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

Version 2

Indholdsfortegnelse

Rettigheder

IT- og Telestyrelsen har alle rettigheder til denne certifikatpolitik (CP), OCES-navnet og OCES-OID. Brug af OCES-OID i certifikater og brug af betegnelsen OCES i forbindelse med udstedelse af 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-funktionscertifikater til de udvalgte certificeringscentre (CA'er), 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 seneste version af denne CP samt tidligere versioner af denne, hvorefter der fortsat eksisterer gyldige certifikater, findes på www.digitalsignatur.dk.
Henvendelse i øvrigt vedrørende digital signatur til IT- og Telestyrelsen. Se nærmere på 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 fire OCES-certifikatpolitikker (CP'er), én for henholdsvis person-, medarbejder-virksomheds- og funktionscertifikater. 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 certifikatindehaver er blevet identificeret og registreret hos et certificeringscenter (CA). CA tildeler et elektronisk certifikat, indeholdende certifikatindehaverens offentlige nøgle. CP'en stiller krav til, hvorledes og under hvilke vilkår, CA skal udføre disse opgaver.

Den CP adresserer ikke kvalificerede certifikater udstedt i medfør af lov nr. 417 af 31. maj 2000 om elektroniske signaturer.

1 Oversigt og formål

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

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.

CP'en er udarbejdet med udgangspunkt i de retningslinjer, som er angivet i ETSI TS 102 042 v 1.3.4. (2007-12):*"Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*.

Certifikatpolitikkens bestemmelser om hvordan CA skal agere giver et højt niveau af sikkerhed for, at applikationen, enheden, processen eller servicen tilhører, benyttes eller kontrolleres af den virksomhed, der fremgår af certifikatet.

Formålet med at implementere funktionscertifikater er, at virksomheder kan etablere automatiserede forretningsprocesser, som kræver autentifikation og integritetssikring.

Et funktionscertifikat kan alene bruges til autentifikation af en applikation, en enhed, en proces eller service og til integritetssikring og kryptering af kommunikationen herimellem. Et funktionscertifikat skal ikke anvendes til indgåelse af juridisk bindende aftaler.

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-funktionscertifikater. Som led i godkendelsen indgås en formel aftale mellem CA og IT- og Telestyrelsen, hvori CA bl.a. forpligter sig til at opfylde kravene i denne CP, herunder krav om revision af CA's opgavevaretagelse, jf. i øvrigt afsnit 7.1
En CP er en del af aftalegrundlaget mellem IT- og Telestyrelsen og det enkelte certificeringscenter (CA) om ret til udstedelse af OCES-certifikater.

Certifikatindehavernes og signaturmodtagernes tillid kan således baseres på certifikatpolitikken, IT- og Telestyrelsens godkendelse af CA og styrelsens løbende tilsyn hermed.

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

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)*"

CWA 14167-1:2003: *"Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements"*

CWA 14167-2:2004: *"Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP"*

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

DS 844: *"Specifikation for kvalificerede certifikater"*

DS 471:1993: *" Teknisk forebyggelse af indbrudskriminalitet"*

DS 484:2005 *"Dansk standard for Informationssikkerhed DS 484"*

ETSI TS 102 042 v 1.3.4. (2007-12):*"Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"*

ETSI TS 102 176-1 V2.0.0 (2007-11): *"Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures;Part 1: Hash functions and asymmetric algorithms"*

ETSI TS 102 176-2 V1.2.1 (2005-07): *"Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures;Part 2: Secure channel protocols and algorithms for signature creation devices"*

ETSI TS 101 862 v1.3.3 (2006-01): *"Qualified Certificate profile"*

FIPS PUB 140-2 (2001): "*Security Requirements for Cryptographic Modules*"

ISO/IEC 15408 (del 1 til 3) 2005: *"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*"

Request for Comments:

- RFC 3039: *Internet X.509 Public Key Infrastructure - Qualified Certificates Profile*
- RFC 3280: *Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile*
- RFC 5019: *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*

Såfremt der måtte være uoverensstemmelse mellem ovenstående referencer og denne CP, finder CP'ens bestemmelser anvendelse for CA med mindre andet følger af lov.

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.

Adgangskode: Kode, som holdes hemmelig af certifikatindehaver, og som anvendes i forbindelse med afgivelse af signatur.

Midlertidig adgangskode: Kode, der benyttes til at aktivere signaturen i forbindelse med generering og installation af nøgler.

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

Certifikatholder ("subject"): En applikation, enhed, proces eller service, 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 hvilken funktion et OCES certifikat enten er under udstedelse eller er blevet udstedt.

