DIGITALISERINGSSTYRELSEN

Offentlig certifikatpolitik for kvalificerede virksomhedscertifikater

Oktober 2021

Version 1.1

Indholdsfortegnelse

1. Introduktion 14

1.1 Oversigt 14

1.2 Dokumentnavn og -identifikation 15

1.2.1 Navngivning 15

1.2.2 Identifikation 15

1.3 PKI parter 15

1.3.1 Certificeringscenter (Certification Authorities eller CA) 15

1.3.2 Registreringstjeneste (Registration Authorities – RA) 16

1.3.3 Certifikatindehaver og certifikatholder 17

1.3.4 Modtagerparter 17

1.3.5 Andre parter 17

1.4 Certifikatanvendelse 17

1.4.1 Tilladt certifikatanvendelse 17

1.4.2 Ikke-tilladt certifikatanvendelse 17

1.5 Politik administration 18

1.5.1 Organisation, der administrerer dokumentet 18

1.5.2 Kontaktinformation 18

1.5.3 Entitet, der afgør CPS' overensstemmelse med politikken 18

1.5.4 CPS godkendelsesprocedure 18

1.6 Definitioner og forkortelser 19

1.6.1 Definitioner 19

1.6.2 Forkortelser 21

2. Ansvar for offentliggørelse 23

2.1 Repository 23

2.2 Offentliggørelse af certifikatinformation 24

2.3 Tid eller frekvens for offentliggørelse 25

2.4 Adgangskontrol for repository 25

3. Identifikation og autentifikation 25

3.1 Navngivning 25

3.1.1 Typer af navne 25

3.1.2 Krav om meningsfulde navne 25

3.1.3 Anonymitet og pseudonymisering af certifikatholder og -indehaver 26

3.1.4 Regler for fortolkning af forskellige navneformer 26

3.1.5 Entydighed af navne 26

3.1.6 Genkendelse, kontrol og betydning af varemærker 26

3.2 Initiel identitetskontrol 26

3.2.1 Metode til at bevise besiddelse af privat nøgle 27

3.2.2 Kontrol af organisationsidentitet 27

3.2.3 Kontrol af fysisk persons identitet 28

3.2.4 Ikke-kontrollerede information om certifikatholder 28

3.2.5 Kontrol af rettigheder 28

3.2.6 Kriterier for interoperabilitet 28

3.3 Identifikation og autentikation ved genudstedelse 28

3.3.1 Identifikation og autentikation ved fornyelse 28

3.3.2 Identifikation og autentikation ved genudstedelse efter spærring 28

3.4 Identifikation og autentikation ved anmodning om spærring 28

4. Operationelle krav i certifikatlivscyklus 29

4.1 Certifikatanmodning 29

4.1.1 Hvem kan anmode om certifikat 29

4.1.2 Tilslutningsproces og ansvarsfordeling 29

4.2 Behandling af certifikatanmodning 30

4.2.1 Gennemførsel af identifikation og autentifikation 30

4.2.2 Godkendelse eller afvisning af certifikatanmodning 30

4.2.3 Tidsfrister for behandling af certifikatanmodning 30

4.3 Certifikatudstedelse 30

4.3.1 CA opgaver ved certifikatudstedelse 30

4.3.2 CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatudstedelse 31

4.4 Accept af certifikat 31

4.4.1 Handling, der betragtes som certifikatholders certifikataccept . 31

4.4.2 CA's offentliggørelse af certifikatet 32

4.4.3 CA's notifikation til andre parter om certifikatudstedelse 32

4.5 Nøglepar og certifikatanvendelse 32

4.5.1 Certifikatholders anvendelse af privat nøgle og certifikat 32

4.5.2 Modtagerparts anvendelse af offentlig nøgle og certifikat 34

4.6 Certifikatgenudstedelse 34

4.6.1 Årsag til certifikatgenudstedelse 34

4.6.2 Hvem kan anmode om certifikatgenudstedelse 34

4.6.3 Behandling af anmodning om certifikatgenudstedelse 34

4.6.4 CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatgenudstedelse 35

4.6.5 Handling, der betragtes som certifikatholders certifikataccept . 35

4.6.6 CA's offentliggørelse af genudstedt certifikat 35

4.6.7 CA's notificering til andre parter om certifikatgenudstedelse ... 35

4.7 Certifikatfornyelse 35

4.7.1 Årsag til certifikatfornyelse 35

4.7.2 Hvem kan anmode om certifikatfornyelse 36

4.7.3 Behandling af anmodning om certifikatfornyelse 36

4.7.4 CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatfornyelse 36

4.7.5 Handling, der betragtes som certifikatholders certifikataccept . 36

4.7.6 CA's offentliggørelse af fornyet certifikat 36

4.7.7 CA's notifikation til andre parter om certifikatfornyelse 36

4.8 Certifikatopdatering 36

4.8.1 Årsag til certifikatopdatering 36

4.8.2 Hvem kan anmode om certifikatopdatering 37

4.8.3 Behandling af anmodning om certifikatopdatering 37

4.8.4 CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatopdatering 37

4.8.5 Handling, der betragtes som certifikatholders certifikataccept . 37

4.8.6 CA's offentliggørelse af opdateret certifikat 37

4.8.7 CA's notifikation til andre parter om certifikatopdatering..... 37

4.9 Certifikatspærring og -suspendering 37

4.9.1 Årsager til spærring 37

4.9.2 Hvem kan anmode om spærring..... 38

4.9.3 Procedure for anmodning om spærring..... 38

4.9.4 Tidsfrister for anmodning om spærring..... 39

4.9.5 Tidsfrister for CA's håndtering af anmodninger om spærring.. 39

4.9.6 Krav til modtagerparters verifikation af certifikatstatus..... 39

4.9.7 Udstedelsesfrekvens for spærrelister 39

4.9.8 Maksimal forsinkelse for offentliggørelse af spærrelister 40

4.9.9 Understøttelse af online statuskontrol 40

4.9.10 Krav til modtagerparters online kontrol af certifikatstatus..... 40

4.9.11 Andre muligheder for kontrol af certifikatstatus..... 40

4.9.12 Særlige krav i forbindelse med spærring pga. nøglekompromittering 40

4.9.13 Årsager til suspendering..... 40

4.9.14 Hvem kan anmode om suspendering 40

4.9.15 Procedure for suspenderingsanmodning..... 40

4.9.16 Begrænsninger på suspenderingsperiode..... 41

4.10 Certifikatstatusservice 41

4.10.1 Operationelle karakteristika..... 41

4.10.2 Tilgængelighed af service 42

4.10.3 Ekstra funktioner 42

4.11 Certifikatholder eller -indehavers ophør af anvendelse af tjenesten 42

4.12 Nøgledeponering og -genopretning 43

4.12.1 Politik for nøgledeponering 43

4.12.2 Sessionsnøgle indkapsling samt politikker og procedure for genskabelse 43

5. Fysiske, administrative og operationelle kontroller 43

5.1 Fysiske kontroller 43

5.1.1 Placering og opbygning af lokaliteter 44

5.1.2 Fysisk adgang 44

5.1.3 Strømforsyning og air conditioning 45

5.1.4 Vandindtrængning 45

5.1.5 Brandbeskyttelse 45

5.1.6 Håndtering af lagringsmedie 45

5.1.7 Bortskaffelse af affald 46

5.1.8 Off-Site sikkerhedskopi 46

5.2 Administrative kontroller 46

5.2.1 Betroede roller 46

5.2.2 Antal krævede personer per opgave 47

5.2.3 Identifikation og autentikation for hver rolle 47

5.2.4 Roller der ikke kan besættes af samme person (Separation of Duties) 47

5.3 Personalesikkerhed 47

5.3.1 Kvalifikationer, erfaring og godkendelseskrav 47

5.3.2 Procedure for baggrundscheck 48
5.3.3 Uddannelseskrav 48
5.3.4 Frekvens for og krav til efteruddannelse 48
5.3.5 Frekvens og regler for jobrotation 48
5.3.6 Sanktioner ved uautoriserede handlinger 48
5.3.7 Krav til uafhængige kontraktansatte 48
5.3.8 Dokumentation og uddannelsesmateriale til personale 48
5.4 Audit logningsprocedurer 49
5.4.1 Type af hændelser, der skal logges 49
5.4.2 Frekvens for processering af auditlog 49
5.4.3 Opbevaringstid for auditlog 49
5.4.4 Beskyttelse af auditlog 49
5.4.5 Procedure for sikkerhedskopi for auditlog 50
5.4.6 Auditsystem (intern eller ekstern) 50
5.4.7 Notifikation til part, der var årsag til logningshændelse 50
5.4.8 Sårbarhedsvurdering 50
5.5 Datalagring 50
5.5.1 Type af data der skal lagres 50
5.5.2 Lagringstid for data 51
5.5.3 Beskyttelse af lagrede data 51
5.5.4 Procedure for sikkerhedskopiering af lagrede data 51
5.5.5 Krav til tidsstempling af lagrede data 52
5.5.6 Lagringssystemer (interne eller eksterne) 52

5.5.7 Procedure for fremsøgning og verifikation af lagrede data 52

5.6 Skift af nøgler 52

5.7 Kompromittering og beredskabsplanlægning 52

5.7.1 Hændelses- og kompromitteringshåndtering 53

5.7.2 Skader på hardware, software og/eller data 54

5.7.3 Procedure ved privatnøglekompromittering 54

5.7.4 Business Continuity kapaciteter efter en kritisk hændelse 55

5.8 Ophør af CA eller RA 55

6. Tekniske sikkerhedskontroller 56

6.1 Generering og installation af nøglepar 56

6.1.1 Generering af nøglepar 56

6.1.2 Levering af privat nøgle til certifikatholder 58

6.1.3 Levering af offentlig nøgle til certifikatudsteder 59

6.1.4 Levering af CA's offentlige nøgle til modtagerparter 59

6.1.5 Nøglelængder 59

6.1.6 Generering og kvalitetskontrol af offentlig nøgle parametre 59

6.1.7 Nøgleanvendelsesformål (X.509v3 keyUsage) 59

6.2 Beskyttelse af private nøgler og anvendelse af kryptografiske moduler 60

6.2.1 Kryptografiske moduler – standarder og evalueringer 60

6.2.2 Privat nøgle (n ud af m) multi-person kontrol 60

6.2.3 Nøgledeponering 60

6.2.4 Sikkerhedskopiering af privat nøgle 61

6.2.5 Arkivering af privat nøgle 61

6.2.6 Overførsel af privat nøgle til eller fra et kryptografisk modul... 61
6.2.7 Lagring af privat nøgle i kryptografisk modul 61
6.2.8 Aktivering af privat nøgle 61
6.2.9 Deaktivering af privat nøgle 62
6.2.10 Destruktion af privat nøgle..... 62
6.2.11 Klassificering af kryptografisk modul 62
6.3 Andre aspekter af nøglehåndtering..... 62
6.3.1 Lagring af offentlige nøgler 63
6.3.2 Anvendelsesperiode for certifikat og nøglepar..... 63
6.4 Aktiveringsdata 63
6.4.1 Generering og installation af aktiveringsdata..... 63
6.4.2 Beskyttelse af aktiveringsdata 63
6.4.3 Andre aspekter ved aktiveringsdata..... 64
6.5 IT-sikkerhedskontroller 64
6.5.1 Særlige tekniske krav til IT-sikkerhed 64
6.5.2 Klassificering af IT-sikkerhed 64
6.6 Tekniske kontroller for livscyklus 65
6.6.1 Kontroller relateret til systemudvikling..... 65
6.6.2 Kontroller relateret til informationssikkerhedsledelse..... 65
6.6.3 Kontroller relateret til systemer sikkerhedslivscyklus 66
6.7 Sikkerhedskontroller for netværk..... 66
6.8 Tidsstempling..... 67
7. Profiler for certifikater, spærrelister og OCSP..... 68

7.1 Certifikatprofil 68
7.1.1 Versionsnummer 68
7.1.2 Certifikat-extensions 68
7.1.3 Algoritme object identifiers 69
7.1.4 Navneformer 69
7.1.5 Navnebegrænsninger 70
7.1.6 Certifikat politik object identifier 70
7.1.7 Extension for politikanvendelsesbegrænsninger 70
7.1.8 Policy qualifiers - syntaks and semantic 70
7.1.9 Semantik for processering af kritisk certifikatpolitik extension 70
7.2 Spærrelisteprofil 71
7.2.1 Versionsnummer 71
7.2.2 CRL og CRL entry extensions 71
7.3 OCSP-profile 71
7.3.1 Versionsnummer 71
7.3.2 OCSP extension 71
8. Overensstemmelsesvurdering og andre vurderinger 72
8.1 Frekvens og baggrund for systemrevision 72
8.2 Systemrevisors identitet og kvalifikationer 72
8.3 Systemrevisors relation til den reviderede part 72
8.4 Emner omfattet af systemrevision 72
8.5 Krævede handlinger som følge af fundne mangler 72
8.6 Rapportering af resultater 72

9. Andre forretningsmæssige og juridiske anliggender 73

9.1 Vederlag 73

9.1.1 Vederlag for udstedelse og fornyelse af certifikater 73

9.1.2 Vederlag for adgang til certifikat 73

9.1.3 Vederlag for adgang til spærrings- og statusinformation 73

9.1.4 Vederlag for andre services 73

9.1.5 Vilkår for tilbagebetaling 73

9.2 Økonomisk ansvar 74

9.2.1 Forsikringsdækning 74

9.2.2 Øvrige aktiver 74

9.2.3 Forsikringsdækning eller garanti for slutbrugere 74

9.3 Fortrolighed i forhold til forretningsdata 74

9.3.1 Omfang af fortrolighed 74

9.3.2 Hvad er ikke omfattet af fortrolighed 74

9.3.3 Ansvar for beskyttelse af fortrolig information 74

9.4 Behandling af personoplysninger 74

9.4.1 Plan for privatlivsbeskyttelse 74

9.4.2 Persondata, der betragtes som fortrolige 75

9.4.3 Persondata, der ikke betragtes som fortrolige 75

9.4.4 Ansvar for beskyttelse af fortrolige persondata 75

9.4.5 Underretning og samtykke 75

9.4.6 Videregivelse i henhold til retslige eller administrative processer 75

9.4.7 Andre årsager til videregivelse 75

9.5 Rettigheder 75
9.6 Garantier 75
9.6.1 CA's garantier 75
9.6.2 RA's garantier 76
9.6.3 Certifikatholder/-indehavers garantier 76
9.6.4 Modtagerparts garantier 76
9.6.5 Andre parters garantier 76
9.7 Begrænset hæftelse 76
9.8 Ansvarsbegrænsninger 76
9.9 Skadesløsholdelse 77
9.10 Varighed og ophør 77
9.10.1 Varighed 77
9.10.2 Opsigelse 77
9.10.3 Ophør 77
9.11 Personlige meddelelser og kommunikation mellem parterne 77
9.12 Tillæg 77
9.12.1 Ændringshåndtering 77
9.12.2 Notifikationsmekanisme og -varsler 77
9.12.3 Situationer, der betinger ændring af OID 77
9.13 Tvistligheder 77
9.14 Lovvalg 77
9.15 Overholdelse af gældende lovgivning 78
9.16 Diverse bestemmelser 78

9.16.1 Aftalens elementer 78
9.16.2 Overdragelse 78
9.16.3 Fortolkning 78
9.16.4 Håndhævelse 78
9.16.5 Force Majeure 78
9.17 Øvrige bestemmelser 78
Bilag A 80

1. Introduktion

Denne certifikatpolitik (CP) er udarbejdet af og administreres af Digitaliseringsstyrelsen i Danmark. Digitaliseringsstyrelsen er den offentlige myndighed, som har tilsynsansvaret for tillidstjenesteudbydere i Danmark. Digitaliseringsstyrelsen 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 https://certifikat.gov.dk.

