Krav til CA'er, der udsteder OCES-virksomhedscertifikater

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

Indholdsfortegnelse

Rettigheder 4
Forord 5
Introduktion 6
1 Oversigt og formål 7
2 Referencer 8
3 Definitioner og forkortelser 9
3.1 Definitioner 9
3.2 Forkortelser 10
3.3 Notation 10
4 Koncept 11
4.1 CA 11
4.2 CA-tjenester 11
4.3 CP og CPS 12
4.3.1 Formål 12
4.3.2 Specifikationsgrad 12
4.3.3 Tilgang 12
4.3.4 Andre CA-betingelser 12
4.4 Certifikatindehavere 12
5 Introduktion til certifikatpolitik 13
5.1 Generelt 13
5.2 Identifikation 13
5.3 Anvendelsesområde 13
5.4 Overensstemmelse 14
5.4.1 Overensstemmelseserklæring 14
5.4.2 Krav til overensstemmelse 14
6 Forpligtigelser og ansvar 15
6.1 CA's forpligtigelser 15
6.2 Certifikatindehaverens forpligtigelser 16
6.3 Signaturmodtagernes forhold 16
6.4 Ansvar 16
Særligt i forhold til certifikatindehavere og signaturmodtagere 16
Forsikring 17
Beskyttelse af fortrolig information 17
7 Krav til CA-praksis 18
7.1 Certificeringspraksis (CPS) 18
7.2 PKI-nøglehåndtering 21
7.2.1 CA nøglegenerering 21
7.2.2 CA-nøglelagring, back-up og genskabelse 21
7.2.3 CA's distribution af offentlig nøgle 21
7.2.4 Nøgleopbevaring og -genskabelse 21
7.2.5 CA's brug af nøgler 22
7.2.6 CA's afslutning af nøglebrug 22
7.2.7 Håndtering af kryptografiske moduler 22
7.2.8 CA'ens nøglehåndteringstjeneste 23
7.3 PKI-certifikathåndtering 23
7.3.1 Registrering af certifikatindehaver 23
7.3.2 Certifikatfornyelse og nøglefornyelse 24

7.3.3 Certifikatgenerering 25
7.3.4 Certifikatbetingelser 29
7.3.5 Certifikatudbredelse 29
7.3.6 Certifikatspærring 30
7.4 CA styring og drift 32
7.4.1 Sikkerhedsimplementering 32
7.4.2 Identifikation og klassifikation af IT-aktiver 33
7.4.3 Personalesikkerhed 33
7.4.4 Fysisk sikkerhed 34
7.4.5 Styring af IT-systemers og netværks drift 36
7.4.6 Kontrol af adgang til systemer, data og netværk 37
7.4.7 Udvikling, anskaffelse og vedligeholdelse af IT-systemer 38
7.4.8 Beredskabsplanlægning 38
7.4.9 Ophør af CA 39
7.4.10 Opfølgning på lovbestemte og kontraktlige krav 39
7.4.11 Opbevaring af certifikatinformation 40
7.5 Organisatoriske aspekter 41
7.6 Placering af datacentre 41

Rettigheder

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

Forord

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

IT- og Telestyrelsen er den offentlige myndighed, som bemyndiger udstedelsen af OCES-virksomhedscertifikater 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. Kontaktpersoner i IT- og Telestyrelsen er Signatursekretariaet. Se https://www.signatursekretariatet.dk.

Introduktion

Af regeringsgrundlaget fremgår det, at

" kommunikationen mellem borgere og det offentlige skal forbedres ved at give alle borgere en digital signatur."

For at understøtte dette mål har Ministeriet for Videnskab, Teknologi og Udvikling igangsat et projekt, der har til formål at udbrede digitale signaturer til borgere, medarbejdere og virksomheder i Danmark. Projektet skal etablere de nødvendige rammer og den nødvendige infrastruktur til udstedelse, håndtering og anvendelse af digitale signaturer, herunder sikre den fornødne support og rådgivning til myndigheder, borgere og virksomheder.

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).