Certifikatindehaver ("subscriber"): En fysisk eller juridisk person, der indgår aftale med det udstedende certificeringscenter (CA), 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, udstede og administrere 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 sammenhænge, 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 lagre nøgler samt anvende den digitale signatur. Enheden skal være certificeret efter FIPS 140-2 level 3, CWA 14167-3 eller SSCD-PP Type 3.

[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.

Medarbejder: Person, der er tilknyttet den virksomhed, der fremgår af certifikatet.

Nøgledeponering (”Key Escrow”): Lagring af nøgler, med henblik på at give tredjemand adgang til disse for at kunne foretage dekryptering af information.

OCES-funktionscertifikat: 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. OCES-funktionscertifikater kan kun anvendes til autentifikation, integritetssikring og kryptering. OCES-funktionscertifikater skal ikke anvendes til indgåelse af juridisk bindende aftaler.

Offentligt certifikat ("public-key certificate"): Se OCES-funktionscertifikat.

Privat Nøgle (”Private key”): Certifikatindehavers nøgle til brug for afgivelse af en digital signatur eller til dekryptering. Den private nøgle er personlig og holdes hemmelig af certifikatindehaver.

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

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 signeringsnøgler (privat og offentlig nøgle).

Signaturmodtager ("verifier"): En fysisk eller juridisk person som modtager signerede data fra en certifikatindehaver.

Subcertificering af CA: Et overordnet CA’s udstedelse af et certifikat med den underordnede CA’s offentlige rodnøgle. Subcertificering kan forekomme i flere niveauer, således at der dannes en sammenhørende kæde af certifikater.

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
FID	Funktions Identifikationsnummer
LDAP	"Lightweight Directory Access Protocol"
NIST	National Institute of Standards and Technology.

OCES	Offentlige Certifikater til Elektronisk Service
OCSP	"Online Certificate Status Protocol"
OID	Object identifier, jf. ITU-T's ASN.1 standard
OTP	"One Time Password"
PKI	"Public Key Infrastructure"
RA	"Registration Authority"
UTC	Fælles tidsangivelse ("Universal Time Coordinated ")

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

4.1 CA

En fysisk eller juridisk person, der er betroet af både certifikatindehavere og signaturmodtagere til at generere, udstede 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 dele af de samlede CA-tjeneste, 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 CA kan subcertificere sin offentlige OCES rodnøgle under andre CA'er. En CA's OCES rodnøgle kan også subcertificere en anden CA's offentlige rodnøgle, såfremt denne er godkendt til OCES.

En OCES CA skal altid tilbyde et selvsigneret OCES rodcertifikat til signaturmodtagerne.

4.2 CA-tjenester

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

- Registrering: Verificering af certifikatindehaverens identitet og eventuelle tilhørende id- og registreringsoplysninger. Resultatet af registreringen overgives til certifikatgenereringen.
- Certifikatgenerering: Generering og elektronisk signering af certifikater baseret på den verificerede identitet og eventuelle andre id- og registreringsoplysninger fra registreringen.
- Certifikatdistribution: Distribution af certifikater til certifikatindehavere.
- Katalogtjeneste: Offentliggørelse af certifikater, så signaturmodtagere kan få adgang til certifikaterne.
- Publikation af forretningsbetingelser mm.: 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 opfyldes hos den respektive CA. I certifikatet henvises til CP'en, således at en signaturmodtager kan gøre sig bekendt med, hvilke grundlæggende krav CA'en opfylder, herunder hvilke krav CA skal pålægge certifikatindehaveren af opfylde.

4.3.2 Specifikationsgrad

CPS'en angiver den detaljerede beskrivelse af forhold og betingelser, herunder forretnings- og driftsprocedurer for udstedelse og vedligeholdelse af certifikater. CPS'en er således mere detaljeret end CP'en, der alene beskriver de generelle krav.

CPS skal angive, 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 også forskellig. En CP, som nærværende, er for eksempel fastlagt uafhængigt af specifikke detaljer i driftsmiljøerne hos CA, 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.

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

CP'en og CPS'en, beskriver de grundlæggende rammer for CA's virke. Herudover vil CA typisk operere med kunderettede kommercielle betingelser og vilkår, der retter sig imod certifikatudstedelse, certifikatanvendelse og tilrådighedsstillelse af statusinformation.

5 Certifikatpolitik og revision

5.1 Generelt

Dette dokument beskriver certifikatpolitik for OCES-funktionscertifikater.