Kvalificeret signatur og kvalificeret segl bruges til at sikre autenticitet og integritet af data i elektronisk form. Anvendelsen af kvalificerede signatur og segl forudsætter i praksis, at der er etableret en offentlig nøgleinfrastruktur (PKI). Digitaliseringsstyrelsen har udarbejdet et sæt af kvalificerede certifikatpolitikker for henholdsvis privatpersoner, medarbejder- og virksomhedscertifikater. Desuden har Digitaliseringsstyrelsen udarbejdet et sæt af OCES-certifikatpolitikker.

Kvalificerede CP'er udgør sammen med OCES-CP'er en fællesoffentlig standard, der regulerer udstedelsen og anvendelsen af certifikater til elektroniske signaturer og elektroniske segl.

Kvalificerede tillidstjenesteudbydere, der udsteder kvalificerede certifikater, kan anvendes disse kvalificerede CP'er udarbejdet og administreret af Digitaliseringsstyrelsen, men kan også anvende egenudviklede kvalificerede CP'er, så længe de opfylder krav i eIDAS-forordningen inklusiv tilhørende regulering.

Kravene i Digitaliseringsstyrelsens kvalificerede CP'er er i overensstemmelse med krav til *Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD*, forkortet QCP-l-qscd jf. de europæiske standarder ETSI EN 319 401, ETSI EN 319 411-1 og ETSI EN 319 411-2. Afbildning af krav fra denne CP og ETSI EN 319 401, ETSI EN 319 411-1 samt ETSI EN 319 411-2 findes i bilag A.

Kravene anført i denne CP omfatter:

1. Obligatoriske krav, der skal opfyldes. Disse krav er anført med "skal".
2. Krav, der beskriver forbud i forhold til opfyldelse af denne CP, er anført med "må ikke".
3. Krav, der bør opfyldes. Opfyldes kravene ikke, skal der gives begrundelse herfor. Disse krav er anført med "bør".
4. Krav, der kan opfyldes, hvis CA ønsker det. Disse krav er anført med "kan".

1.1 Oversigt

Denne certifikatpolitik beskriver generelle retningslinjer for udstedelsen af et kvalificeret certifikat udstedt til en juridisk enhed (kvalificeret virksomhedscertifikat).

CP'en er udarbejdet med udgangspunkt i RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

Certifikatpolitikkens bestemmelser om hvordan CA skal agere, giver et højt niveau af sikkerhed for, at certifikatholderen har den identitet, der fremgår af certifikatet.

Certifikatindehavernes og modtagerparternes tillid kan således baseres på certifikatpolitikken og den tilhørende EU-regulering herunder Digitaliseringsstyrelsens løbende tilsyn med CA.

Certificeringscentre under dansk tilsyn, som udsteder kvalificerede certifikater, er offentliggjort på hjemmesiden: https://certifikat.gov.dk.

1.2 Dokumentnavn og -identifikation

1.2.1 Navngivning

Dette dokument med navnet "Offentlig certifikatpolitik for kvalificerede virksomhedscertifikater version 1.0" forkortet VQ-CP beskriver certifikatpolitik for kvalificerede certifikater til juridiske enheder, hvor den juridiske enheds seglgenereringsdata er beskyttet af et kvalificeret signaturgenereringssystem (QSCD).

1.2.2 Identifikation

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

OCES-virksomhedscertifikat:

iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) virksomhed(3) major-ver(1) minor-ver(1)

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

1.3 PKI parter

1.3.1 Certificeringscenter (Certification Authorities eller CA)

Et certificeringscenter (CA) er en fysisk person eller juridisk enhed, der er betroet af både certifikatindehavere og modtagerparter til at generere, udstede og administrere elektroniske certifikater. 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.

[KRAV 1.3.1-01] CA's organisation skal være pålidelig.

[KRAV 1.3.1-02] CA skal være en registreret fysisk person eller juridisk enhed.

[KRAV 1.3.1-03] CA kan samarbejde med andre parter for at tilbyde dele af de samlede CA-tjenester, men CA har altid det overordnede ansvar for alle handlinger vedrørende håndtering af certifikater, ligesom CA er ansvarlig for, at kravene i denne CP til CA's tjenester altid er overholdt.

En PKI kan indeholde et hierarki af CA'er, hvor øverste CA i hierarkiet benævnes rod-CA. Et rod-CA har et selvudstedt certifikat benævnt rodcertifikat med et tilhørende nøglepar benævnt hhv. offentlig og privat rodnøgle.

[KRAV 1.3.1-04] CA kan subcertificere sin offentlige rodnøgle under andre overliggende CA'er. En CA's rodnøgle kan også subcertificere en anden underliggende CA's offentlige rodnøgle, såfremt denne er en kvalificeret tillidstjeneste. Rod-CA er ansvarlig for at sikre at ethvert underliggende CA efterlever eIDAS krav til kvalificerede tillidstjenester, der udsteder kvalificerede certifikater.

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

- Registrering: Verificering af certifikatholderens identitet og eventuelle tilhørende id- og registreringsoplysninger. Resultatet af registreringen overgives til certifikatgenereringen. Denne funktion foretages af RA på vegne af CA.
- Certifikatgenerering: Generering og elektronisk signering af certifikater baseret på den verificerede identitet og eventuelle andre id- og registreringsoplysninger fra registreringen. Certifikatgenerering omfatter udstedelse, genudstedelse og fornyelse af certifikater
- Certifikatdistribution: Distribution af certifikater til certifikatholdere.
- Katalogtjeneste: Offentliggørelse af certifikater, så modtagerparter 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 certifikater.

1.3.2 Registreringstjeneste (Registration Authorities – RA)

Registreringstjenesten (RA) varetager identifikationen og registreringen af certifikatholdere på vegne af CA inden udstedelse og genudstedelse af certifikat.

RA kan enten være nøje knyttet til CA'en, eller den kan være en selvstændig funktion. CA hæfter under alle omstændigheder for RA's opfyldelse af de stillede krav og forpligtelser på ganske samme måde som for sine egne forhold. Der er det CA's ansvar at sikre, at RA følger de bestemmelser, som er fastlagt i denne CP.

[KRAV 1.3.2-01] CA skal sikre, at RA:

- verificerer ansøgerens identitet og oplysninger og
- opretholder et teknisk driftsmiljø i overensstemmelse med kravene i denne CP.

Note: CA skal kun sikre, at den del af RA's tekniske driftsmiljø, der er relateret til CA's tjeneste opretholdes i overensstemmelse med kravene i denne CP. Dette omfatter fx terminaler, der benyttes til registrering af certifikatholdere, men ikke driftsaktiver, der ikke kan påvirke RA's services for CA.

1.3.3 Certifikatindehaver og certifikatholder

Forud for udstedelse af certifikater indgår CA en aftale med certifikatindehaveren i egenskab af den virksomhed (juridiske enhed), der ønsker certifikater til fysiske eller logiske enheder tilknyttet certifikatindehaveren. Den enhed tilknyttet certifikatindehaveren, der registreres og får udstedt et certifikat, benævnes certifikatholder.

I denne CP benyttes termerne certifikatindehaver og certifikatholder for at skelne mellem den, der har indgået aftale med en CA, og den fysiske eller logiske enhed, der er identificeret i certifikatet.

Det er certifikatindehaveren, der har det endelige ansvar for brugen af certifikatet og de tilhørende private nøgler, selvom det er certifikatholderen, der håndterer den private nøgle.

1.3.4 Modtagerparter

En modtagerpart er den part, der fæster tillid til et certifikat udstedt af CA. Det kan typisk være en fysisk person eller juridisk enhed, der modtager et elektronisk signeret dokument eller autentificere en certifikatholder ved anvendelse af PKI.

1.3.5 Andre parter

CA'er, der udsteder certifikater efter denne CP er kvalificerede tillidstjenesteleverandører jf. eIDAS og er i denne sammenhæng omfattet af tilsyn som beskrevet i eIDAS Kapitel III. I Danmark er Digitaliseringsstyrelsen tilsynsførende myndighed i forhold til eIDAS.

1.4 Certifikatanvendelse

1.4.1 Tilladt certifikatanvendelse

[KRAV 1.4.1-01] Et kvalificeret virksomhedscertifikat kan anvendes til sikring af afsender- og meddelelsesautenticitet, herunder kvalificeret elektronisk segl samt meddelelsesintegritet. Det kan også anvendes til at sikre hemmeligholdelse (kryptering).

Note: Bemærk dog afgrænsninger i afsnit 1.4.2.

[KRAV 1.4.1-02] Certifikater udstedt under denne CP kan være gyldige i maksimalt 4 år.

1.4.2 Ikke-tilladt certifikatanvendelse

[KRAV 1.4.2-02] Certifikater udstedt under denne CP må ikke anvendes til signering af andre certifikater.

[KRAV 1.4.2-03] Certifikatholders private nøgle må ikke anvendes uden i hvert tilfælde at være autoriseret af certifikatholder.

[KRAV 1.4.2-04] Certifikatholders private nøgle må ikke anvendes ud over det i certifikatets keyUsage angivne jf. KRAV 7.1.2-04.

1.5 Politik administration

1.5.1 Organisation, der administrerer dokumentet

Denne CP er ejet og vedligeholdt af Digitaliseringsstyrelsen.

1.5.2 Kontaktinformation

Forespørgsler vedrørende denne CP kan rettes til:

Digitaliseringsstyrelsen

Landgreven 4

1301 København K

Telefon: 3392 5200

E-mail: digst@digst.dk

1.5.3 Entitet, der afgør CPS' overensstemmelse med politikken

[KRAV 1.5.3-01] CA kan udstede kvalificerede certifikater under denne CP, hvis CA er anmeldt til Digitaliseringsstyrelsen jf. eIDAS artikel 21.

[KRAV 1.5.3-02] CA skal forelægge Digitaliseringsstyrelsen en overensstemmelsesvurderingsrapport mindst én gang årlig.

1.5.4 CPS godkendelsesprocedure

[KRAV 1.5.4-01] CA skal udfærdige en certificeringspraksis (CPS), der adresserer alle krav i denne CP. CPS'en skal også omfatte alle eksterne organisationer, der understøtter CA's tjeneste og skal være i overensstemmelse med denne CP. CPS kan være delt op i en offentlig og en privat del, hvor den offentlige del af CPS offentliggøres.

Note: Eksterne organisationer i ovenstående krav omfatter eventuelle underleverandører herunder ekstern RA.

[KRAV 1.5.4-02] CPS skal udformes med henblik på løbende at kunne fortage konkret måling på effektivitet, kvalitet og sikkerhed.

[KRAV 1.5.4-03] CPS skal inkludere det samlede CA-hierarki, herunder rod-CA og underliggende CA'er.

[KRAV 1.5.4-04] CPS skal være struktureret efter retningslinjerne i RFC 3647.

[KRAV 1.5.4-05] CPS skal være på dansk eller engelsk.

[KRAV 1.5.4-06] CPS skal beskrive de anvendte signaturalgoritmer og tilhørende parametre i den offentlige del. Desuden skal den offentlige del af CPS beskrive praksis vedrørende brug af CA nøgler til underskrivelse af certifikater, CRL og OCSP.

[KRAV 1.5.4-07] CA's ledelse skal have ansvaret for og godkende den samlede CPS og sikre korrekt implementering herunder at CPS'en er kommunikeret til relevante medarbejdere og partnere.

[KRAV 1.5.4-08] CPS skal gennemgås og revideres regelmæssigt og mindst én gang årligt. Ansvar for vedligehold af CPS skal fastlægges og dokumenteres. Ændringer i CPS skal dokumenteres.

1.6 Definitioner og forkortelser

1.6.1 Definitioner

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

Aktiveringsdata: Data, der kan aktivere anvendelse af certifikatholders private nøgle(r). Dette kan fx være et kodeord.

Bemyndiget: Person eller logisk enhed, der af en ledelsesrepræsentant med nødvendig prokura hos certifikatindehaver er givet bemyndigelse til på virksomhedens vegne at registrere certifikatholdere og administrere certifikater for certifikatindehavere.

Certificeringscenter ("certification authority" – "CA"): En fysisk person eller juridisk enhed, der som tillidstjenesteudbyder genererer, udsteder og administrerer certifikater. I eIDAS forordningen benyttes betegnelsen certificeringstjenesteudbyder for denne enhed.

Certificeringspraksis ("Certification Practice Statement" – "CPS"): En specifikation af hvilke principper og procedurer, en CA anvender ved udstedelse af certifikater til opfyldelse af tilhørende CP'er. Se evt. beskrivelse i RFC 3647 afsnit 3.4.

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

Certifikatindehaver ("subscriber"): En fysisk person eller juridisk enhed, der indgår aftale med det udstedende certificeringscenter (CA) om udstedelse af certifikater til en eller flere certifikatholdere.

