. CA skal desuden sikre, at:

- Al anden information beskyttes mod uretmæssig adgang
- Alle aktiviteter, der kræver deltagelse af mere end en person, logges
- Alle informationer om registrering, herunder certifikatfornyelser, logges
- Alle adgange og adgangsforsøg til områder, der skal beskyttes af adgangskontrol, logges
- Al videoovervågning logges
- Der er skriftlige regler for regelmæssig gennemgang af alle logs
- Alle audit-logs signeres elektronisk og tidsstemples
- Audit-logs behandles som fortroligt materiale
- Der foretages backup af audit-logs med regelmæssige mellemrum

CA skal sikre, at backup-medier opbevares i overensstemmelse med kravene i 7.4.4 i medie-brandskab.

CA skal sikre, at IT- og Telestyrelsen informeres om væsentlige uregelmæssigheder i logningsproceduren samt notificeres en gang årlig i alle andre tilfælde.

CA skal sikre, at følgende information arkiveres:

- Alle logs
- Certifikatanmodninger og tilhørende kommunikation
- Signerede ordrer og skriftlig aftaler
- Certifikatfornyelser
- CPS og CP

CA skal sikre, at arkiveret information kan gøres tilgængelig i tilfælde af tvister, og at alt arkiveret materiale opbevares i mindst 6 år.

CA skal sikre, at alt materiale i arkiv opbevares i overensstemmelse med kravene i afsnit 7.4.4.

CA skal sikre, at alt elektronisk arkivmateriale sikkerhedskopieres med regelmæssige mellemrum.

CA skal sikre, at alt elektronisk arkivmateriale påføres elektronisk tidsstempling på arkiveringstidspunktet. Andet arkivmateriale indføres i en log.

7.5 Organisatoriske aspekter

CA's organisation skal være pålidelig.

CA skal være en registreret fysisk eller juridisk person.

CA skal sikre, at alle tjenester tilbydes til alle indenfor OCES-medarbejdercertifikaternes anvendelsesområde på lige fod. Dette betyder, at der ikke må gøres forskel på vilkår og betingelser for adgang til tjenester.

Alle CA's administrative og forretningsmæssige procedurer skal være tilpasset det nødvendige sikkerhedsbehov, driften af en CA foreskriver.

CA skal have tilstrækkelig finansiel styrke til at dække det ansvar, man påtager sig som CA, herunder også forpligtelserne i 7.4.9, dels gennem forsikring, dels gennem egenkapital.

CA skal til enhver tid have tilstrækkelig med uddannet personale til at kunne drive alle udbudte tjenester på forsvarlig vis. Personalet skal til enhver tid have den kompetence, de enkelte definerede betroede funktioner foreskriver.

CA skal sikre, at der foreligger politikker og procedurer for håndtering af alle former for kundehenvendelser eller henvendelser fra signaturmodtagere.

CA skal sikre, at der foreligger skriftlige aftaler med alle underleverandører af CA-tjenester.

7.6 Placering af datacentre

CA'er, der ønsker at placere hele eller dele af driftsmiljøet i udlandet, skal opfylde de samme krav i henhold til denne CP som en herværende CA. Den løbende kontrol skal således kunne gennemføres uanset, hvor CA geografisk er placeret.

Foretages systemrevisionen ikke af en statsautoriseret revisor, kræves der, jf. afsnit 7.1., en dispensation fra IT- og Telestyrelsen.