5.2 Identifikation

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

Funktionscertifikat:

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

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

Alle OCES-funktionscertifikater, der udstedes efter denne CP, skal referere hertil 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, jf. afsnit 1.

5.3 Anvendelsesområde

Et OCES-funktionscertifikat kan anvendes til sikring af afsender- og meddelelsesautencitet og -integritet. Det kan også anvendes til at sikre hemmeligholdelse (kryptering).

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

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

OCES-funktionscertifikater kan være gyldige i maksimalt 4 år.

Et OCES-funktionscertifikat skal ikke anvendes til at indgå bindende juridiske aftaler.

5.4 CA’s ret til at udstede OCES-certifikater

CA kan udstede OCES-funktionscertifikater efter denne CP, hvis CA,

- har indgået skriftlig aftale med IT- og Telestyrelsen herom og
- har indsendt en CA-rapport jf. afsnit 5.5 til IT- og Telestyrelsen 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.

En opdateret CA-rapport skal 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.

5.5 CA-rapport

Rapporten skal 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.

5.6 Systemrevision

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

- Generelle it-kontroller i virksomheden.
- It-baserede brugersystemer m.v. til generering af nøgler og nøglekomponenter samt registrering, udstedelse, verificering, opbevaring og spærring af certifikater.
- It-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 et ledelsesmøde forstås et møde mellem den øverste ledelse af CA, i praksis ofte et bestyrelsesmøde. Ved udtrykket CA's ledelse forstås i denne sammenhæng den øverste ledelse af CA, dvs. bestyrelse eller tilsvarende ledelsesorgan afhængigt af, hvorledes CA er organiseret. 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'en, 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 og
- 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.

6 Forpligtelser og ansvar

6.1 CA's forpligtelser

CA skal opfylde alle krav specificeret i afsnit 7.

CA er ansvarlig for sine underleverandørers opfyldelse af procedurer og krav i denne certifikatpolitik.

CA skal sikre varetagelsen af alle aspekter i forbindelse med:

- distribution af rodcertifikater,
- anvisning af, hvorledes nøgler genereres og opbevares,
- udstedelse af OCES-funktionscertifikater til certifikatindehavere,
- spærring af OCES-funktionscertifikater efter anmodning,
- publikation af spærrelister,
- underretning af certifikatindehavere om snarlig udløb af gyldighed for certifikater og evt. fornyelse af nøgle-par og
- fornyelse af OCES-funktionscertifikater.

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

CA skal anvende en pålidelig tidskilde i forbindelse med CA relaterede aktiviteter,

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. afsnit 5.6.

Registreringsenheden (RA) kan enten være nøje knyttet til CA, 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’s Web-tjeneste, hvis RA er en integreret del af CA),
- verificerer ansøgerens identitet og oplysninger og
- opretholder et teknisk driftsmiljø i overensstemmelse med kravene i denne CP.

6.2 Certifikatindehaverens forpligtelser

CA skal ved aftale forpligte certifikatindehaveren til at opfylde 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,
- at tage rimelige forholdsregler for at beskytte den private nøgle og tilhørende sikkerhedsmekanismer mod kompromittering, ændring, tab og uautoriseret brug,
- at beskytte den private nøgle med en adgangskode, der mindst består af 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal,
- anvendes adgangskoden i miljøer, der effektivt kan spærre for udtømmende søgninger, skal denne dog alene være på minimum fire tegnanvendelse af en anden adgangskode – f.eks. biometrisk – skal implementere en sikkerhed, der mindst er på niveau med sikkerheden af traditionelle adgangskoder i denne certifikatpolitik,
- at hemmeligholde og beskytte adgangskoden, så uvedkommende 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 den udstedende CA om spærring af OCES-certifikatet i tilfælde af certifikatindehavers konkurs eller likvidering,
- omgående at anmode om fornyelse af certifikatet, hvis indholdet af OCES-certifikatet ikke længere er i overensstemmelse med de faktiske forhold,
- omgående at ophøre med anvendelse af certifikatet, hvis certifikatindehaveren opnår kendskab til, at CA er blevet kompromitteret og
- såfremt den private nøgle beskyttes af en OTP-enhed, skal denne omgående spærres, hvis der opstår mistanke om, at OTP-enheden er kompromitteret.

Supplerende forpligtelser

Krav om beskyttelse af den private nøgle med adgangskode kan fraviges i forbindelse med automatiseret anvendelse, såfremt installationen er sikret mod uautoriseret adgang. Certifikatindehaver skal i givet fald påtage sig ansvaret herfor og skal kunne dokumentere sikringens beskaffenhed.