Certifikatholder ("subject"): En fysisk person eller en enhed hos en certifikatindehaver, som i certifikatet er identificeret som den rette anvender af den private

nøgle, hørende til den offentlige nøgle, der er givet i certifikatet, og til hvem et kvalificeret certifikat enten er under udstedelse eller er blevet udstedt.

Certifikatpolitik ("certificate policy"): Et sæt regler, der angiver krav til udstedelse og brug af certifikater i en eller flere specifikke sammenhænge, hvor der findes fælles sikkerhedskrav. Se evt. beskrivelse i RFC 3647 afsnit 3.1.

Databeskyttelsesloven: Lov nr 502 af 23/05/2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

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

Egenkontrol ("Sole control"): Egenskab, hvor det med tidssvarende tekniske og administrative foranstaltninger er sikret, at en given enhed alene har kontrol med anvendelsen af en ressource.

Eksempler:
En certifikatholder (enhed), kan have egenkontrol med en privat signeringsnøgle (ressource), ved at nøglen er placeret sikkert på et kryptografisk hardwaremodul, hvor aktiveringen af nøglen er baseret på noget som kun ihændehaves og kendes af certifikatholderen.

ISO 27001: "ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems" samt efterfølgende rettelser som fx Cor 1:2014 og Cor 2:2015.

ISO 27002: "ISO/IEC 27002:2013 - Information technology -- Security techniques – Code of practice for information security controls" samt efterfølgende rettelser som fx Cor 1:2014 og Cor 2:2015.

Kvalificeret certifikat: "Kvalificeret certifikat for elektronisk signatur" eller "kvalificeret certifikat for elektronisk segl" som defineret i eIDAS i hhv. artikel 3 litra 15) og artikel 3 litra 30).

Kvalificeret signaturgenereringssystem ("qualified signature creation device (QSCD)"): "Kvalificeret elektronisk signaturgenereringssystem" eller "kvalificeret elektronisk seglgenereringssystem" som defineret i eIDAS i hhv. artikel 3 litra 23) og artikel 3 litra 32).

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.

Modtagerpart ("relying party"): en fysisk person eller juridisk enhed, der er afhængig af en CA som tillidstjeneste.

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

Overensstemmelsesvurderingsorgan: Juridisk enhed, der auditerer CA's overholdelse af nærværende certifikatpolitik. Se afsnit 8 for krav til overensstemmelsesvurderingsorgan.

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

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

Rod-CA: Øverste CA i et hierarki af CA'er.

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 ("self signed").

Rodnøgle: Rod-CA's private og offentlige nøgler, som anvendes til at signere certifikater og spærrelister.

Sikringsniveau (”Level of Assurance (LoA)”): Graden af tillid til en autentificeret elektronisk identitet.

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

1.6.2 Forkortelser

AIA	“Authority Information Access”
BCP	“Business Continuity Plan”
CA	Certificeringscenter (“Certificate Authority”)
CEN	“European Committee for Standardization”
CP	Certifikatpolitik (“Certificate Policy”)

CPS	Certificeringspraksis ("Certification Practice Statement")
CRL	Spærreliste ("Certificate Revocation List")
CVR	Central Virksomhed Register
eIDAS	EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF
ENISA	"The European Union Agency for Network and Information Security"
ETSI	"European Telecommunications Standards Institute"
GDPR	EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF
IETF	"Internet Engineering Task Force"
ISO	"International Organization for Standardization"
KSC	Nøgleceremoni ("Key Signing Ceremony")
LDAP	"Lightweight Directory Access Protocol"
NCP	"Normalized Certificate Policy"
NSIS	"National Standard for Identiteters Sikringsniveau"
OCES	"Offentlige Certifikater til Elektronisk Service"
OCSP	"Online Certificate Status Protocol"
OID	Object identifier, jf. ITU-T's ASN.1 standard
PKI	"Public Key Infrastructure"
QSCD	"Qualified Signature Creation Device"
RA	"Registration Authority"

UTC	Fælles tidsangivelse ("Universal Time Coordinated")
UUID	"Universally Unique Identifier"

2. Ansvar for offentliggørelse

2.1 Repository

[KRAV 2.1-01] CA-praksis skal til enhver tid være i overensstemmelse med det i CPS'en beskrevne.

[KRAV 2.1-02] CA skal gøre den offentlige del af gældende CPS tilgængelig på CA's hjemmeside på 24/7 basis.

[KRAV 2.1-03] CA skal offentliggøre vilkår og betingelser for anvendelse af tjenesten for både certifikatindehaveren og modtagerparter. Vilkår og betingelser skal blandt andet indeholde:

a) en beskrivelse af tjenesten,
b) CP'er der er omfattet af tjenesten,
c) eventuelle begrænsninger i anvendelsen af tjenesten,
d) Certifikatindehavers forpligtelser,
e) tid for opbevaring af hændelseslog,
f) ansvarsbegrænsninger,
g) begrænsninger i brugen af tjeneste, herunder CA's ansvarsbegrænsning i forhold til forkert brug af tjenesten,
h) lovvalg
i) procedure for tvister,
j) at CA agerer som kvalificeret tillidstjenesteudbyder jf. eIDAS,
k) CA's kontaktinformation og
l) eventuelle tilsagn om tilgængelighed.

[KRAV 2.1-04] Derudover skal vilkår og betingelser for certifikatindehavere indeholde:

m) angivelser af, hvad der udgør certifikat accept jf. afsnit 4.4.1 og at den private nøgle ikke må benyttes,
    - førend certifikatet er accepteret af certifikatindehaver, bortset fra den brug, der indgår i certifikatansøgningsprocessen eller

- efter at certifikatindehaver har fået mistanke om kompromittering af den private nøgle, bortset fra brug til autentificering i forbindelse med anmodning om spærring af tilhørende certifikat og dekryptering af data krypteret med den tilhørende offentlige nøgle,

n) angivelse af, hvor længe data gemmes,

o) certifikatindehavers forpligtelser jf. afsnit 4.5.1.

p) information til modtagerparter jf. afsnit 4.5.2 og

q) information om gyldighedsperioden for certifikatet.

[KRAV 2.1-05] CA skal særligt informere modtagerparter om, at modtagerpart, forud for at have tillid til et certifikat skal sikre sig følgende:

- at certifikatet er gyldigt og ikke spærret på tidspunktet for anvendelse af den private nøgle - dvs. ikke opført på CA's spærreliste,
- at det formål, certifikatet søges anvendt til, er passende i forhold til evt. anvendelsesbegrænsninger i certifikatet samt
- at anvendelsen af certifikatet i øvrigt er passende i forhold til niveauet af sikkerhed, som er beskrevet i denne CP.

[KRAV 2.1-06] Vilkår og betingelser skal stilles til rådighed via et varigt kommunikationsmedie.

[KRAV 2.1-07] Vilkår skal være formuleret i et letforståeligt sprog og skal være tilgængelig på 24/7 basis. Ved systemfejl eller faktorer, der ikke er under CA's kontrol, skal CA bestræbe sig på at sikre, at denne informationstjeneste ikke er utilgængelig i længere tid end en maksimumsperiode som angivet i den offentlige del af CPS'en.

[KRAV 2.1-08] Vilkår og betingelser kan overføres elektronisk.

2.2 Offentliggørelse af certifikatinformation

[KRAV 2.2-01] CA skal stille udstedte certifikater til rådighed for certifikatholdere, certifikatindehavere og modtagerparter indtil minimum to måneder efter udløb af det enkelte certifikats gyldighedsperiode. Dog skal certifikater kun være tilgængelig for 3. parter, hvis certifikatindehaver har givet samtykke til offentliggørelse.

[KRAV 2.2-02] Efter udstedelse skal det fuldstændige og nøjagtige certifikat være tilgængeligt for den certifikatholder, for hvem certifikatet udstedes.

[KRAV 2.2-03] CA skal gøre følgende typer af information tilgængelig for alle:

- CA's rodcertifikat.
- CA's underliggende CA-certifikater.
- Denne CP, så længe der er gyldige certifikater udstedt efter denne CP og så længe, der er certifikater på spærrelisten for denne CP.
- Spærreliste for certifikater udstedt efter denne CP.

Note: CA kan gøre CP tilgængelig via et link til Digitaliseringsstyrelsens offentliggørelse af CP.

[KRAV 2.2-04] Spærrelisteinformation skal være tilgængelig uden nogen form for adgangskontrol.

[KRAV 2.2-05] CA skal sikre, at de krav, CA stiller til certifikatindehaver og modtagerpart på baggrund af denne CP uddrages og dokumenteres, jf. afsnit 6.2 og afsnit 6.3.

2.3 Tid eller frekvens for offentliggørelse

[KRAV 2.3-01] CA's offentlige del af CPS skal offentliggøres umiddelbart efter godkendelse.

2.4 Adgangskontrol for repository

[KRAV 2.4-01] CA må ikke begrænse adgangen til den offentlige del af CPS og vilkår til anvendelse af tjenesterne herunder skal CPS og vilkår kunne tilgås internationalt.

3. Identifikation og autentifikation

3.1 Navngivning

3.1.1 Typer af navne

[KRAV 3.1.1-01] Certifikatindehaver skal identificeres ved et navn registret i CVR. Dog med mulighed for afvigelser jf. afsnit 3.1.2.

[KRAV 3.1.1-02] Certifikatholder skal være en identificerbar fysisk eller logisk enhed hos certifikatindehaver. I denne sammenhæng kan certifikatholderen være placeret andre steder end hos certifikatindehaveren fx hos en driftsleverandør.

3.1.2 Krav om meningsfulde navne

[KRAV 3.1.2-01] Certifikatindehavers navn skal være navn eller binavn registreret i CVR. Dog kan selskabsformer i navnet fx "ApS", "A/S" og "Fonden" udelades. Danske bogstaver og specialtegn kan erstattes, hvis det ikke giver anledning til oplagte misforståelser og lange navne kan forkortes, hvis det ikke giver anledning til oplagte misforståelser.

[KRAV 3.1.2-02] Certifikatholders navn skal være meningsfuld for alle relevante modtagerparter i forhold til den fysiske eller logiske enhed som er identificeret.

[KRAV 3.1.2-03] Certifikatholders navn ikke være af en art, der kan give anledning til oplagte misforståelser og må ikke være identisk eller forvekslelig med et varemærke. Desuden kan CA afvise anvendelse af et pseudonym.

Note: CA kan fx afvise et pseudonym, hvis det kan være krænkende eller uetisk.

3.1.3 Anonymitet og pseudonymisering af certifikatholder og -indehaver

N/A

3.1.4 Regler for fortolkning af forskellige navneformer

N/A

3.1.5 Entydighed af navne

[KRAV 3.1.5-01] Entydighed af certifikatholder skal sikres ved anvendelse af serialNumber i subject distinguishedName.

3.1.6 Genkendelse, kontrol og betydning af varemærker

N/A

3.2 Initiel identitetskontrol

[KRAV 3.2-01] CA skal verificere certifikatindehaverens identitet og kontrollere, at certifikatanmodningerne er nøjagtige, godkendte og komplette i henhold til indsamlet identifikationsdokumentation eller -bevis.

[KRAV 3.2-02] CA skal enten via direkte bevis eller via en attest fra en passende og autoriseret kilde, indsamle dokumentation for identiteten og i givet fald eventuelle specifikke egenskaber for certifikatholder, til hvem der udstedes et certifikat. Indleverede beviser kan være i form af enten papir eller elektronisk dokumentation (i begge tilfælde skal RA validere deres ægthed). Verifikation af certifikatholders identitet skal være på tidspunktet for registrering ved anvendelse af passende midler.

[KRAV 3.2-03] CA skal logge alle relevante informationer, der er nødvendige for at verificere certifikatholderens identitet og hvis muligt alle specifikke attributter herunder referencenumre og eventuelle gyldighedsperioder i identitetsdokumentation brugt ved verifikationen.

[KRAV 3.2-04] CA's politik for identitetskontrol må kun indsamle data til bevis for identitet, der er tilstrækkelig for opfyldelse af krav til anvendelse af det udstedte certifikat.

[KRAV 3.2-05] For at undgå interessekonflikter, skal certifikatindehaver og CA være separate enheder. Eneste undtagelse er hvis en organisation helt eller delvis driver RA opgaver i forbindelse med udstedelse af certifikater til personer associeret med egen organisation og at disse undtagelser er dokumenteret i CA's CPS.

Note: Ovenstående krav forhindrer ikke CA's organisation i at få certifikater til egne certifikatholdere. Dette skal blot håndteres fra en enhed, der ikke drifter og/eller forvalter CA systemet.

3.2.1 Metode til at bevise besiddelse af privat nøgle

[KRAV 3.2.1-01] CA skal inden udstedelse af certifikat sikrer sig, at certifikatindehaver eller certifikatholder er i besiddelse af privat nøgle, hørende til certifikatholders offentlige nøgle, der skal indgå i certifikatet.

[KRAV 3.2.1-02] CA skal dokumentere metoden til bevis for besiddelse af privat nøgle i CPS.

3.2.2 Kontrol af organisationsidentitet

[KRAV 3.2.2-01] CA skal etablere en procedure for verifikation af certifikatindehavers identitet, der sikrer, at

a) Certifikatindehaver er en juridisk enhed registreret i CVR-registret.
b) Verifikation af certifikatindehavers identitet er sikret på NSIS sikringsniveau "betydelig" eller "høj".
c) En ledelsesrepræsentant med nødvendig prokura hos certifikatindehaver udpeger en bemyndiget jf definition i afsnit 1.6.1.
d) Den bemyndigede kan autentificeres på NSIS sikringsniveau "betydelig" eller "høj" eller eIDAS sikringsniveau "betydelig" eller "høj".
e) Al kommunikation baseret på fysisk fremsendelse, der indgår i sikring af certifikathavers identitet, er baseret på gældende postadresse registreret i CVR-registret.

[KRAV 3.2.2-02] Såfremt CA på forhånd har kendskab til certifikatindehaverens identitet, kan ovenstående krav helt eller delvist fraviges.

[KRAV 3.2.2-03] CA skal dokumentere procedure for verifikation af certifikatindehavers identitet i CPS.