De tre OCES-certifikatpolitikker (CP'erne), dvs. certifikatpolitikker for person, medarbejder- og virksomhedscertifikater, er centrale i bestræbelserne på at fremme anvendelsen af digitale signaturer. Den fastsætter således krav til nøgleinfrastrukturen og herigennem sikkerhedsniveauet for den digitale signatur, der kan anvendes på grundlag af denne.

Den digitale signatur kan anvendes, når man en gang for alle 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.

1 Oversigt og formål

Denne certifikatpolitik (CP) beskriver de retningslinjer, der gælder for udstedelsen af et OCES-virksomhedscertifikat, 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 1.1.1. (2002-04) "*Policy requirements for certification authorities issuing public key certificates".*

Et virksomhedscertifikat garanterer, at certifikatindehaveren er den virksomhed, der fremgår af certifikatet.

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

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 forholde til deres "kunder", certifikatindehavere og signaturmodtagere, idet formålet er, at certifikatpolitikken skal sikre, at signaturerne kan bruges på en for alle parter betryggende måde.

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)*"

ETSI TS 102 042 v 1.1.1. (2002-04) "*Policy requirements for certification authorities issuing public key certificates".*

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 matte være uoverensstemmelse mellem disse tekniske dokumenter 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.

attributcertifikat ("attribute certificate"): En elektronisk attest, som binder en given attributværdi til en bestemt certifikatindehavers nøglecertifikat. Attributværdien angiver en bemyndigelse (prokura). Attributcertifikatet er signeret af den enhed, som har givet denne bemyndigelse.

bemyndiget: Person, der af 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 ("certificate"): Kan enten være et nøglecertifikat eller et attributcertifikat. I denne CP er certifikat synonymt med nøglecertifikat.

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

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

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

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

elektronisk signatur ("electronic signature"): Data i en elektronisk form, som er vedhæftet eller logisk tilknyttet andet elektronisk data og som tjener til autentificering af data.

entitet ("entity"): En part i Public Key Infrastructure. Certificeringscentre, registreringscentre, certifikatindehavere og signaturmodtagere er entiteter.

kvalificeret certifikat ("qualified certificate"): Et certifikat udstedt i henhold til lov om elektroniske signaturer, lov nr. 417 af 31. maj 2000.

nøglecertifikat ("public-key certificate"): En elektronisk attest, som angiver certifikatindehaverens offentlige nøgle sammen med supplerende information og som

[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.

entydigt knytter den offentlige nøgle til identifikation af certifikatindehaveren. Et nøglecertifikat skal signeres af et certificeringscenter (CA), som derved bekræfter certifikatets gyldighed.

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

rodcertifikat ("root certificate"): Et nøglecertifikat udstedt af en CA til brug for signering af andre certifikater. Et rodcertifikat er signeret med sin egen nøgle (egensignering ("self signing")).

signaturmodtager ("verifier or relying party"): En fysisk eller juridisk person som der modtager signerede data fra en certifikatindehaver.

slut-entitet ("end-entity"): En certifikatindehaver eller signaturmodtager.

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, og angiver styrelsens minimumskrav til de systemer og aftaler, som certificeringscentrene (CA'erne), som de kommercielle udbydere af certifikater, skal opfylde i forholde til deres "kunder", certifikatindehavere og signaturmodtagere, idet formålet er, at 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 Telestyrelsen's 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 nødvendig 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 vedr. 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 certifikatindehaverens 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 certifikatindehavere og offentliggørelse af certifikater, så signaturmodtagere kan få adgang til certifikaterne
- Katalogtjeneste
- 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 mulig.

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, medens 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's 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 Tilgang

Tilgangen til en CP og en CPS er derfor ligeledes forskellig. En CP, som nærværende, er defineret uafhængig 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, medens CPS'en altid udarbejdes af en CA.

Da en CPS indeholder forretningsmæssige følsomme informationer, kan det ikke forventes, at hele CPS'en er offentlig tilgængelig. En uvildig tredjepart (systemrevisor) foretager en revision af CPS og erklærer, 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. Dette vil normalt omfatte de kommercielle betingelser, hvorpå CA udsteder certifikater og stiller statusinformation til rådighed.