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

CA skal endelig orientere certifikatindehaver om, at det er certifikatindehavers ansvar gennem aftale at sikre den private nøgle mod uautoriseret brug, såfremt den private

nøgle hørende til funktionscertifikatet genereres, opbevares eller anvendes hos tredjepart (f.eks. i outsourcede it-installationer).

Såfremt certifikatindehaver skifter virksomhedsadresse, skal dette straks meddeles til CA.

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 der ikke indgås bindende juridiske aftaler med OCES-funktionscertifikatet,
- at det formål, et certifikat i øvrigt søges anvendt til, er passende i forhold til evt. 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 afsnit 7.3.3,
- manglende spærring af certifikatet, jf. afsnit 7.3.6,
- manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. afsnit 7.3.3 og afsnit 7.3.6, eller
- tilsidesættelse af afsnit 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. 10 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 produkter og algoritmer, 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,
- hvilken pålidelig tidskilde CA benytter.

CA's-praksis skal til enhver tid være i overensstemmelse med det i CPS'en beskrevne. CA skal offentliggøre CPS'en på sin hjemmeside. Følsomme informationer, f.eks. forretningshemmeligheder kan undtages fra offentliggørelse.

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.

For kritiske dele af CA's infrastruktur, skal CA skal følge relevante og officielle anbefalinger fra NIST vedr. anvendelsen af tidssvarende algoritmer og nøglelængder.

7.2.1 CA nøglegenerering

CA skal sikre, at generering af nøgler sker under kontrollerede forhold. Nedenstående forhold skal særligt iagttages.

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 et kryptografisk modul, der opfylder kravene i FIPS 140-2 level 3, CWA 14167-3, 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-nøgle af en længde på mindst 2048 bit eller tilsvarende. Certifikatudsteders rodnøgler skal være gyldige i mindst 5 år.

Betegnelsen ”OCES” skal indgå i rodcertifikatets commonName.

7.2.2 CA-nøglelagring, back-up og genskabelse

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

CA's rodnøgler og andre private nøgler skal opbevares i kryptografiske moduler, der opfylder FIPS 140-2 level 3, CWA 14167-3 eller højere.

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.

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

7.2.3 CA's publicering af den offentlige nøgle

CA's rodcertifikat skal gøres tilgængelig for signaturmodtagere via CA’s hjemmeside på en måde, der sikrer integriteten af den offentlige nøgle og autentificerer dens oprindelse.

CA skal give mulighed for verifikation af rodcertifikatets via anden kanal. Verifikation kan f.eks. ske ved anvendelse af et fingerprint for certifikatet.

7.2.4 Nøgledeponering

CA må ikke foretage nøgledeponering af certifikatindehavers nøgler.

7.2.5 CA's brug af nøgler

CA skal sikre, at CA'ens 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 fastsat gyldighedsperiode. Efter udløb skal den private nøgle enten destrueres eller opbevares på en sådan måde, at den ikke kan genskabes og tages i brug igen.

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

7.2.7 Håndtering af kryptografiske moduler

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

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

7.3 Certifikathåndtering

7.3.1 Registrering af certifikatindehaver og certifikatholder

Registrering af certifikatindehaver

CA skal sikre, at certifikatindehaver forud for udstedelsen af et OCES-funktionscertifikat gøres opmærksom på og accepterer vilkår og betingelser for anvendelsen af certifikatet, herunder at funktionscertifikater kan fornyes ved hjælp af en automatiseret proces udelukkende signeret af funktionscertifikatets private nøgle, jf. pkt 7.3.2. Certifikatindehaver forpligtes i denne forbindelse til at udpege en af ledelsen godkendt bemyndiget, der har beføjelser til at administrere funktionscertifikater på vegne af virksomheden.

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

- OCES-certifikatindehaveren oplyser virksomhedens CVR-nr. samt navn og e-mail på den bemyndigede,
- OCES-certifikatindehaverens CVR-postadresse indhentes ved online opslag i CVR registeret,
- evt. afdelingsnavn indhentes gennem bemyndigede og

- OCES-certifikatindehaveren udstyres med en midlertidig adgangskode fremsendt via pinkodebrev til virksomhedens ledelse på virksomhedens CVR-postadresse.

Det er tilstrækkeligt at CVR-postadressen verificeres i forbindelse med registrering af certifikatindehaver. 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. Procedurer skal forelægges og godkendes af IT- og Telestyrelsen før implementering.

Registrering af certifikatholder
CA skal etablere og opretholde en funktion, hvorigennem den bemyndigede kan foretage ansøgning om og udstedelse af funktionscertifikater. CA skal sikre, at registreringsprocessen sker gennem den af virksomheden bemyndigede person.