[KRAV 3.2.2-04] Den bemyndigede skal ved registrering indestå for at certifikatholder er identificeret ved

a) Et identifikationsnummer, der entydigt refererer til certifikatholder
b) Organisationens navn
c) Alle data om certifikatindehaver, der vil indgå i certifikatets organisatoriske attributter
d) CVR-nummer

[KRAV 3.2.2-05] Hvis certifikatholder er en enhed eller et system, der specifikt skal anvendes af én fysisk person, skal den bemyndigede desuden registrere og indestå for

a) Et nationalt identitetsnummer eller andre attributter, der i videst muligt omfang kan sikre den fysiske persons entydighed.

3.2.3 Kontrol af fysisk persons identitet

N/A

3.2.4 Ikke-kontrollerede information om certifikatholder

[KRAV 3.2.4-01] Certifikatindehaver skal angive en fysisk adresse eller andre attributter, der beskriver hvordan certifikatindehaver skal kontaktes.

3.2.5 Kontrol af rettigheder

Se KRAV 3.2.2-01 c) for kontrol af rettigheder for bemyndiget.

3.2.6 Kriterier for interoperabilitet

N/A

3.3 Identifikation og autentikation ved genudstedelse

[KRAV 3.3-01] Alle anmodninger om et certifikat til en certifikatholder, der tidligere er registreret af CA, skal være fuldstændige, nøjagtige og autoriserede.

[KRAV 3.3-02] Hvis der er ændringer i CA's vilkår og betingelser, skal CA's vilkår og betingelser kommunikeres til og accepteres af certifikatindehaver.

[KRAV 3.3-03] Krav til identitetskontrol jf. afsnit 3.2 skal være overholdt.

3.3.1 Identifikation og autentikation ved fornyelse

[KRAV 3.3.1-01] CA skal kontrollere eksistens og gyldighed af det certifikat, der skal fornys, og at de oplysninger, der bruges til at verificere certifikatholders identitet og attributter, stadig er gyldige.

3.3.2 Identifikation og autentikation ved genudstedelse efter spærring

[KRAV 3.3.2-01] CA skal kontrollere eksistens og gyldighed af det certifikat, der skal genudstedes, og at de oplysninger, der bruges til at verificere certifikatholders identitet og attributter, stadig er gyldige.

Note: I forhold til gyldighed skal det kontrolleres at certifikatet er spærret i ovenstående krav.

3.4 Identifikation og autentikation ved anmodning om spærring

[KRAV 3.4-01] CA skal med rimelighed og under hensyntagen til den generelle sikkerhed, sikre at spærringsanmodninger og rapportering om hændelser, der kan give anledning til spærring af certifikater, kommer fra autoriserede kilder.

[KRAV 3.4-02] CA skal dokumentere procedurerne for spærring af slutbruger- og CA-certifikater i den offentlige del af CPS, herunder

- Hvem der kan anmode om spærring eller rapportere om hændelser, der indikerer behov for spærring af et certifikat.
- Hvordan anmodninger eller rapporteringer kan foretages.
- Eventuelle krav til efterfølgende bekræftelse af anmodninger om spærring eller rapporter om hændelser, der indikerer behov for spærring af et certifikat.
- Gyldige årsager til at certifikater kan spærres.
- Mekanismer til distribution af information om spærrede certifikater (fx spærrelister og OCSP).
- Den maksimale tid mellem modtagelsen af en anmodning om spærring og til beslutningen om at spærre certifikatet.
- Den maksimale tid mellem beslutningen om at spærre certifikatet og til den faktiske information om at certifikatet er offentligt tilgængeligt (fx via offentliggørelse af spærreliste).

4. Operationelle krav i certifikatlivscyklus

4.1 Certifikatanmodning

4.1.1 Hvem kan anmode om certifikat

[KRAV 4.1.1-01] Certifikatindehaver kan anmode om et certifikat til certifikatholder via den bemyndigede.

4.1.2 Tilslutningsproces og ansvarsfordeling

[KRAV 4.1.2-01] Certifikatanmodning skal ske gennem en RA efter en tilslutningsproces. Den bemyndigede skal ved anmodningen være autentificeret på niveau svarende til NSIS sikringsniveau "betydelig" eller "høj" eller eIDAS sikringsniveau "betydelig" eller "høj".

Note: RA kan være en del af CA's organisation og/eller en eller flere eksterne samarbejdspartnere.

[KRAV 4.1.2-02] Hvis ekstern RA anvendes, skal registreringsdata udveksles sikkert og kun gennem RA'ere, hvis identitet er autentificeret.

[KRAV 4.1.2-03] CA skal sikre, at tilslutningsprocessen først kan afsluttes efter certifikatindehaverens accept af vilkår og betingelser for anvendelse af CA-tjenesten.

[KRAV 4.1.2-04] Hvis certifikatholders nøglepar ikke genereres af CA, skal certifikatanmodningsprocessen kontrollere, at certifikatholderen er i besiddelse af eller

har kontrol over den private nøgle, der er forbundet med den offentlige nøgle, der skal indsættes i certifikatet og at den private nøgle er beskyttet af et QSCD.

4.2 Behandling af certifikatanmodning

4.2.1 Gennemførsel af identifikation og autentifikation

[KRAV 4.2.1-01] Inden udstedelse af et certifikat til en registreret certifikatholder skal certifikatholder være identificeret og autentificeret fx ved anvendelse af et referencenummer og en kode sendt sikkert til den bemyndigede.

4.2.2 Godkendelse eller afvisning af certifikatanmodning

[KRAV 4.2.2-01] CA skal godkende eller afvise en certifikatanmodning og give certifikatindehaver adgang til information om status for certifikatanmodninger. CA skal begrunde en afvisning af en certifikatanmodning over for certifikatindehaver.

4.2.3 Tidsfrister for behandling af certifikatanmodning

[KRAV 4.2.3-01] CA bør behandle certifikatanmodninger uden unødig forsinkelse.

4.3 Certifikatudstedelse

4.3.1 CA opgaver ved certifikatudstedelse

[KRAV 4.3.1-01] CA skal udstede certifikater sikkert for at bevare deres autenticitet.

Særligt skal følgende iagttages:

- **[KRAV 4.3.1-02]** CA skal træffe foranstaltninger mod forfalskning af certifikater.
- **[KRAV 4.3.1-03]** Hvis CA genererer certifikatholders nøglepar, skal CA garantere fortrolighed under processen med generering af disse data.
- **[KRAV 4.3.1-04]** Proceduren for certifikatudstedelse skal være sikkert forbundet med den tilknyttede registrering, certifikatfornyelse eller certifikatopdatering, herunder tilvejebringelse af en offentlig nøgle for certifikatholderen.
- **[KRAV 4.3.1-05]** CA må ikke udstede certifikater, hvis levetid overstiger udløbstidspunkt for CA's overliggende certifikater.
- **[KRAV 4.3.1-06]** Hvis CA genererer certifikatholders nøglepar, skal proceduren for udstedelse af certifikatet være sikkert forbundet med CA's generering af nøgleparret.

- **[KRAV 4.3.1-07]** Hvis CA genererer certifikatholders nøglepar, skal den private nøgle sendes sikkert til certifikatholderen; eller til den tillidstjeneste, der forvalter certifikatholderens private nøgle, herunder skal det kryptografiske modul, som beskytter certifikatholders nøgle, leveres sikkert.
- **[KRAV 4.3.1-08]** Et navn, der er anvendt til at angive én certifikatholder i et certifikat, må ikke anvendes til at angive en anden certifikatholder i et certifikat i løbet af CA's livstid.

Note: Navnet i ovenstående krav omfatter hele identifikationen i certifikatet inklusiv subject serialNumber jf. afsnit 7.1.4.

[KRAV 4.3.1-10] CP skal være identificeret i certifikatet med QCP-l-qscd (certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD) jf. afsnit 7.1.6.

4.3.2 CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatudstedelse

[KRAV 4.3.2-01] CA kan notificere certifikatindehaver ved certifikatudstedelse.

4.4 Accept af certifikat

4.4.1 Handling, der betragtes som certifikatholders certifikataccept

[KRAV 4.4.1-01] Vilkår og betingelser skal angive, hvad der anses for at udgøre accept af certifikatet.

Særligt gælder

- **[KRAV 4.4.1-02]** Inden indgåelse af kontraktforhold med en certifikatindehaver skal CA underrette indehaveren om vilkår og betingelser for brug af certifikatet som angivet i afsnit 2.1.
- **[KRAV 4.4.1-04]** CA skal meddele vilkår og betingelser gennem varigt (dvs. med integritet over tid) kommunikationsmedie og i en læsbar form før aftalen indgås.
- **[KRAV 4.4.1-05]** Vilkår og betingelse kan formidles elektronisk.
- **[KRAV 4.4.1-06]** Vilkårene og betingelserne kan baseres på model angivet i ETSI EN 319 411-1 bilag A.
- **[KRAV 4.4.1-08]** Aftalen i ovenstående krav skal indebære en udtrykkelig accept af vilkår og betingelser ved en viljeshandling, der senere kan bevises.

Note: Ovenstående bevis, kan fx være baseret på systembevis.

- **[KRAV 4.4.1-09]** Certifikatindehaver skal godkende aftalen med CA, der som minimum skal inkludere:

  a) certifikatindehavers forpligtelser, herunder forpligtelser for håndtering af certifikat og tilhørende private nøgle.

b) samtykke til at CA opbevarer oplysninger, der benyttes ved registrering, tilhørende behandling, herunder om det er certifikatindehaver eller certifikatholder der registreres, enhver senere spærring, identiteten og eventuelle specifikke attributter, der er inkluderet i certifikatet, samt videregivelsen af disse oplysninger til tredjepart på de samme betingelser som krævet i denne politik i tilfælde af CA, der nedlægger sine tjenester.

c) om og under hvilke betingelser certifikatindehaver skal godkende offentliggørelsen af certifikatet

d) bekræftelse af, at oplysningerne i certifikatet skal være korrekte

e) forpligtelser til at anmode CA om spærring af certifikater udstedt til certifikatholdere, når disse ikke længere er tilknyttet certifikatindehaveren.

- **[KRAV 4.4.1-12]** Aftalen kan være i elektronisk form. Hvis aftalen er i elektronisk form, bør den være signeret med en avanceret elektronisk signatur eller et avanceret elektronisk segl jf. eIDAS.
- **[KRAV 4.4.1-13]** Ovenstående registreringer skal gemmes i den tidsperiode, der er oplyst til certifikatindehaver (som en del af vilkår og betingelser).

4.4.2 CA's offentliggørelse af certifikatet

[KRAV 4.4.2-01] CA skal offentliggøre certifikatet jf. afsnit 2.2 under hensyntagen til KRAV 4.4.1-09 c).

4.4.3 CA's notifikation til andre parter om certifikatudstedelse

[KRAV 4.4.3-01] CA kan notificere andre parter om udstedelse af certifikat under hensyntagen til KRAV 4.4.1-09 c).

4.5 Nøglepar og certifikatanvendelse

4.5.1 Certifikatholders anvendelse af privat nøgle og certifikat

[KRAV 4.5.1-01] CA skal med aftale sikre, at certifikatindehaverende forpligter sig til punkterne a) til j) herunder.

a) Oplysninger sendt til CA i overensstemmelse med kravene i denne politik skal være korrekte og komplette, især med hensyn til registrering.
b) Nøgleparret bruges kun i overensstemmelse med fastlagt tilladt brug og ikke uden for eventuelle begrænsninger, der er meddelt certifikatindehaver og certifikatholder, herunder at den private nøgle ikke må anvendes til signering af andre certifikater.
c) Uautoriseret brug af certifikatholders private nøgle skal forhindres, herunder

   i) at valg af kodeord sikrer, at de ikke umiddelbart kan gættes ved kendskab til certifikatholder,
   ii) at der tages rimelige forholdsregler, for at beskytte de sikkerhedsmekanismer, der sikrer den private nøgle mod kompromittering, ændring, tab og uautoriseret brug og
   iii) at hemmeligholde kodeord, så andre ikke får kendskab til disse.

d) Hvis certifikatindehaver eller certifikatholder genererer certifikatholders nøgler:
   i) en forpligtelse eller en anbefaling til at generere certifikatholders nøgler ved hjælp af en algoritme som specificeret i ETSI TS 119 312 til brug af den certificerede nøgle som identificeret i CP; og
   ii) en forpligtelse eller anbefaling til brug af nøglelængde og algoritme som specificeret i ETSI TS 119 312 for brug af den certificerede nøgle som identificeret i CP under certifikatets gyldighedsperiode eller
   iii) ved anvendelse af algoritmer og nøglelængder anbefalet af Digitaliseringsstyrelsen, der kan erstatte d).i) og d).ii).

e) Hvis certifikatindehaver eller certifikatholder genererer certifikatholders nøglepar, og den private nøgle kan anvendes til generering af elektroniske segl, skal certifikatholder have egenkontrol over den private nøgle.

f) Certifikatholders private nøgle(r) må kun benyttes til kryptografiske funktioner inden for det sikre kryptografiske modul (QSCD).

g) Certifikatholders private nøgle(r) skal genereres i certifikatholders kryptografiske modul (QSCD), hvis certifikatholders nøgle(r) genereres under kontrol af certifikatindehaver eller certifikatholder.

h) Underrette CA uden unødig forsinkelse, hvis et af følgende forekommer inden udløb af gyldighedsperioden angivet i certifikatet:
   i) Certifikatholders adgang til private nøgle er mistet eller certifikatholders private nøgle er stjålet eller potentielt kompromitteret.
   ii) Certifikatholders egenkontrol med den private nøgle er mistet på grund af kompromittering af aktiveringsdata (fx PIN kode).
   iii) Unøjagtigheder eller ændringer af data, der er inkluderet i certifikatet og som er kommet til certifikatindehaver eller certifikatholders kendskab.

i) Anvendelse af certifikatholders private nøgle ophører umiddelbart efter en kompromittering, efter anmodning om spærring, notifikation om spærring eller efter udløb af certifikat med undtagelse af eventuelt dekryptering af data.

j) Anvendelse af certifikatholders private nøgle ophører i tilfælde af certifikatindehaver eller certifikatholder er underrettet om, at certifikatholders certifikat er blevet spærret, eller hvis overliggende CA'er er blevet kompromitteret.

Note: Termen "mistet" i KRAV 4.5.1-02 h).i) omfatter ikke løsninger, hvor den private nøgle ikke lagres, men kun anvendes til en enkel operation (signering) og herefter destrueres.