4.4 Certifikatindehavere

Ved udstedelse af et certifikat indgår CA en aftale med certifikatindehaveren.

5 Introduktion til certifikatpolitik

5.1 Generelt

Dette dokument beskriver certifikatpolitik for OCES-virksomhedscertifikater.

5.2 Identifikation

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

Virksomhedscertifikat:

{ 1 2 208 stat(169) pki(1) cp(1) nq(1) virksomhed(3) ver(1) }.

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

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

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

5.4 Overensstemmelse

5.4.1 Overensstemmelseserklæring

At en CA har retten til at udstede OCES-virksomhedscertifikater betyder, at CA har en overensstemmelseserklæring på, at kravene i denne CP er opfyldt. IT- og Telestyrelsen kan efter godkendelse af CA's rapport, jf. 7.1., udstede en sådan overensstemmelseserklæring.

5.4.2 Krav til overensstemmelse

Før end CA må udstede OCES-virksomhedscertifikater, skal CA som minimum:

- indgå skriftlig aftale med IT- og Telestyrelsen
- indsende en rapport jf. 7.1. til IT- og Telestyrelsen, indeholdende en erklæring fra uvildig tredjepart systemrevisor. Revisionserklæringen skal godtgøre, at CA 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
- have modtaget en overensstemmelseserklæring fra IT og Telestyrelsen, om at kravene i denne CP er opfyldt

6 Forpligtigelser og ansvar

6.1 CA's forpligtigelser

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

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

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-virksomhedscertifikater til certifikatindehavere
- spærring af OCES-virksomhedscertifikater efter anmodning
- publikation af spærrelister
- underretning af certifikatindehavere om snarlig udløb af gyldighed for certifikat og evt. fornyelse af nøgle-par
- fornyelse af OCES-virksomhedscertifikater

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, eller den kan være en selvstændig funktion, der kan være fælles for flere CA'er. 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-side for registreringsprocedurer (kan være en del af CA's Web-tjeneste, hvis RA er en integreret del af CA)
- verificerer ansøgerens identitet og oplysninger
- opretholder et teknisk driftsmiljø i overensstemmelse med kravene i denne CP

6.2 Certifikatindehaverens forpligtigelser

Certifikatindehaver defineres som den virksomhed hvortil et OCES-certifikat enten er under udstedelse eller er blevet udstedt.

CA skal sikre, at certifikatindehaveren er orienteret om, at denne er ansvarlig for:

- at give fyldestgørende og korrekte svar på alle anmodninger fra CA (eller RA) om information i ansøgningsprocessen
- at opbevare et nøglepar som anvist af CA
- at tage rimelige forholdsregler for at beskytte den private nøgle mod kompromittering, ændring, tab og uautoriseret brug
- 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 eller hvis indholdet af OCES-certifikatet ikke længere er i overensstemmelse med de faktiske forhold

6.3 Signaturmodtagernes forhold

CA skal orientere signaturmodtagere om, at det er deres ansvar at kontrollere, at det formål et certifikat søges anvendt til, er passende i forhold til anvendelsesbegrænsninger på OCES-certifikatet samt i øvrigt passende i forhold til niveauet af sikkerhed, som er beskrevet i denne CP.

6.4 Ansvar

Særligt i forhold til certifikatindehavere og signaturmodtagere

CA skal i forhold til sine medkontrahenter (certifikatindehavere og signaturmodtagere) påtage sig erstatningsansvar efter dansk rets almindelige regler.

CA skal desuden påtage sig erstatningsansvar for tab hos sådanne medkontrahenter, 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 i form af certifikatindehavere og signaturmodtagere. 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 overfor 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.

Beskyttelse af fortrolig information

Særlige forpligtelser med henblik på beskyttelse af fortrolig information
Information, som ikke indgår i certifikater og spærrelister, anses som fortroligt.

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

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.

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.