CA skal etablere en procedure for registrering af funktionscertifikatet, der sikrer, at

- den bemyndigede angiver virksomhedens CVR-nr.,
- den bemyndigede angiver funktionscertifikatets funktion og
- den bemyndigede udstyres med en engangskode til installation og aktivering af den private nøgle og tilhørende certifikat.

Generering og installation af certifikatholderens nøgler
CA skal etablere en installationsprocedure, der teknisk sikrer, at:

- midlertidig adgangskode til installation af den private nøgle og tilhørende nøgle overføres til den bemyndigede via en sikker elektronisk forbindelse eller fremsendes via pinbrev,
- certifikatindehaver skal angive den midlertidige adgangskode for at påbegynde installation af den private nøgle og tilhørende certifikat,
- nøglepar genereres hos certifikatindehaver,
- certifikatholders nøgler er RSA-nøgler med en længde på mindst 2048 bit eller tilsvarende,
- den offentlige nøgle overføres til CA sammen med oplysninger om funktionscertifikatets funktion i en meddelelse signeret med den private nøgle,
- den private nøgle er krypteret og beskyttet af en adgangskode,
- adgangskoden til aktivering af den private nøgle genereres og indtastes i forbindelse med nøglegenereringen,
- den private nøgle er aktiveret, når certifikatindehaveren har angivet adgangskoden, der består af mindst 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal. Anvendes en adgangskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan denne dog vælges fra et udfaldsrum på

mindst 10^4 mulige koder, for eksempel som 4 cifre valgt ud af tal mellem 0 og 9. Anvendelse af anden adgangskode – f.eks. biometrisk – skal implementere en sikkerhed, der mindst er på niveau med disse krav.
- rodcertifikatet er installeret hos OCES-certifikatindehaver og
- 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 certifikatindehavere anvise kryptografiske moduler til dette formål.

CA skal på sin hjemmeside anvise metode for certifikatindehaver til at lave sikkerhedskopi af den private nøgle i krypteret form.

RA skal godkende en certifikatansøgning, hvis proceduren gennemføres som anvist

CA skal sikre, at der fra det tidspunkt, CA eller en af CA udpeget 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 én arbejdsdag. Der må aldrig gå mere end tre arbejdsdage.

7.3.2 Certifikatfornyelse

Fornyelse af et OCES-certifikat betyder anvendelse af et gyldigt certifikat til udstedelse af et nyt certifikat efter denne certifikatpolitik til den samme certifikatindehaver. Det nye certifikat skal have samme funktion, angivet i ”commonName”, som det eksisterende certifikat samt gældende OID. Certifikatet udstedes med en ny nøgle, ny gyldighedsperiode, et nyt certifikat-serienummer. Et OCES-certifikat må fornyes for op til fire år ad gangen.

CA og certifikatindehaver kan træffe aftale om, at funktionscertifikatet fornyes via en automatiseret fornyelsesproces.

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

Et OCES funktionscertifikat kan fornys af den bemyndigede på baggrund af behørig identifikation eller i forbindelse med en automatisk fornyelsesproces, forudsat at CA og certifikatindehaver har truffet beslutning herom.

CA skal sikre, at den funktion, hvorigennem den bemyndigede kan foretage ansøgning om og udstedelse af funktionscertifikater tillige kan håndtere anmodning om fornyelse.

CA skal godkende bevis for besiddelsen af den private nøgle tilhørende den bemyndigedes medarbejdercertifikat eller den private nøgle hørende til det certifikat, der ønskes fornyet, som værende tilstrækkelig autentifikation til at gennemføre fornyelse.

RA skal således sikre, at den bemyndigede besidder den private nøgle, som svarer til den offentlige nøgle, som præsenteres i certifikatansøgningen.

I forbindelse med en automatiseret fornyelsesproces skal funktionscertifikatets private nøgle anses som tilstrækkelig autentifikation.

Certifikatansøgning og -udstedelse skal i øvrigt opfylde kravene i afsnit 7.3.1 om generering og installation af certifikatindehavers nøgler.

Efter spærring eller udløb af funktionscertifikatet, eller hvis funktionscertifikatets private nøgle er blevet kompromitteret, kan et funktionscertifikat 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-funktionscertifikat i dette tilfælde sker som ny udstedelse efter samme retningslinjer, som angivet i afsnit 7.3.1.