[KRAV 4.5.1-03] Hvis certifikatholders nøgler håndteres i et QSCD af en tillidstjenesteudbyder eventuelt af CA selv, må den private nøgle kun anvendes i QSCD'et.

[KRAV 4.5.1-04] Hvis certifikatholders nøgler håndteres i et QSCD af en tillidstjenesteudbyder eventuelt af CA selv i et QSCD, skal den private nøgle være under certifikatholders egenkontrol.

[KRAV 4.5.1-05] Hvis certifikatholders nøgler håndteres i et QSCD af en tillidstjenesteudbyder eventuelt af CA selv, skal certifikatholders nøgler udelukkende anvendes til generering af kvalificerede elektroniske segl.

[KRAV 4.5.1-06] Hvis certifikatholders nøgler håndteres af en tillidstjenesteudbyder, der ikke er CA selv, skal CA ved aftale sikre at tillidstjenesten overholder kravene KRAV 4.5.1-02 – KRAV 4.5.1-05.

4.5.2 Modtagerparts anvendelse af offentlig nøgle og certifikat

[KRAV 4.5.2-01] CA's information til modtagerparter skal inkludere følgende anbefalinger:

a) Modtagerpart skal verificere gyldighed eller spærring af certifikatet ved brug af opdaterede spærringsstatusoplysninger stillet til rådighed for modtagerpart.

b) Modtagerpart skal tage hensyn til eventuelle begrænsninger for brugen af det certifikat, enten angivet direkte i certifikatet eller i de vilkår og betingelser, der er stillet til rådighed af CA.

c) Modtagerpart skal træffe andre forholdsregler, der er foreskrevet i aftaler eller andre steder.

4.6 Certifikatgenudstedelse

Genudstedelse af et kvalificeret certifikat betyder udstedelse af et nyt certifikat efter denne certifikatpolitik til den samme certifikatholder med samme offentlig nøgle som tidligere udstedt certifikat, men med ny gyldighedsperiode, et nyt certifikat-serienummer og det gældende Politik OID.

4.6.1 Årsag til certifikatgenudstedelse

N/A

4.6.2 Hvem kan anmode om certifikatgenudstedelse

[KRAV 4.6.2-01] Certifikatindehaver kan anmode om certifikatgenudstedelse til certifikatholder.

4.6.3 Behandling af anmodning om certifikatgenudstedelse

[KRAV 4.6.3-01] Certifikatanmodninger for en certifikatholder, der tidligere er registreret hos CA skal være komplette, præcise og autoriserede.

[KRAV 4.6.3-02] Særligt skal CA kontrollere eksistensen og gyldigheden af certifikatet, der skal genudstedes, og at de oplysninger, der bruges til at verificere certifikatholders identitet og attributter, stadig er gyldige.

[KRAV 4.6.3-03] Hvis nogen af CA's vilkår og betingelser er ændret, skal disse meddeles certifikatindehavere og accepteres i overensstemmelse med kravene for første udstedelse.

[KRAV 4.6.3-04] Krav svarende til første udstedelse for identifikation og autentifikation skal efterleves jf. afsnit 3.3.

[KRAV 4.6.3-05] CA må kun udstede et nyt certifikat med certifikatholderens eksisterende certificerede offentlige nøgle, hvis den kryptografiske sikkerhed for nøgler og algoritmer stadig er tilstrækkelig i det nye certifikats gyldighedsperiode, og der ikke er indikationer på, at certifikatholderens private nøgle er blevet kompromitteret, eller at certifikatet er blevet spærret på grund af et sikkerhedsbrud.

4.6.4 CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatgenudstedelse

[KRAV 4.6.4-01] CA's notifikation til certifikatindehaver ved certifikatgenudstedelse skal følge regler for notifikation af første certifikat jf. afsnit 4.3.2.

4.6.5 Handling, der betragtes som certifikatholders certifikataccept

[KRAV 4.6.5-01] Handlinger, der betragtes som certifikatholders certifikataccept skal følge regler for accept af første certifikat jf. afsnit 4.4.1.

4.6.6 CA's offentliggørelse af genudstedt certifikat

[KRAV 4.6.6-01] Offentliggørelse af et genudstedt certifikat skal følge regler for offentliggørelse af første certifikat jf. afsnit 4.4.2.

4.6.7 CA's notificering til andre parter om certifikatgenudstedelse

[KRAV 4.6.7-01] CA's notifikation til andre parter ved certifikatgenudstedelse skal følge regler for notifikation af første certifikat jf. afsnit 4.3.3.

4.7 Certifikatfornyelse

4.7.1 Årsag til certifikatfornyelse

Fornyelse af et kvalificeret certifikat betyder udstedelse af et nyt certifikat efter denne certifikatpolitik til tidligere registreret certifikatholder, med et nyt nøglepar, ny gyldighedsperiode, et nyt certifikat-serienummer og det gældende Politik OID.

[KRAV 4.7.1-01] Et certifikat udstedt under denne CP må fornys for op til fire år ad gangen.

[KRAV 4.7.1-02] CA eller certifikatindehaver kan angive, om et certifikat skal kunne fornys.

[KRAV 4.7.1-03] CA skal sikre, at anmodning om og udstedelse af fornyet certifikat kan ske online, medmindre det eksisterende certifikat er markeret til ikke at kunne fornys jf. KRAV 4.7.1-02.

[KRAV 4.7.1-04] For certifikater, der kan fornys, kan CA i en passende tid før udløb notificere certifikatholderen herom. Desuden kan CA samtidig hermed notificere den bemyndiget om udløb.

4.7.2 Hvem kan anmode om certifikatfornyelse

[KRAV 4.7.2-01] Et certifikat udstedt under denne CP kan fornys af certifikatholder, hvis det eksisterende certifikat er markeret til fornyelse jf. KRAV 4.7.1-02.

4.7.3 Behandling af anmodning om certifikatfornyelse

[KRAV 4.7.3-01] CA skal sikre, at anmodningen om fornyelse signeres med certifikatholderens gyldige private nøgle eller at certifikatholder er autentificeret med NSIS sikringsniveau "betydelig" eller "høj" eller eIDAS sikringsniveau "betydelig" eller "høj".

[KRAV 4.7.3-02] Certifikatansøgning og -udstedelse skal i øvrigt opfylde kravene i afsnit 6.1 om generering og installation af certifikatholders nøgler.

4.7.4 CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatfornyelse

[KRAV 4.7.4-01] CA's notifikation til certifikatindehaver ved certifikatfornyelse skal følge regler for notifikation af første certifikat jf. afsnit 4.3.2.

4.7.5 Handling, der betragtes som certifikatholders certifikataccept

[KRAV 4.7.5-01] Handlinger, der betragtes som certifikatholder certifikataccept skal følge regler for accept af første certifikat jf. afsnit 4.4.1.

4.7.6 CA's offentliggørelse af fornyet certifikat

[KRAV 4.7.6-01] Offentliggørelse af et fornyet certifikat skal følge regler for offentliggørelse af første certifikater jf. afsnit 4.4.2.

4.7.7 CA's notifikation til andre parter om certifikatfornyelse

[KRAV 4.7.7-01] CA's notifikation til andre parter ved certifikatfornyelse skal følge regler for notifikation af første certifikat jf. afsnit 4.3.3.

4.8 Certifikatopdatering

4.8.1 Årsag til certifikatopdatering

[KRAV 4.8.1-01] Anmodninger om certifikater udstedt til en certifikatholder, der tidligere er registreret hos CA, skal være fuldstændige, korrekte og godkendte.

Dette omfatter certifikatopdatering, der skyldes ændringer i certifikatholders attributter.

4.8.2 Hvem kan anmode om certifikatopdatering

[KRAV 4.8.2-01] Certifikatindehaver kan anmode om certifikatopdatering.

4.8.3 Behandling af anmodning om certifikatopdatering

[KRAV 4.8.3-01] Hvis navne eller attributter, som indgår i certifikatet, er ændret, eller det tidligere certifikat er blevet spærret, skal registreringsoplysningerne kontrolleres, registreres, accepteres af certifikatindehaveren i overensstemmelse med afsnit 3.3.

4.8.4 CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatopdatering

[KRAV 4.8.4-01] CA's notifikation til certifikatholder og/eller certifikatindehaver ved certifikatopdatering skal følge regler for notifikation af første certifikat jf. afsnit 4.3.2.

4.8.5 Handling, der betragtes som certifikatholders certifikataccept

[KRAV 4.8.5-01] Handlinger, der betragtes som certifikatholder certifikataccept skal følge regler for accept af første certifikat jf. afsnit 4.4.1.

4.8.6 CA's offentliggørelse af opdateret certifikat

[KRAV 4.8.6-01] Offentliggørelse af et opdateret certifikat skal følge regler for offentliggørelse af første certifikater jf. afsnit 4.4.2.

4.8.7 CA's notifikation til andre parter om certifikatopdatering

[KRAV 4.8.7-01] CA's notifikation til andre parter ved certifikatopdatering skal følge regler for notifikation af første certifikat jf. afsnit 4.3.3.

4.9 Certifikatspærring og -suspendering

4.9.1 Årsager til spærring

[KRAV 4.9.1-01] CA skal omgående og senest indenfor 12 timer spærre et certifikat udstedt under denne CP, hvis CA får kendskab til et eller flere af følgende forhold:

a) Certifikatindehaveren ønsker at spærre certifikatet eller afslutte brugen heraf.
b) Certifikatholderen har mistet adgangen til den private nøgle.
c) Der er vished eller mistanke om, at certifikatholderens private nøgle er kompromitteret.
d) Den private nøgle er ødelagt eller gået tabt på anden vis.

e) Certifikatholder ikke længere har tilknytning til certifikatindehaveren.
f) Der er konstateret unøjagtighed i certifikatets indhold eller anden information knyttet til certifikatindehaveren/holderen, jf. dog nedenfor vedr. certifikatholders ændring af navn.
g) Certifikatindehaverens konkurs.
h) Certifikatindehaverens virksomhed ophører.

Note: Termen "mistet" i KRAV 4.9.1-01 b) samt termerne "ødelagt" og "gået tabt" i KRAV 4.9.1-01 d) omfatter ikke løsninger, hvor den private nøgle ikke lagres, men kun anvendes til en enkel operation (signering) og herefter destrueres.

[KRAV 4.9.1-02] Hvis certifikatindehaver ændrer navn, skal CA omgående notificere certifikatindehaver om, at certifikatet skal fornyes inden for 120 dage. Sker dette ikke, skal CA spærre certifikatet.

Note: Det bemærkes, at ovenstående krav ikke finder anvendelse hvis certifikatindehaver beholder det tidligere navn som binavn jf. KRAV 3.1.2-01.

[KRAV 4.9.1-03] CA's egen manglende overholdelse af denne CP giver ikke alene CA ret til at spærre et certifikat.

Note: Hvis der er konstateret unøjagtigheder i et certifikat grundet CA manglende overholdelse skal certifikatet dog stadig spærres.

[KRAV 4.9.1-04] Et spærret certifikat må ikke genaktiveres.

4.9.2 Hvem kan anmode om spærring

[KRAV 4.9.2-01] Følgende kan anmode om spærring af certifikat:

- Certifikatholder
- Bemyndiget
- CA, hvis reglerne i denne CP ikke er overholdt, eller hvor forholdene i øvrigt tilsiger dette
- Tegningsberettigede i virksomheden mod behørig dokumentation
- Tilsyn eller kurator, såfremt certifikatindehaver har anmeldt betalingsstandsning eller tages under konkursbehandling.

4.9.3 Procedure for anmodning om spærring

[KRAV 4.9.3-01] CA skal spærre certifikater rettidigt ud fra godkendte og validerede anmodninger om spærring af certifikater fra en af parterne beskrevet i afsnit 4.9.2.

[KRAV 4.9.3-02] Spærringsanmodninger skal som minimum kunne sendes via følgende kanaler:

- Fysisk post
- Web
- Telefonisk

[KRAV 4.9.3-03] CA skal orientere certifikatindehaver om gennemført spærring via kommunikationskanal aftalt mellem CA og certifikatindehaver.

[KRAV 4.9.3-04] Hvis CA foretager spærring uden at være anmodet om det, skal CA sende meddelelse med angivelse af årsag til spærring til certifikatindehaver via kommunikationskanal aftalt mellem CA og certifikatindehaver.

[KRAV 4.9.3-05] I tilfælde af certifikatindehavers konkurs kan skifteret eller kurator anmode om spærring. I givet fald skal CA ligeledes sende kvittering for spærring til skifteretten hhv. kuratoren.

4.9.4 Tidsfrister for anmodning om spærring

[KRAV 4.9.4-01] CA skal ved aftale sikre at certifikatindehaver skal anmode om spærring uden unødig forsinkelse, hvis en eller flere årsager til spærring jf. afsnit 4.9.1 er indtruffet.

4.9.5 Tidsfrister for CA's håndtering af anmodninger om spærring

[KRAV 4.9.5-01] CA skal indlede behandling af spærringsanmodninger og rapportering om hændelser, der kan give anledning til spærring af certifikater, umiddelbart efter modtagelse.

[KRAV 4.9.5-02] CA skal sikre, at spærring sker umiddelbart efter anmodning er modtaget og eventuelt bekræftelse af anmoders identitet og autorisation er sket.

[KRAV 4.9.5-03] Hvis en anmodning om spærring betyder at certifikatet skal spærres på et fremtidigt planlagt tidspunkt (fx hvis certifikatholder har planlagte ophør fra en bestemt dato), kan den planlagte dato betragtes som bekræftelsestidspunktet for CA.

[KRAV 4.9.5-04] CA kan gennem den offentlige del af CPS give garantier for en hurtigere procestid for visse årsager til spærring.

[KRAV 4.9.5-05] Tiden, der anvendes i forbindelse med spærring, skal synkroniseres med UTC mindst en gang hver 24. time.

4.9.6 Krav til modtagerparters verifikation af certifikatstatus

N/A

4.9.7 Udstedelsesfrekvens for spærrelister

[KRAV 4.9.7-01] Spærrelister (CRL'er) for certifikatholderes certifikater, herunder eventuelle varianter (fx Delta CRL'er), skal genereres og offentliggøres mindst hver 24. time.