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

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
- det omfang CA har udliciteret CA-opgaver til andre virksomheder eller myndigheder, skal rapporterne ligeledes omfatte udførelsen af disse opgaver

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

Godkendelse og løbende revision

En CA, der ønsker at udstede OCES-virksomhedscertifikater, 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)

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 ledelsen 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'ens regnskabsår udarbejder den valgte systemrevisor et protokollat til CA'ens 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 PKI-nøglehåndtering

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 kryptografisk modul skal opbevares i henhold til kravene i 7.4.4.

Hvis CA's rodnøgler eller andre private nøgler skal overføres til 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.

Certifikatudsteders andre nøgler skal være RSA-nøgler af længde på mindst 1024 bit eller tilsvarende. Andre nøgler skal være gyldige i mindst 2 år.

Betegnelsen ”OCES” skal indgå i rodcertifikatets Common Name.

7.2.2 CA-nøglelagring, back-up og genskabelse

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 140-1 level 3, CWA 14167-2, eller højere. Det kryptografisk modul skal opbevares i henhold til kravene i 7.4.4.

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

7.2.3 CA's distribution af offentlig nøgle

CA skal sikre, at den offentlige nøgle overføres til CA sammen med oplysninger i en meddelelse signeret med certifikatindehaverens private nøgle ifølge den procedure, som er beskrevet i 7.3.1.

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 certifikatindehaveres private nøgler til afsender og meddelelsesautencitet, herunder elektronisk signatur samt meddelelsesintegritet ikke

opbevares eller kan genskabes hos CA, uden certifikatindehaverens skriftlige godkendelse.

CA skal sikre, at certifikatindehaverens 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-virksomhedscertifikater.

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'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 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 destrueres, hvis de kryptografiske moduler til certifikat- og statusinformationssignering kasseres.

7.2.8 CA'ens nøglehåndteringstjeneste

CA skal sikre, orientere certifikatindehaver om, at nøglepar skal genereres og opbevares på den af CA anviste måde.

Der er ikke specifikke krav til kontrol af OCES-certifikatindehaverens private nøgle.

Den private nøgle kan opbevares på harddisk, diskette eller lignende.

CA skal orientere certifikatindehaveren om, at den private nøgle hos denne skal være krypteret og beskyttet af aktiveringskode samt, at der skal benyttes en standard efter CA's anvisning.

CA skal orientere certifikatindehaver om, at en evt. sikkerhedskopi af den private nøgle hos denne skal opbevares i krypteret form på betryggende vis. CA kan anvise metode, der skal følges.

CA skal sikre, at aktiveringskode til aktivering af den private nøgle genereres og indtastes i forbindelse nøglegenereringen.

CA skal sikre, at den private nøgle er aktiveret, når certifikatindehaveren har angivet aktiveringskode.

CA skal orientere certifikatindehaveren om, at denne skal beskytte aktiveringskoden, så andre ikke får kendskab til disse. CA skal desuden orientere om, at den private nøgle anses for kompromitteret og spærres, hvis andre får kendskab til aktiveringskoden.

CA skal orientere certifikatindehaveren om, at en den anvendte tegnbaserede aktiveringskode, skal være mindst 8 tegn og at denne skal skiftes hver 3. måned samt at repræsentation af anden aktiveringskode er mindst 128 bit lang. Dog accepteres fire cifrede aktiveringskoder i miljøer, der effektivt kan spærre for udtømmende søgninger, eksempelvis smartcard, USB-tokens og lignende.

CA skal orientere certifikatindehaveren om, at den private nøgle skal overskrives, når den ikke længere skal benyttes.

7.3 PKI-certifikathåndtering

7.3.1 Registrering af certifikatindehaver

RA skal sikre, at certifikatindehaveren besidder den private nøgle, som svarer til den offentlige nøgle, som præsenteres i certifikatansøgningen. Det er tilstrækkeligt at verifikationen sker ved, at certifikatindehaveren signerer certifikatansøgningen med sin private nøgle. Den verificerende RA skal validere signaturen vha. den offentlige nøgle givet i certifikatansøgningen.

Der er ikke krav om personlig fremmøde.

RA skal sikre, at certifikatindehaver forud for udstedelsen af et OCES-virksomhedscertifikat fremsender relevant legitimation, der mindst skal omfatte virksomhedens navn, e-postadresse og CVR-postadresse.