CA skal senest 4 uger før udløb notificere den bemyndigede herom via e-post til den bemyndigedes registrerede e-postadresse. CA og certifikatindehaver kan træffe aftale om, at denne notificering undlades eller sendes til en anden e-postadresse end den bemyndigedes.

7.3.3 Certifikatgenerering

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

OCES-funktionscertifikater må ikke indeholde en e-postadresse.

OCES-funktionscertifikater 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.
En markering af, at certifikatet er et funktionscertifikat samt en brugerdefineret unktionsbetegnelse.	CommonName indeholder en brugerdefineret funktionsbetegnelse samt en markering af, at certifikatet er et funktionscertifikat.
Særlige oplysninger om underskriveren, 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.
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 3280.

OCES-funktionscertifikater skal indeholde:	***Løsning***
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 3280.
Den udstedende CA's avancerede elektroniske signatur.	X.509.v3 og RFC 3280.
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-FID:funktionsId
commonName	M	Tekststreng (funktionscertifikat)
postalAddress	O	Virksomhedens postadresse

Eksempel:
countryName=DK,
organizationName=ABC // CVR:12345678
commonName=Serverautentifikation (funktionscertifikat)
serialNumber=CVR:12345678-FID:funktionsId

Regler:
countryName=DK, organizationName, organizationalUnitName, serialNumber, og commonName skal tilsammen entydigt udpege virksomheden, der er indehaver af certifikatet. CVR-nummer skal være indeholdt i **serialNumber**.
Ikke nævnte felter er valgfrie.

Øvrige felter (extensions)

Versionsnummer skal være ”v3”.

Funktionscertifikater kan anvendes til autentifikation og kryptering. **KeyUsage** "extension" skal have følgende specifikationer sat:

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

contentCommitment specifikationen (**contentCommitment(1)**) må ikke være sat for funktionscertifikater.

KeyUsage ”extension” skal defineres som kritisk.

I oversigterne nedenfor anvendes følgende 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		
	1. Anvendelse	2. CA	3. Slut bruger	4. Key Man.
AuthorityKeyIdentifier	O	O	O	O
SubjectKeyIdentifier	O	O	O	O
KeyUsage	CM	CMR	(C)MR	(C)MR
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.

SubjectAltName og Subject distinguishedName må ikke indeholde e-post adresser.

7.3.4 Publicering af vilkår og betingelser

CA skal på sin hjemmeside offentliggøre sine vilkår og betingelser for anvendelse af certifikater udstedt efter denne CP.

CA skal orientere certifikatindehaver om, at OCES-funktionscertifikater ikke må bruges i situationer, hvor kvalificerede certifikater er påkrævet.

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

CA skal orientere certifikatindehaver om, at OCES-funktionscertifikater ikke skal anvendes til bindende juridisk aftaler.

CA skal orientere certifikatindehaver om, at den private nøgle ikke må benyttes førend OCES-certifikatet er modtaget af certifikatindehaveren, bortset fra den brug, der indgår i certifikatansøgningsprocessen.

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 certifikatindehaverens mistanke om at den private nøgle er kompromitteret, må denne kun anvendes til anmodning om spærring.

Såfremt den private nøgle er tilgængelig for certifikatindehaver, må den private nøgle dog stadig benyttes til dekryptering af data, der er krypteret med den tilhørende offentlige nøgle.
I forbindelse med udstedelse af nye nøgler, herunder ved fornyelse heraf, 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-funktionscertifikat og om, at et OCES-funktionscertifikat 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.
- CA skal give mulighed for verifikation af rodcertifikatets fingerprint via anden kanal.

- Andre certifikater, der anvendes for signering af information mellem CA og certifikatindehavere eller 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 specifikke forretningshemmeligheder.
- Oversigt over alle OCES-funktionscertifikater indtil minimum to måneder efter udløb af det enkelte certifikats gyldighedsperiode. Undtagen herfra er undtagen de certifikater, som skal holdes hemmelige.
- Spærreliste for OCES-funktionscertifikater udstedt efter denne CP.

Spærrelisteinformation skal være tilgængelig 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

Generelt om spærring af certifikat

CA skal omgående spærre et OCES-funktionscertifikat, hvis CA får kendskab til et eller flere af følgende forhold:

- Certifikatindehaveren ønsker at spærre OCES-certifikatet.
- Certifikatindehaveren har mistet adgangen til den private nøgle, f.eks. som følge af bortkommen adgangskode.
- Der er vished eller mistanke om, at certifikatindehaverens private nøgle er kompromitteret.
- Den private nøgle er ødelagt eller gået tabt på anden vis.
- Der er konstateret unøjagtighed i certifikatets indhold eller anden information knyttet til certifikatindehaveren.
- Certifikatindehaverens konkurs.
- Certifikatindehaverens virksomhed ophører.