[KRAV 4.9.7-02] Enhver spærreliste (CRL) for certifikatholderes certifikater, herunder eventuelle varianter (fx Delta CRL), skal inkludere feltet nextUpdate defineret i IETF RFC 5280, som skal indeholde tidspunktet for den næste planlagte CRL-udstedelse, medmindre det er den sidste CRL, der er udstedt for disse certifikater, i hvilket tilfælde feltet nextUpdate skal sættes til "99991231235959Z"

[KRAV 4.9.7-03] Spærrelister for CA-certifikater, herunder eventuelle varianter (fx Delta CRL'er), skal genereres og offentliggøres mindst én gang om året med højest ét år for næste opdatering angivet i feltet nextUpdate.

[KRAV 4.9.7-04] Hvis et CA-certifikat spærres skal det overliggende CA umiddelbart efter udstede og offentliggøre en ny spærreliste.

[KRAV 4.9.7-05] For enhver aktuel spærreliste herunder eventuelle varianter (fx Delta CRL) skal der offentliggøres en ny spærreliste senest en time inden tidspunktet angivet i feltet nextUpdate.

[KRAV 4.9.7-06] I tilfælde af at et CA udsteder krydscertifikater til andre tillidstjenester, bør CA udstede spærrelister mindst hver 31. dag.

4.9.8 Maksimal forsinkelse for offentliggørelse af spærrelister

[KRAV 4.9.8-01] CA skal efter gennemført spærring offentliggøre en opdateret spærreliste. Dette skal ske senest 1 minut efter, spærring er sket. Dog skal opdateret spærreliste for rod-CA offentliggøres senest 10 minutter efter en spærring.

4.9.9 Understøttelse af online statuskontrol

[KRAV 4.9.9-01] CA skal tilbyde online kontrol af status via protokollen Online Certificate Status Protocol, OCSP.

4.9.10 Krav til modtagerparters online kontrol af certifikatstatus

N/A

4.9.11 Andre muligheder for kontrol af certifikatstatus

[KRAV 4.9.11-01] CA skal gøre information om certifikatstatus tilgængelig via manuelt online opslag.

4.9.12 Særlige krav i forbindelse med spærring pga. nøglekompromittering

N/A

4.9.13 Årsager til suspendering

[KRAV 4.9.13-01] Et certifikat udstedt under denne CP må ikke suspenderes.

4.9.14 Hvem kan anmode om suspendering

N/A

4.9.15 Procedure for suspenderingsanmodning

N/A

4.9.16 Begrænsninger på suspenderingsperiode

N/A

4.10 Certifikatstatusservice

[KRAV 4.10-01] CA skal levere tjenester til kontrol af certifikaters status.

[KRAV 4.10-02] CA skal i CPS og vilkår dokumentere præcist, hvordan KRAV 4.10.1-01 og KRAV 4.10.1-05 opfyldes, herunder

a) perioden, hvor statusinformation er tilgængelig,

b) hvorledes statusinformation leveres i tilfælde af kompromittering af CA-nøgler og

c) hvorledes statusinformation leveres i tilfælde af ophør af CA.

4.10.1 Operationelle karakteristika

[KRAV 4.10.1-01] Statusinformation for certifikater udstedt under denne CP skal være tilgængelige ud over gyldighedsperioden for certifikatet.

[KRAV 4.10.1-02] Integriteten og autenticiteten af statusinformation skal beskyttes.

[KRAV 4.10.1-03] Som minimum skal CRL og OCSP være understøttet som metoder til kontrol af certifikatstatus.

[KRAV 4.10.1-04] Statusinformation skal indeholde oplysninger om spærringsstatus for et certifikat som minimum indtil certifikatets udløbstidspunkt og CA bør ikke fjerne spærrede certifikater fra spærrelister (CRL) efter certifikaters udløbstidspunkt.

[KRAV 4.10.1-05] CA skal sikre integritet og tilgængelighed af den sidste udstedte spærreliste i en periode, der skal være angivet i CPS.

[KRAV 4.10.1-06] CA bør ikke udstede en sidste spærreliste før alle certifikater, der potentielt kan komme på spærrelisten, enten er spærret eller udløbet.

[KRAV 4.10.1-07] Spærrelisterne skal digitalt underskrives af det CA, som har udstedt et spærret certifikat.

[KRAV 4.10.1-08] CA skal gøre spærrelister tilgængelige for download via følgende kanaler:

- LDAP
- HTTP

[KRAV 4.10.1-09] Opdaterede spærreinformationer skal være tilgængelige via alle tilbudte metoder til kontrol af certifikatstatus og alle services skal være konsistente over tid under hensyntagen til mindre forsinkelser.

[KRAV 4.10.1-10] OCSP-responses kan prægenereres, men det kræves at hvis et certifikat spærres da skal det tilhørende OCSP response regenereres og senest 1

minut efter at spærringen er registreret, skal OCSP svar indikere, at certifikatet er spærret.

[KRAV 4.10.1-11] OCSP respondere skal udstyres med dedikerede virksomheds-certifikater som udelukkende bruges til OCSP. Foruden de formalia som kræves for et virksomhedscertifikat, 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.

[KRAV 4.10.1-12] Levetiden for OCSP responder-certifikater for CA'er, der udsteder certifikater til certifikatholdere, skal være maksimal 72 timer og de tilhørende nøgler skal beskyttes af kryptografiske moduler, som angivet i afsnit 6.2.

[KRAV 4.10.1-13] Levetiden for OCSP responder-certifikater for rod-CA skal være maksimalt 3 måneder og de tilhørende nøgler skal beskyttes af kryptografiske, som angivet i afsnit 6.2.

[KRAV 4.10.1-14] Når et CA-certifikat er ved at udløbe kan CA danne et sidste OCSP-svar, der anvendes på alle OCSP-anmodninger med nextUpdate-feltet sat til værdien "99991231235959Z".

4.10.2 Tilgængelighed af service

[KRAV 4.10.2-01] Oplysninger om certifikatstatus skal være tilgængelige 24 timer i døgnet, 7 dage om ugen. Ved systemfejl, i servicevinduer eller ved andre faktorer, som ikke er underlagt CA's kontrol, skal CA bestræbe sig på at sikre, at denne informationstjeneste ikke er utilgængelig i længere tid end en maksimumsperiode som angivet i den offentlige del af CPS.

[KRAV 4.10.2-02] Alle tjenester til kontrol af certifikatstatus skal have en svartid, så 99% af svarerne målt over en periode på 60 minutter skal være under 1 sekund målt på serverindgang – dvs. fra serveren har registreret forespørgslen, til den begynder at returnere svaret.

[KRAV 4.10.2-03] Certifikatstatus services skal være internationalt offentlig tilgængelige.

4.10.3 Ekstra funktioner

N/A

4.11 Certifikatholder eller -indehavers ophør af anvendelse af tjenesten

N/A

4.12 Nøgledeponering og -genopretning

4.12.1 Politik for nøgledeponering

[KRAV 4.12.1-01] CA må ikke foretage nøgledeponering (key escrow) af certifikatholders nøgler.

4.12.2 Sessionsnøgle indkapsling samt politikker og procedure for genskabelse

N/A

5. Fysiske, administrative og operationelle kontroller

[KRAV 5-01] CA skal sikre, at den agerer lovligt og troværdigt.

[KRAV 5-02] CA skal gennemføre risikovurdering for at identificere, analysere og evaluere forretningsmæssige og tekniske risici.

[KRAV 5-03] CA skal implementere passende foranstaltninger til håndtering af risici med udgangspunkt i risikovurderingen. Foranstaltningerne skal sikre, at sikkerhedsniveauet står i forhold til risikoen.

[KRAV 5-04] CA skal fastlægge og dokumentere alle sikkerhedskrav og operationelle procedurer, der er nødvendige for overholdelse af denne CP. Dokumentationen skal være en del af CPS.

[KRAV 5-05] Risikovurderingen skal revideres regelmæssigt og mindst én gang årligt.

[KRAV 5-06] CA's ledelse skal godkende risikovurderingen og acceptere den identificerede restrisiko.

[KRAV 5-07] CA skal vedligeholde en oversigt over aktiver herunder informationsaktiver. Alle informationsaktiver skal klassificeres i henhold til CA's risikovurdering og CA skal sikre en tilstrækkelig beskyttelse af alle aktiver.

[KRAV 5-08] CA skal implementere en effektiv adgangskontrol, der beskytter mod uautoriseret fysisk eller logisk adgang til CA's systemer, herunder skal CA tilvejebringe RA systemer, som sikrer, at det kun er autoriserede medarbejdere hos RA, der har adgang til at betjene disse.

5.1 Fysiske kontroller

[KRAV 5.1-01] CA skal sikre den fysiske adgang til elementer i CA's systemer i forhold til fastlagt politik for klassifikation, herunder minimering af risici i forhold til den fysiske sikkerhed.

[KRAV 5.1-02] CA skal implementere en effektiv beskyttelse mod

- tab, skader og kompromittering af aktiver og forretningsaktiviteter samt

- kompromittering eller tyveri af information og driftsudstyr

[KRAV 5.1-03] CA skal implementere fysiske og miljømæssige kontroller til beskyttelse af driftslokaler, systemressourcer og faciliteter til at understøtte driften.

[KRAV 5.1-04] CA skal implementere fysisk og miljømæssig kontroller til beskyttelse af systemer til håndtering af certificeringsgenerering og spærring. Kontrollerne skal inkludere fysisk adgangskontrol, beskyttelse mod naturkatastrofer, brandsikkerhed, manglende supporterende funktioner (fx strømforsyning, telekommunikation), bygningsskader, vibrationer, lækager, beskyttelse mod tyveri, indbrud og genopretning efter katastrofer (disaster recovery).

[KRAV 5.1-05] CA skal implementere kontroller til beskyttelse mod at udstyr, information, medier og software relateret til CA's tjenester bliver fjernet fra driftslokaler uden autorisation.

5.1.1 Placering og opbygning af lokaliteter

[KRAV 5.1.1-01] CA skal tydeligt beskrive, på hvilke lokaliteter medarbejdere og datacentre i forbindelse med CA's virke er placeret. De lokaler, hvor udstyr til drift af CA er placeret, herunder men ikke begrænset til servere til håndtering af nøgler og servere til statusinformation, benævnes CA driftslokaler.

[KRAV 5.1.1-02] CA skal sikre, at adgang til CA driftslokaler er begrænset til autoriserede personer.

[KRAV 5.1.1-03] CA skal segmentere sine systemer i netværk eller zoner i forhold til en risikovurdering under hensyntagen til funktionelle, logiske og fysiske (inkl. placering) sammenhænge mellem de kritiske systemer og services.

[KRAV 5.1.1-04] Kravene i denne CP gælder uanset om CA placerer hele eller dele af driftsmiljøet uden for Danmarks grænser. Den løbende kontrol, der er fastsat i CP'en, skal således kunne gennemføres uanset, hvor CA geografisk er placeret.

5.1.2 Fysisk adgang

[KRAV 5.1.2-01] CA skal etablere fysisk perimeterbeskyttelse baseret på en konkret risikovurdering.

[KRAV 5.1.2-02] Komponenter, der er afgørende for sikker drift af CA, skal befinde sig inden for en beskyttet sikkerhedsperimeter med fysisk beskyttelse mod indtrængen, adgangskontrol og alarmer for at opdage indtrængen.

[KRAV 5.1.2-03] Fysisk beskyttelse skal opnås ved at skabe klart definerede sikkerhedsgrænser (dvs. fysiske barrierer) omkring services til håndtering af certifikatgenerering og spærring.

[KRAV 5.1.2-04] CA skal sikre at CA driftslokaler, der anvendes til håndtering af certifikatgenerering og spærring, skal drives i et miljø, som fysisk beskytter disse services mod kompromittering via uautoriseret adgang til systemer eller data.

[KRAV 5.1.2-05] CA skal sikre, at adgang til alle zoner i alle CA driftslokaler begrænses til det nødvendige efter princippet om mindsteprivilegier (least priviledge).

[KRAV 5.1.2-06] CA skal ved adgangsprocedurerne sikre, at personale hos underleverandører er omfattet af CA's regler for betroet personale eller ikke kan arbejde uovervåget hos CA.

[KRAV 5.1.2-07] Andre funktioner relateret til CA's drift kan ske inden for samme sikrede zone, forudsat at adgangen er begrænset til autoriseret personale.

[KRAV 5.1.2-08] Eventuelle dele af CA driftslokalerne, der er delt med andre organisationer, skal være uden for perimeteren af services til certifikatgenerering og spærring.

[KRAV 5.1.2-09] CA skal sikre, at der etableres effektiv vagt 24 timer i døgnet.

[KRAV 5.1.2-10] CA skal sikre, at adgang til og ophold i de centrale CA driftslokaler videoovervåges.

[KRAV 5.1.2-11] CA skal sikre at enhver adgang til det fysisk sikre område skal være underlagt uafhængigt audit, og ikke-autoriseret person skal ledsages af en autoriseret person i det sikrede område.

[KRAV 5.1.2-12] CA's private rodnøgler skal opbevares og anvendes fysisk isoleret fra normale operationer, således at kun udpeget betroet personale har adgang til nøglerne til brug for digital signering af underliggende CA-certifikater, spærrelister og OCSP-svar.

[KRAV 5.1.2-13] Enhver adgang og udgang skal logges.

5.1.3 Strømforsyning og air conditioning

Se KRAV 5.1-04.

5.1.4 Vandindtrængning

Se KRAV 5.1-04.

5.1.5 Brandbeskyttelse

Se KRAV 5.1-04.

5.1.6 Håndtering af lagringsmedie

[KRAV 5.1.6-01] Alle medier i CA's driftssystem skal håndteres sikkert i overensstemmelse med klassificering herunder skal

- medier beskyttes mod skade, tyveri og uautoriseret adgang og forældelse,
- fortrolige data beskyttes mod uautoriseret adgang ved genbrug af lagringsmedier. I denne sammenhæng betragtes registreringsdata også som fortrolige data.

[KRAV 5.1.6-02] CA skal have mediehåndteringsprocesser, der sikrer medier mod forældelse og degenerering i den periode, hvor data skal lagres.

5.1.7 Bortskaffelse af affald

[KRAV 5.1.7-01] Lagringsmedier med fortroligt data skal bortskaffes med en sikker metode i overensstemmelse med klassificering.

5.1.8 Off-Site sikkerhedskopi

[KRAV 5.1.8-01] 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.