CA skal etablere en procedure, der sikrer, at:

- nøglepar genereres
- den offentlige nøgle overføres til CA signeret med den private nøgle
- rodcertifikatet er installeret hos OCES-certifikatindehaver
- rodcertifikatet kan verificeres via anden kanal
- OCES-certifikatindehaverens CVR-postadresse verificeres ved brug af disse oplysninger i tilmeldingsprocessen
- evt. afdelingsnavn verificeres gennem bemyndigede
- OCES-certifikatindehaveren udstyres med en engangskode, fremsendt via pinkodebrev til bemyndiget
- 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 CA's ansvar at verificere, at bemyndigede er godkendt af virksomhedens ledelse
- tidspunkt og dato for udstedelsen af certifikatet efterfølgende kan fastlægges

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.

RA skal godkende en certifikatansøgning hvis:

- proceduren gennemføres som anvist
- ansøgeren er godkendt til at modtage et OCES-certifikat
- ansøgeren kan verificeres via CVR-registeret, og
- ansøgeren giver korrekt engangskode i højst 5 forsøg

CA skal sikre, at der fra en 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

CA skal godkende bevis for besiddelsen af den private nøgle som værende tilstrækkelig autentifikation i det tilfælde, hvor et nøglepar skal fornyes, uden at den private nøgle er blevet kompromitteret.

Efter spærring skal CA benytte samme procedure til fornyelse som ved førstegangsvalideringen.

Fornyelse af OCES-certifikat betyder udstedelse af et nyt certifikat med det samme navn og information som i det gamle certifikat, men med en ny nøgle, ny gyldighedsperiode og et nyt certifikat-serienummer.

Et certifikat kan blive fornyet, hvis nøglernes gyldighedsperiode ikke er udløbet, den private nøgle ikke er kompromitteret og hvis oplysningerne i certifikatet er uforandrede.

Et OCES-certifikat må fornyes for to år ad gangen og kan kun fornyes én gang.

Certifikatindehaveren kan anmode om fornyelse inden udløb af nuværende OCES-certifikat.

CA skal senest 14 dage før udløb notificere certifikatindehaveren via e-post til den i certifikatet angivne e-postadresse eller til CVR-postadressen.

CA skal acceptere anmodning om fornyelse af OCES-certifikat, hvis OCES-certifikatet, der skal fornyes, ikke er spærret.

CA skal sikre, at anmodningen om fornyelse signeres med certifikatindehaverens private nøgle.

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

CA skal sikre, at udstedelsen af nyt OCES-certifikat med ny nøgle kan ske enten efter spærring af gammelt OCES-certifikat eller efter udløb af gyldighed for nøglepar.

CA skal sikre, at certifikatindehaveren kan anmode om fornyelse.

CA skal sikre, at behandlingen af anmodning om nyt OCES-certifikat ved nøglefornyelse sker efter samme retningslinjer, som angivet i 7.3.1.

CA skal sikre, at et nyt certifikat udstedes, når oplysninger i OCES-certifikatet ændres, så som navn, postadresse og e-postadresse.

CA skal sikre, at certifikatindehaveren mod behørig identifikation kan anmode om fornyelse af OCES-certifikat.

CA skal sikre, at behandling af anmodning om nyt OCES-certifikat med ændret information sker efter retningslinjerne, som angivet i 7.3.1.

7.3.3 Certifikatgenerering

OCES-virksomhedscertifikater skal benytte Forum for Digital Signatur's certifikatprofil, FDS-certifikat-profilen, for kvalificerede certifikater, idet dog QcStatement ikke angiver, at der er tale om et kvalificeret certifikat.