Spærres den bemyndigedes OCES-medarbejdercertifikat på foranledning af certifikatindehaveren, skal CA sikre, at certifikatindehaveren omgående tager stilling til, hvorvidt virksomhedens OCES-funktionscertifikater skal spærres.

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

Ved anmodning om spærring skal CA sikre, at identifikationen sker på en måde, der sikrer identiteten bedst muligt f.eks. ved en kombination af navn på certifikatindehaver, CVR-nummer, CVR-postadresse og e-postadresse.

Følgende kan anmode om spærring af certifikat:

- Bemyndigede,
- 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 certifikatindehaveren har anmeldt betalingsstandsning eller tages under konkursbehandling,
- en af Skifteretten udpeget bobestyrer eller arvinger efter certifikatindehaver, såfremt certifikatindehaver er afgået ved døden.

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 online via CA's hjemmeside.

Anmodning om spærring
CA skal sikre, at der ved telefonisk anmodning om spærring afgives den fornødne information til sikring af identifikation samt årsag til spærring.

Anmodning om spærring via online web-formular eller e-post skal indeholde den fornødne information til sikring af identifikation eller være signeret med den bemyndigedes medarbejdercertifikat.

Yderligere forhold vedr. spærringer
CA orienterer om gennemført spærring via e-post til den bemyndigedes e-postadresse eller anden elektronisk kanal, der stilles til rådighed for den bemyndigede.

Hvis CA foretager spærring uden at være anmodet om det, skal CA sende e-postmeddelelse med angivelse af årsag via e-post til den bemyndigedes oplyste e-postadresse.

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

CA skal efter at et forhold, der giver anledning til spærring er konstateret sikre, at der sker spærring uden ugrundet forsinkelse.

Et OCES funktionscertifikat kan ikke suspenderes.

Håndtering af spærrelister
CA skal sikre, at spærring sker umiddelbart efter anmodning er modtaget og eventuelt bekræftelse af anmoders identitet er sket.

CA skal efter gennemført spærring offentliggøre en opdateret spærreliste. Dette skal ske senest 1 minut, efter spærring er sket.

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

CA skal fastsætte levetiden for spærrelisten til 12 timer. CA skal offentliggøre en ny spærreliste hver gang der foretages en spærring, dog senest 6 timer før udløb af den aktuelle spærreliste.

CA skal gøre spærrelister tilgængelige for download via følgende kanaler:

- LDAP
- HTTP

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

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

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

For OCSP skal CA benytte en profil i overensstemmelse med IETF RFC 5019.

OCSP respons kan prægenereres, men det kræves at hvis et certifikat spærres da skal det tilhørende OCSP respons regenereres og senest 1 minut efter at spærringen er registreret, skal OCSP svar indikere, at certifikatet er spærret.

OCSP respondere skal udstyres med dedikerede virksomhedscertifikater som udelukkende bruges til OCSP. Foruden de formalia som kræves for en virksomhedssignatur er der følgende krav til indholdet:

- Key Usage: Digital Signatur
- Extended Key Usage: OCSP Signing
- CRL Distribution Point: Ikke inkluderet
- AIA: Ikke inkluderet
- OCSP No Check: Inkluderet men tom

Levetiden for OCSP responder-certifikater skal være maksimal 72 timer og de tilhørende nøgler skal beskyttes af kryptografiske moduler på linje med øvrige CA nøgler, som angivet i afsnit 7.2.1.

CA skal sikre spærrelister mod kompromittering, og at spærrelisterne og OCSP-tjenester er tilgængelige via internet alle dage 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.

7.4 CA styring og drift

Krav i kapitel 7.4 retter sig alene mod RA, hvor dette eksplicit er nævnt.

7.4.1 Sikkerhedsimplementering

CA skal sikre, at dens administrative og ledelsesmæssige procedurer er tilstrækkelige og lever op til de basale krav i Dansk standard for informationssikkerhed DS 484.

I det omfang CA vurderer, at de særlige forhold vedr. CA drift giver anledning til at krav om skærpede sikkerhedsforanstaltninger, dvs. opfyldelse af skærpede krav, som beskrevet i DS 484, skal disse anvendes. CA skal i den årlige CA-rapport redegøre for hvilke krav om skærpede sikkerhedsforanstaltninger, der er implementeret.

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

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

7.4.2 Identifikation og klassifikation af it-aktiver

CA skal i overensstemmelse med det i afsnit 7.4.1 anførte opfylde de basale og skærpede krav i DS 484.