5.2 Administrative kontroller

5.2.1 Betroede roller

[KRAV 5.2.1-01] Betroede roller, hvoraf CA's sikkerhed er afhængig, skal være klart identificeret og ledelsesgodkendte.

[KRAV 5.2.1-02] CA skal etablere og implementere procedurer for alle betroede og administrative roller som kan have indvirkning på CA's sikkerhed og drift.

[KRAV 5.2.1-03] Alle CA's medarbejdere med betroede roller skal være fri for interessekonflikter, der kan skade uafhængigheden af CA's drift.

[KRAV 5.2.1-04] De betroede roller skal inkludere roller, med følgende ansvar:

a) Security Officers: Samlet implementeringsansvar for administrationen af sikkerhedspraksis.

b) System Administrators: Autoriseret til at installere, konfigurere og vedligeholde CA's kritiske systemer til service management inklusive systemgenskabelse.

c) Systemoperatører: Ansvarlig for driften af CA's kritiske systemer på daglig basis. Autoriseret til at udføre sikkerhedskopi af system.

d) Systemrevisorer: Autoriseret til at se lagrede data og audit-logfiler fra CA's kritiske systemer.

e) Registration Officers: Som defineret i CEN TS 419 261.

f) Revocation Officers: Som defineret I CEN TS 419 261.

[KRAV 5.2.1-05] Opgaver og ansvarsområder, der kan indeholde konfliktende interesser, skal adskilles for at reducere mulighederne for uautoriseret eller utilsigtet ændring eller misbrug af CA's aktiver.

5.2.2 Antal krævede personer per opgave

[KRAV 5.2.2-01] Certifikatudstedelse fra rod-CA skal være under dual kontrol af autoriseret, betroet personale, således at én person ikke alene kan udstede certifikater.

5.2.3 Identifikation og autentikation for hver rolle

[KRAV 5.2.3-01] Personale, der skal tilgå eller konfigurere rettigheder for betroede roller skal være formelt godkendt af en sikkerhedsansvarlig på øverste ledelsesniveau efter "least privilege"-princippet.

[KRAV 5.2.3-02] Tildeling af en betroet rolle til en medarbejder skal godkendes af ledelsen og accepteres af medarbejderen, der tildeles rollen.

[KRAV 5.2.3-03] CA's personale (både midlertidigt og permanent) skal have jobbeskrivelser defineret ud fra de roller de skal udfylde under hensyntagen til adskillelse af pligter (segregation of duties), mindsteprivilegier (least priviledge), følsomheden af data som kan tilgås, baggrundstjek og medarbejders uddannelse og awareness.

[KRAV 5.2.3-04] Hvor det er relevant skal jobbeskrivelser skelne mellem generelle funktioner og CA-specifikke funktioner. Sidstnævnte bør omfatte krav til færdigheder og erfaring.

[KRAV 5.2.3-05] Personale må ikke have adgang til funktioner forbeholdt betroede roller før de nødvendige kontroller er gennemført.

5.2.4 Roller der ikke kan besættes af samme person (Separation of Duties)

[KRAV 5.2.4-01] CA skal sikre, at personer med auditørfunktioner hos CA ikke refererer til samme ledelse som driftsansvarlige og administratorer refererer til.

5.3 Personalesikkerhed

[KRAV 5.3-01] CA skal sikre at personale og underleverandører understøtter en tillidsfuld drift af CA.

5.3.1 Kvalifikationer, erfaring og godkendelseskrav

[KRAV 5.3.1-01] CA skal ansætte personale, og hvor det er relevant, anvende underleverandører, som har den nødvendige ekspertise, pålidelighed, erfaring og kvalifikationer, og som har modtaget uddannelse vedrørende informationssikkerhed og beskyttelse af persondataoplysninger, der er relevant for de udbudte tjenester og jobfunktionen.

[KRAV 5.3.1-02] Ledende medarbejdere skal have erfaring eller træning i forhold til drift af CA, kendskab til sikkerhedsprocedurer for personale med sikkerhedsansvar og erfaring med informationssikkerhed og risikovurdering, der er tilstrækkelig til at kunne udføre ledelsesfunktioner for CA.

[KRAV 5.3.1-03] Sikkerhedsroller og -ansvar som angivet i CA's informationssikkerhedspolitik skal dokumenteres i stillingsbeskrivelser eller i dokumenter, der er tilgængelige for alle berørte medarbejdere.

5.3.2 Procedure for baggrundscheck

[KRAV 5.3.2-01] CA skal gennemføre en tilstrækkelig identifikation af personale i forbindelse med ansættelse.

[KRAV 5.3.2-02] 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.

5.3.3 Uddannelseskrav

[KRAV 5.3.3-01] CA's personale inklusive personale ved eventuelle underleverandører skal være i stand til at opfylde kravet om "ekspertviden, erfaring og kvalifikationer" gennem formelle uddannelser og akkrediteringer eller gennem egentlig erfaring eller en kombination af de to.

[KRAV 5.3.3-02] RA personale skal gennemføre en uddannelse, som sætter dem i stand til at udføre deres arbejde korrekt og sikkert.

5.3.4 Frekvens for og krav til efteruddannelse

[KRAV 5.3.4-01] Ovenstående uddannelseskrav bør omfatte regelmæssige (mindst hver 12 måneders) opdateringer om nye trusler og nuværende sikkerhedspraksis.

5.3.5 Frekvens og regler for jobrotation

N/A

5.3.6 Sanktioner ved uautoriserede handlinger

[KRAV 5.3.6-01] Personale skal anvende administrative procedurer og processer, der er i overensstemmelse med CA's informationssikkerhedsstyringsprocedurer.

[KRAV 5.3.6-02] Der skal anvendes passende disciplinære sanktioner for personale, der overtræder CA's politikker eller procedurer.

5.3.7 Krav til uafhængige kontraktansatte

[KRAV 5.3.7-01] CA skal sikre, at personalet hos underleverandører opfylder samme krav til uddannelse, erfaring og sikkerhedsklassifikation som CA's egne medarbejdere i de funktioner, underleverandørens personale varetager for CA.

5.3.8 Dokumentation og uddannelsesmateriale til personale

N/A

5.4 Audit logningsprocedurer

5.4.1 Type af hændelser, der skal logges

[KRAV 5.4.1-01] Alle sikkerhedskritiske aktiviteter skal logges, herunder ændringer i forbindelse med sikkerhedspolitik, systemstart og nedlukning, systemnedbrud og hardwarefejl, firewall og routeraktiviteter og forsøg på PKI-systemadgang.

[KRAV 5.4.1-02] Alle begivenheder i forbindelse med registrering inklusive anmodninger om genudstedelse eller fornyelse af certifikater skal logges.

[KRAV 5.4.1-03] Alle livscyklushændelser relateret til CA's private nøgler skal logges af CA.

[KRAV 5.4.1-04] Alle livscyklushændelser hos CA relateret til certifikater skal logges af CA herunder skal al relevante information om udsendte og modtagne data gemmes og alle hændelser relateret til registrering, generering, formidling og eventuelt spærring af kvalificerede certifikater logges. Endelig skal hændelser i forbindelse med håndtering af certifikatholders kryptografiske moduler logges.

[KRAV 5.4.1-05] Alle livscyklushændelser relateret til nøgler håndteret af CA, inklusiv eventuel håndtering af certifikatholderes nøgler skal logges af CA.

[KRAV 5.4.1-06] Alle rapporteringer og anmodninger om spærring og den resulterende handling skal logges af CA.

[KRAV 5.4.1-07] Alle adgange og adgangsforsøg til områder, der skal beskyttes af adgangskontrol, skal logges af CA.

[KRAV 5.4.1.08] Alle livscyklushændelser hos CA relateret til QSCD'er skal logges, herunder initiering og eventuel personalisering.

5.4.2 Frekvens for processering af auditlog

[KRAV 5.4.2-01] CA skal dokumentere og følge skriftlige politikker for regelmæssig gennemgang af alle auditlogs. Frekvens for gennemgang skal være fastlagt i CPS.

5.4.3 Opbevaringstid for auditlog

[KRAV 5.4.3-01] CA skal lagre log over alle livscyklushændelser relateret til CA's håndtering af nøgler, inklusiv eventuel håndtering af certifikatholderes nøgler i mindst syv år efter gyldighedsophør af ethvert certifikat relateret til loggen.

[KRAV 5.4.3-02] CA skal lagre alle øvrige auditlogs i mindst syv år.

5.4.4 Beskyttelse af auditlog

[KRAV 5.4.4-01] CA skal sikre fortroligheden og integriteten af logdata herunder skal hændelser logges på en måde, så log ikke let kan slettes eller ødelægges i den

periode, som loggen skal gemmes (medmindre den er overflyttet sikkert til medie til langtidsopbevaring).

[KRAV 5.4.4-02] CA skal sikre beskyttelse af certifikatholderes privatliv.

[KRAV 5.4.4-03] CA skal opbevare og håndtere logdata i henhold til gældende lov også efter ophør af CA tjenesten.

[KRAV 5.4.4-04] CA skal i CPS dokumentere hvorledes, logdata kan tilgås både før og efter ophør af CA tjenesten og CA skal i CPS dokumentere opbevaringstid jf. afsnit 5.4.3 og hvilke logdata der overdrages i forbindelse med ophør af CA tjenesten.

5.4.5 Procedure for sikkerhedskopi for auditlog

[KRAV 5.4.5-01] CA skal implementere procedure for regelmæssig sikkerhedskopiering af auditlogs.

5.4.6 Auditsystem (intern eller ekstern)

N/A

5.4.7 Notifikation til part, der var årsag til logningshændelse

N/A

5.4.8 Sårbarhedsvurdering

N/A

5.5 Datalagring

[KRAV 5.5-01] 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.

[KRAV 5.5-02] CA og RA skal sikre, at alt elektronisk arkivmateriale gemmes med angivelse af arkiveringstidspunktet.

Note: Der er ikke krav om at tidsstempling skal være baseret på elektroniske tidsstempler eller kvalificerede elektroniske tidsstempler jf. [eIDAS]

5.5.1 Type af data der skal lagres

[KRAV 5.5.1-01] CA skal registrere og kunne tilgå alle relevante oplysninger vedrørende data genereret og modtaget af CA i et passende tidsrum, herunder efter ophør af aktiviteterne i CA, navnlig med henblik på at kunne fremlægge bevismateriale i retssager og kunne sikre tjenestens kontinuerte drift.

[KRAV 5.5.1-02] Alle registreringsoplysninger skal registreres, herunder:

a) Type(r) af dokumentation, som er fremlagt i forbindelse med registreringen.

b) Registrering af unikke identifikationsdata, numre eller en kombination heraf af identifikationsdokumenter, hvis det er relevant og med respekt for certifikatholders privatlivsbeskyttelse.

c) Placering af gemte kopier af ansøgninger og identifikationsdokumenter, herunder indgående aftaler.

d) Eventuelle specifikke valg i aftaler fx samtykke til offentliggørelse af certifikater.

e) Identiteten på den person, der accepterer aftaler.

f) Den anvendte metode for validering af dokumentation for identitet, hvis relevant.

g) Angivelse af navn på modtagne CA og RA, hvis relevant.

[KRAV 5.5.1-03] CA skal sikre at følgende data lagres:

a) Certifikatanmodninger og relevant tilhørende kommunikation, herunder anmodninger relateret til fornyelse.
b) Signerede ordrer og skriftlige aftaler,
c) CPS (alle godkendte versioner).

[KRAV 5.5.1-04] Al videoovervågning af CA driftslokaler skal lagres.

5.5.2 Lagringstid for data

[KRAV 5.5.2-01] Data skal lagres i mindst syv år til at kunne anvendes som bevis og under hensyntagen til privatlivsbeskyttelse. Politik for lagringstid skal dokumenteres og oplyses i vilkår og betingelser. Dette er også gældende for evt. data fra RA's it-systemer, som er relevante for dokumentation af CA's virke.

[KRAV 5.5.2-02] Specielt skal CA skal gemme dokumentation beskrevet i afsnit 4.4 i mindst syv år efter gyldighedsophør af ethvert certifikat relateret til loggen.

5.5.3 Beskyttelse af lagrede data

[KRAV 5.5.3-01] CA skal sikre fortroligheden og integriteten af lagrede data relateret til driften af CA's services.

[KRAV 5.5.3-02] CA skal sikre komplethed, fortroligheden og integriteten af lagrede data relateret til driften af CA's services i henhold til dokumenteret forretningspraksis offentliggjort i CPS.

5.5.4 Procedure for sikkerhedskopiering af lagrede data

[KRAV 5.5.4-01] Der skal tages regelmæssige sikkerhedskopier af kritiske data og software i overensstemmelse med ISO 27002, clause 12.3.

[KRAV 5.5.4-02] Der bør sikres tilstrækkelige sikkerhedskopieringsfaciliteter for at sikre, at al væsentlig information og software kan genskabes efter en kritisk hændelse eller fejl i lagringsmedier.

[KRAV 5.5.4-03] CA's systemdata, der er nødvendige for at genetablere CA-drift efter en kritisk hændelse/katastrofe, skal sikkerhedskopieres og opbevares sikkert, gerne på off-site lokation, så det er muligt for CA at genetablere drift inden for rimelig tid.

[KRAV 5.5.4-04] Back-up løsninger skal testes regelmæssigt for at sikre, at de opfylder kravene i fastlagte genetableringsplaner.

[KRAV 5.5.4-05] Sikkerhedskopierings- og gendannelsesfunktioner skal udføres af de relevante betroede roller, der er specificeret i afsnit 5.2.1.

[KRAV 5.5.4-06] Data, der gennem risikoanalyse er identificeret til at kræve håndtering ved brug af dual kontrol, fx nøgler, skal anvende dual kontrol i forbindelse med genskabelse.

5.5.5 Krav til tidsstempling af lagrede data

N/A

5.5.6 Lagringssystemer (interne eller eksterne)

N/A

5.5.7 Procedure for fremsøgning og verifikation af lagrede data

[KRAV 5.5.7-01] Data herunder auditlog skal kunne fremfindes og stilles til rådighed som bevis i en retssag.

5.6 Skift af nøgler

[KRAV 5.6-01] CA skal sikre, at der, inden udløb af den private nøgle, genereres et nyt CA-nøglepar, der kan benyttes til udstedelse af certifikater.