OCES-virksomhedscertifikater 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
Certifikatindehaverens 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 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 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.
Eventuelle beløbsmæssige begrænsninger med hensyn til de transaktioner, for hvilke certifikatet kan anvendes	QcStatement i OID: id-etsi-qcs-QcLimitValue

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-nr konkateneret med et løbenummer
commonName	M	Certifikatindehaverens navn plus evt afdeling adskilt af "-"
postalAddress	O	Virksomhedens postadresse
emailAddress	O	Virksomhedens e-postadresse

Eksempel:
"countryName=DK,
organizationName= // CVR:
commonName= navn
emailAddress= <navn>@<gyldigt DNS domæne>
serialNumber=CVR: "

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

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)

nonRepudiation specifikationen (**nonRepudiation(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 anvendes til autentifikation og signatur, skal følgende specifikationer være sat til:
digitalSignature (0)

nonRepudiation specifikationen (**nonRepudiation(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 spefikationer 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	(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.

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

7.3.4 Certifikatbetingelser

Der er ikke angivet specifikke krav til OCES-certifikatindehaveres kryptografiske moduler. CA skal overfor certifikatindehavere anvise kryptografiske moduler.

Skal certifikatindehaveres private nøgle overføres til kryptografisk modul skal dette ske i krypteret form.

OCES-certifikatindehaveres nøgler skal være RSA-nøgler af længde på mindst 1024 bit eller tilsvarende.

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

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

CA skal orientere signaturmodtagere om, at det er signaturmodtagers ansvar at kontrollere, at det formål, et certifikat søges anvendt til, er passende i forhold til anvendelsesbegrænsninger på OCES-certifikatet samt i øvrigt passende i forhold til niveauet af sikkerhed, som er beskrevet i denne CP.

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

CA skal orientere certifikatindehaver om, at den private nøgle ikke må benyttes 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.

CA skal orientere certifikatindehaver om, at et OCES-certifikat givet til en certifikatindehaver er gyldigt maksimum to år, hvorefter det kan fornyes.

7.3.5 Certifikatudbredelse

CA skal gøre følgende typer af information tilgængelige 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 slut-entiteter
- 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-virksomhedscertifikater i mindst to måneder efter udløb af gyldighedsperiode, undtagen de certifikater, som skal holdes hemmelige
- spærreliste for OCES-virksomhedscertifikater udstedt efter denne CP Spærrede OCES-virksomhedscertifikater skal forblive på spærrelisten i mindst to måneder efter udløb af gyldighedsperiode

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. Det skal her specielt fremhæves, at denne CP ikke stiller krav om krydscertificering, uafhængig tidsstemplingstjeneste eller arkivfunktion hos CA.

7.3.6 Certifikatspærring

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

- der er vished eller mistanke om, at certifikatindehaverens private nøgle er kompromitteret
- den private nøgle er ødelagt
- der er konstateret unøjagtighed i certifikatets indhold eller anden information knyttet til certifikatindehaveren
- certifikatindehaver er afgået ved døden
- certifikatindehaveren ønsker at afslutte brugen af OCES-certifikatet
- certifikatindehaveren er gået konkurs

CA bør spærre et certifikat, hvis CA får kendskab til, at certifikatindehaveren har mistet adgang til den private nøgle, fx. 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 certifikatindehavers 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 mulig f.eks. ved en kombination af navn, CVR-nummer, CVR-postadresse og e-postadresse.

De følgende kan anmode om spærring af certifikat:

- bemyndigede i virksomhed mod behørig dokumentation
- CA, hvis reglerne i denne CP ikke er overholdt, eller hvor forholdene i øvrigt tilsiger dette
- underskriftberettigede i virksomhed
- Tilsyn eller kurator, såfremt certifikatindehaveren har anmeldt betalingsstandsning eller tages under konkursbehandling
- en af Skifteretten udpeget bobestyrer eller arvinger efter certifikatindehavers, 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 enten 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. Certifikatindehaver kan kræve at få kvitteringen sendt med almindelig post.

CA skal sikre, at der ved anmodning via e-post angives årsag til spærring, og at e-posten signeres med den private nøgle. CA skal kvittere for spærring via signeret e-post til den oplyste e-postadresse. Certifikatindehaver kan kræve at få kvitteringen sendt 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 til den oplyste e-postadresse. Certifikatindehaver kan kræve at få kvitteringen sendt med almindelig post.