7.4.3 Personalesikkerhed

Procedurer for sikkerhedsklassifikation

CA skal kontrollere, at ledere og medarbejdere, der udfører betroede opgaver i eller for CA, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv. Dette er ligeledes gældende for RA medarbejdere.

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 for CA.

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

RA personale skal gennemføre en uddannelse, som sætter dem i stand til at udføre deres arbejde korrekt og sikkert.

7.4.4 Fysisk sikkerhed

Generelt

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.

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

CA driftslokaler

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.

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

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.

Opbevaring og behandling på anden lokalitet
Opbevares eller behandles data på anden lokalitet, skal CA sikre, at dette sker under opfyldelse af samme krav til sikkerhed som krav til CA's hovedsystemer.

7.4.5 Styring af IT-systemers og netværks drift
CA skal i overensstemmelse med det i afsnit 7.4.1 anførte opfylde de basale og skærpede krav i DS 484.

7.4.6 Kontrol af adgang til systemer, data og netværk
CA skal i overensstemmelse med det i afsnit 7.4.1 anførte opfylde de basale og skærpede krav i DS 484.

CA skal tilvejebringe RA systemer, som sikrer, at det kun er bemyndigede medarbejdere hos RA, der har adgang til at betjene disse.

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.

CA skal sikre, at der forud for enhver systemudvikling (dvs. egenudvikling eller udvikling ved tredjemand) foreligger en en ledelsesgodkendt plan for indbygning af sikkerhed i systemerne.

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 i tilfælde af kompromittering af CA's private nøgle eller mistanke herom straks informere alle certifikatindehavere via den registrerede e-mailadresse. CA skal ligeledes straks informere IT- og Telestyrelsen med en uddybende beskrivelse af den opstående situation.

CA skal ligeledes på sin hjemmeside og i det omfang det vurderes relevant under hensyntagen til den opstående situation - via offentlige medier – straks informere signaturmodtagere.

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. Under hensyntagen til den opståede situation, skal signaturmodtagere informeres via offentlige medier og ved annoncering i dagspressen.

CA skal sikre, at alle procedurer for, og etablering af spærrelister, herunder anmodning om spærring, har højeste prioritet i forbindelse med retablering af forretningsgange efter nedbrud.

7.4.9 Ophør af CA

CA skal sikre, at al udstedelse og fornyelse af certifikater straks stoppes, når en CA-funktion ophører med at fungerer.

Forud for ophør skal CA informere certifikatindehavere og alle øvrige parter, der har et kontraktligt forhold til CA.

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 og RA skal sikre overensstemmelse med lovgivningen, herunder særligt lov om behandling af personoplysninger.

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 og RA 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.

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

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

Kan en tvist ikke løses forligsmæssigt, kan enhver af parterne vælge at indbringe tvisten for de almindelige domstole. Værneting er København. Dansk ret er 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 information beskyttes mod uretmæssig adgang,
- alle sikkerhedskritiske aktiviteter, samt aktiviteter, der kræver deltagelse af mere end én 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 log,
- alle audit-logs signeres elektronisk og tidsstemples,
- audit-logs behandles som fortroligt materiale og
- der foretages back-up af audit-logs med regelmæssig mellemrum.

CA skal sikre, at back-up-data opbevares i overensstemmelse med kravene i DS 484.

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

CA skal sikre, at følgende information arkiveres:

- alle logs,
- certifikatanmodninger og tilhørende kommunikation,
- signerede ordrer og skriftlige aftaler,
- certifikatfornyelser og
- CPS og CP.

CA skal sikre, at arkiveret information kan gøres tilgængelig i tilfælde af tvister, og at alt arkiveret materiale opbevares i mindst løbende kalenderår + 5 år. Dette er også gældende for evt. data fra RA's it-systemer, som er relevante for dokumentation af CA's virke.

CA og RA skal sikre, at alt materiale i arkiv opbevares i overensstemmelse med kravene i DS 484.

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

CA og RA 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 lige adgang til alle tjenester inden for OCES-funktionscertifikaternes anvendelsesområde. Dette betyder, at vilkår og betingelser for adgang til tjenester skal være ikke-diskriminerende.

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, der påtages som CA, herunder også forpligtelserne i afsnit 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, der foreskrives for de betroede funktioner.

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

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

7.6 Placering af datacentre

Kravene i denne CP gælder uanset om CA placerer hele eller dele af driftsmiljøet i udlandet. Den løbende kontrol, der er fastsat i CP'en 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.