Hvis CA anmoder om spærring skal CA sende signeret e-postmeddelelse med angivelse af årsag til spærring. Certifikatindehaver kan kræve at få kvitteringen sendt med almindelig post.

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. kurator 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 evt. 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-virksomhedscertifikater.

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 er tilgængelige via Internet daglig mellem klokken 0 og 24. Tjenesterne skal have en gennemsnitlig svartid, der ikke overstiger 1 sek. 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 2459.
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.

Anvendes online kontrol, skal CA sikre, at enhver forespørgsel er elektronisk signeret og angiver OCES-certifikatets unikke identifikationsnummer.

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 bedre end 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 daglig mellem klokken 0 og 24. Tjenesterne skal have en gennemsnitlig svartid på Internet, der ikke overstiger 1 sek. 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 hver tid skal have ansvaret for en sikkerhedsmæssig korrekt drift af CA's funktioner.

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

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 indenfor 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 tilgængelig 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.

CA driftslokaler
CA driftslokaler skal defineres til et sikkerhedsniveau, og overholde kravene i DS 484 del 2.

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 med 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 CA-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 forekomme vandinstallationer i CA-driftslokaler, ej heller må vandinstallationer føres gennem CA-driftslokaler, jf. DS484 del 2, punkt S6.5.1.

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 gennem brug af hændelsesrapportering og hurtig indgriben.

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

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.

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

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 og beskytte disse med korrekt konfigurerede firewalls.

CA skal sikre, at følsom information 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, alle ændringer i rettigheder skal logges og der skal føres kontrol med disse log.

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.

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

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.

CA skal sikre, at der er alarmer for alle uautoriserede ændringer i data vedrørende 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 katastrofeplan, der kan bringe CA's drift tilbage til normal hurtigst muligt efter den alvorlige hændelse er indtrådt. Katastrofeplanen skal indeholde tiltag til at undgå, at lignende hændelser gentages.

CA skal i tilfælde af nøglekompromittering 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, programvare 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 og indtil alle OCES-spærrelister er udtømte, eventuelt ved overdragelse 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 Opfølgning på lovbestemte og kontraktlige krav

CA skal orientere certifikatindehavere og signaturmodtagere om, at det i tilfælde af tvistigheder, som ikke kan løses ved forhandling mellem parterne, er almindelig dansk lov, der er gældende.

CA skal sikre, at al brug af OCES-virksomhedscertifikater og tilhørende tjenester og applikationer sker under iagttagelse af reglerne i persondataloven.

CA skal sikre, at orientering om og tilladelse til brug af privat information følger reglerne herom i persondataloven.

CA skal sikre, at afgivelse af information kun kan ske under iagttagelse af reglerne herom i persondataloven.

7.4.11 Opbevaring af certifikatinformation

Den CA, der har udstedt et OCES-certifikat, er ansvarlig for etablering af et datalagringssystem, der skal indeholde alle data, der er nødvendig for sikker udførsel af alle de opgaver, som denne CA er pålagt. CA skal desuden sikre, at

- Al anden information beskyttes mod uretmæssig adgang
- Alle aktiviteter, der kræver deltagelse af mere end en person, 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 opbevares i minimum 5 år
- Alle audit-logs signeres elektronisk og tidsstemples
- Audit-logs behandles som fortroligt materiale
- Der foretages back-up af audit-logs med regelmæssig mellemrum

CA skal sikre, at back-up-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 i forbindelse med systemrevisionen foretages en sårbarhedsvurdering af logningsproceduren.

CA skal sikre, at følgende information arkiveres:

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

CA skal sikre, 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 regelmæssig mellemrum.

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

7.5 Organisatoriske aspekter

CA organisation skal være pålidelig.

CA skal være en registreret fysisk eller juridisk person.

CA skal sikre, at alle tjenester tilbydes til alle indenfor OCES-virksomhedscertifikaternes anvendelsesområde på lige fod. Dette betyder, at der ikke må gøre 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 hver tid have tilstrækkelig med uddannet personale til at kunne drive alle udbudte tjenester på forsvarlig vis. Personalet skal til hver 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.