5.7 Kompromittering og beredskabsplanlægning

[KRAV 5.7-01] Følgende sikkerhedshændelser skal betragtes som kritiske:

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

5.7.1 Hændelses- og kompromitteringshåndtering

[KRAV 5.7.1-01] Systemaktiviteter som adgang til it-systemer, brug af it-systemer og kald af services skal overvåges.

[KRAV 5.7.1-02] Overvågningen skal tage højde for følsomheden af de data, der indsamles eller analyseres.

[KRAV 5.7.1-03] Unormale systemaktiviteter, der udgør et potentiel sikkerheds-brud, herunder indtrængen i CA's netværk skal registreres og rapporteres som alarmer.

[KRAV 5.7.1-04] CA skal overvåge følgende hændelser:

a) opstart og nedlukning af logfunktionerne og

b) tilgængelighed og brug af nødvendige tjenester med CA's netværk.

[KRAV 5.7.1-05] CA skal handle rettidigt og koordineret for at reagere hurtigt på sikkerhedshændelser og begrænse konsekvenserne af sikkerhedsbrud.

[KRAV 5.7.1-06] CA skal have personale med betroet rolle til opfølgning på ad-varsler om potentielt kritiske sikkerhedshændelser og sikrer, at relevante hændel-ser rapporteres i overensstemmelse med CA's procedurer.

[KRAV 5.7.1-07] CA skal have procedurer og beredskab, der sikre notifikation af sikkerhedshændelse eller tab af integritet til relevante parter jf. gældende regulering fx databeskyttelsesmyndigheder senest 72 timer efter og/eller eIDAS tilsynsorgan senest 24 timer efter, at hændelsen er identificeret.

[KRAV 5.7.1-08] Hvis der er en sandsynlighed for, at en sikkerhedshændelse eller tab af integritet kan påvirke en fysisk person eller en juridisk enhed negativt, skal CA også notificere denne uden unødig forsinkelse.

[KRAV 5.7.1-09] CA's systemer skal overvåges, hvilket skal omfatte monitorering eller regelmæssige gennemgang af auditlogs for at identificere ondsindet aktivitet med henblik på at alarmere potentielle kritiske sikkerhedshændelser til sikkerheds-personale.

[KRAV 5.7.1-10] CA skal håndtere enhver kritisk sårbarhed, som ikke tidligere er håndteret af CA, inden for 48 timer efter at den er identificeret.

[KRAV 5.7.1-11] For enhver identificeret sårbarhed skal CA i forhold til de po-tentielle skader enten

- oprette og implementere en plan for mitigering af sårbarheden eller
- dokumentere grundlaget for CA's beslutning om, at sårbarheden ikke kræ-ver mitigering.

[KRAV 5.7.1-12] Hændelsesrapporterings- og responsprocedurer skal etableres på en sådan måde, at skader fra sikkerhedshændelser og funktionsfejl minimeres.

5.7.2 Skader på hardware, software og/eller data

[KRAV 5.7.2-01] CA skal i tilfælde af kritiske 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 modtagerparter informeres via offentlige medier og ved annoncering i dagspressen.

[KRAV 5.7.2-02] CA skal sikre, at alle procedurer med relation til spærrelister, herunder anmodning om spærring, har højeste prioritet i forbindelse med retablering af forretningsgange efter et nedbrud.

5.7.3 Procedure ved privatnøglekompromittering

[KRAV 5.7.3-01] CA's Business Continuity Plan (eller katastrofegenoprettelsesplan) skal håndtere kompromittering, tab og formodning om kompromittering af en af CA's private nøgler som kritisk hændelse eller katastrofe.

[KRAV 5.7.3-02] Der skal være fastlagt planlagte processer til håndtering af kompromittering, tab eller formodning om kompromittering af en af CA's private nøgler. Planen skal indeholde processer for håndtering af certifikatholderes certifikater udstedt under berørte nøgler.

[KRAV 5.7.3-03] Ved kompromittering af CA's private nøgler skal CA

- informere certifikatindehaver og andre parter, som har et aftaleforhold med CA eller anden relevant relation til CA fx andre tillidstjenesteudbydere og modtagerparter,
- informere Digitaliseringsstyrelsen med en uddybende beskrivelse af den opstående situation,
- gøre information om kompromittering tilgængelig for tredjeparter,
- angive, at certifikater og spærrestatusoplysninger udstedt ved hjælp af denne CA-nøgle ikke længere er gyldige og
- spærre ethvert CA-certifikat, der er udstedt med en offentlig nøgle svarende til den kompromitterede CA-nøgle.

[KRAV 5.7.3-04] I det tilfælde at nogen af de algoritmer eller tilknyttede parametre, der anvendes af CA eller certifikatindehavere, får utilstrækkelige sikkerhed inden for perioden for resterende tilsigtede brug, skal CA informere alle certifikatindehavere og modtagerparter, som CA har aftale eller anden form for etablerede forbindelser med. Desuden skal CA stille disse oplysninger til rådighed for andre modtagerparter.

[KRAV 5.7.3-05] I det tilfælde at nogen af de algoritmer eller tilknyttede parametre, der anvendes af CA eller certifikatindehavere, får utilstrækkelige sikkerhed inden for perioden for resterende tilsigtede brug, skal CA spærre alle gyldige berørte certifikater.

[KRAV 5.7.3-06] CA skal have dokumenteret plan for hændelse med generel kompromittering af mange certifikatholderes private nøgler.

5.7.4 Business Continuity kapaciteter efter en kritisk hændelse

[KRAV 5.7.4-01] CA skal fastlægge, teste og vedligeholde en Business Continuity Plan (BCP), der skal aktiveres i forbindelse med en driftsmæssig katastrofe.

[KRAV 5.7.4-02] I tilfælde af en driftsmæssig katastrofe herunder kompromittering af en af CA's private signeringsnøgler skal driftens genoprettes inden for den frist, der er fastlagt i BCP, idet årsagen til katastrofen er håndteret med passende afhjælpende foranstaltninger.

[KRAV 5.7.4-03] Efter en katastrofe skal CA, hvor det er muligt, implementere mitigerende forholdsregler for at undgå gentagelser.

5.8 Ophør af CA eller RA

[KRAV 5.8-01] CA skal løbende vedligeholde en plan for ophør af CA-tjenesterne.

[KRAV 5.8-02] CA skal i CPS angive bestemmelser ved ophør af tjenesten. Disse skal som minimum inkludere information om hvem der bliver notificeret ved ophør og hvem, der overtager kunder og brugere, hvis der findes denne type aftaler, samt hvem der overtager ansvar for spærringsstatustjenesten.

[KRAV 5.8-03] Forud for ophør skal CA informere relevante myndigheder herunder Digitaliseringsstyrelsen, certifikatindehavere og alle øvrige parter, der har et kontraktligt forhold til CA. Desuden skal CA gøre information om ophør tilgængelig for modtagerparter inden ophøret.

[KRAV 5.8-04] CA skal sikre, at al udstedelse og fornyelse af certifikater straks stoppes, når en CA-funktion ophører med at fungere.

[KRAV 5.8-05] Potentielle forstyrrelser for certifikatindehavere og andre parter skal minimeres som følge af ophør af CA's tjenester. 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. Desuden skal CA sikre, at CA's rodcertifikater og mellemliggende certifikater stilles til rådighed for offentligheden i en rimelig periode.

[KRAV 5.8-06] CA skal sikre, at arkiver er tilgængelige i mindst syv år efter udløb af sidste certifikat udstedt af denne CA, herunder information om registrering, spærringsinformation og hændelseslog.

[KRAV 5.8-07] Som led i at CA ophører med at levere tjenester, skal CA lukke for autorisation for alle eventuelle underleverandører til at handle på vegne af CA ved udførelse af funktioner i forbindelse med processen med udstedelse og håndtering af certifikater.

[KRAV 5.8-08] Som led i at CA ophører med at levere tjenester, skal CA's private nøgler, herunder sikkerhedskopier, destrueres eller gøres utilgængelige for brug på en sådan måde, at de private nøgler ikke kan genskabes.

[KRAV 5.8-09] Hvis det er muligt, skal CA forsøge at overdrage leverance af tillidstjenesten for de eksisterende kunder og brugere til en anden CA.

[KRAV 5.8-10] Hvis en anden krydscertificeret CA ophører, herunder ophører håndtering af spærringstjeneste, skal alle krydscertifikater til denne CA spærres.

[KRAV 5.8-11] Hvis CA er en privat virksomhed eller en fysisk person, skal CA stille en uigenkaldelig anfordringsgaranti eller lignende i et godkendt institut til sikring af betaling af sine økonomiske forpligtelser i henhold til KRAV 5.8-1 til KRAV 5.8-10.

6. Tekniske sikkerhedskontroller

6.1 Generering og installation af nøglepar

6.1.1 Generering af nøglepar

[KRAV 6.1.1-01] Certifikatudsteders certifikater skal være gyldige i mindst 5 år.

[KRAV 6.1.1-02] CA skal implementere en sikker håndtering af kryptografiske nøgler og kryptografiske moduler. Håndteringen skal dække hele livscyklussen for nøgler og moduler.

[KRAV 6.1.1-03] For kritiske dele af CA's infrastruktur, skal CA følge relevante og officielle anbefalinger fra ENISA vedr. anvendelsen af tidssvarende algoritmer og nøglelængder i det omfang at anbefalinger er opdateret.

[KRAV 6.1.1-04] CA skal generere CA-nøgler, herunder nøgler, der anvendes ved spærrings- og registreringstjenester, sikkert, og den private nøgle skal være hemmelig.

[KRAV 6.1.1-05] Særligt skal følgende iagttages:

- CA-nøgle generering og den efterfølgende certificering af den offentlige nøgle skal gennemføres i et fysisk sikret miljø (jf. afsnit. 5.1) af personale i betroede roller (jf. afsnit 5.2).
- CA-nøgler, der anvendes til at signere certifikater, skal oprettes under dual kontrol under overvågning af to personer med hver sin betroede funktion i CA.
- Antallet af personer, der er autoriseret til at udføre CA-nøglegenerering, skal holdes på et minimum og være i overensstemmelse med CA's CPS.
- CA-nøglegenerering skal udføres ved hjælp af en algoritme som specificeret i ETSI TS 119 312 til CA's signeringsformål.

- Den valgte nøglelængde og algoritme for CA-signaturnøglen skal være en, der er angivet i ETSI TS 119 312 til CA's signeringsformål. Dog kan anbefaling til valg af kryptografiske algoritmer og parametre defineret i ETSI TS 119 312 erstattes af nationale anbefalinger.

[KRAV 6.1.1-06] Inden udløb af CA-certifikat, som anvendes til at signere certifikatholders certifikater, skal CA, hvis den fortsætter med tjenesten, oprette et nyt certifikat til signering af certifikatholderes certifikater og gennemfører nødvendige tiltag for at undgå forstyrrelser i driften af enhver part, der har tillid til CA-certifikatet.

[KRAV 6.1.1-07] Inden udløb af CA-certifikat, som anvendes til at signere certifikatholders certifikater, skal det nye CA-certifikat, hvis CA fortsætter med tjenesten, genereres og distribueres i overensstemmelse med nærværende dokument.

[KRAV 6.1.1-08] De to ovenstående krav skal udføres med passende interval mellem CA certifikatets udløbstidspunkt og det sidst udstedte certifikat til en certifikatholder, således at alle parter med en relation til CA (certifikatholdere, certifikatindehavere, modtagerparter og andre relevante CA'er) kan blive opmærksomme på nøgleskiftet og implementere nødvendige tilretninger for at undgå fejl og ulemper. Dette gælder dog ikke, hvis CA ophører med tjenesten inden udløb af CA-certifikat.

[KRAV 6.1.1-09] CA skal have en dokumenteret procedure benævnt "Key Signing Ceremony (KSC)" til gennemførelse af CA-nøglegenerering til certifikat for certifikatudstedes. Dette gælder for alle CA'er, (rod-CA og underliggende CA'er, herunder CA'er, der udsteder certifikater til certifikatholdere).

[KRAV 6.1.1-10] KSC skal som minimum indeholde:

a) Roller der deltager (både interne og eksterne).

b) Funktioner, der skal udføres af hver rolle og i hvilke faser.

c) Ansvar under og efter ceremonien.

d) Krav til dokumentation, der indsamles som bevis for ceremonien.

[KRAV 6.1.1-11] CA skal udarbejde en rapport, der viser, at nøglegenereringen blev udført i overensstemmelse med den angivne KSC-procedure, og at nøgleparrets integritet og fortrolighed var sikret.

[KRAV 6.1.1-12] Rapporten skal som minimum underskrives af

- For rod-CA: af den betroede rolle, der er ansvarlig for sikkerheden i CA's nøglehåndtering (fx sikkerhedsansvarlig) samt en betroet person, der er uafhængig af CA's ledelse (fx overensstemmelsesorganet) som kan bevidne, at rapporten korrekt beskriver at KSC er efterlevet.

- For underliggende CA'er: af den betroede rolle, der er ansvarlig for sikkerheden i CA's nøglehåndtering (fx sikkerhedsansvarlig), som kan bevidne, at rapporten korrekt beskriver at KSC er efterlevet.

[KRAV 6.1.1-13] CA skal sikre, at certifikatholders nøgler, som genereres af CA, genereres sikkert, og at hemmeligholdelsen af certifikatholderens private nøgler er sikret.

[KRAV 6.1.1-14] Hvis CA genererer certifikatholders nøgler, skal disse generes ved hjælp af en algoritme, der er anerkendt som værende egnet til de anvendelser, der er identificeret i denne CP'en i hele certifikatets gyldighedsperiode.

[KRAV 6.1.1-15] Hvis CA genererer certifikatholders nøgler, skal disse generes med nøglelængder og algoritmer som angivet i ETSI TS 119 312. Dog kan anbefaling til valg af kryptografiske algoritmer og parametre defineret i ETSI TS 119 312 erstattes af nationale anbefalinger.

[KRAV 6.1.1-16] Hvis CA genererer certifikatholders nøgler, skal disse generes og opbevares sikkert så længe, de holdes af CA på en måde der sikrer, at det kun er certifikatholderen selv, som kan anvende den private nøgle.

[KRAV 6.1.1-17] Uanset om CA kontrollerer det kryptografiske modul til håndtering af certifikatholders nøgler initieres af CA eller andre, skal CA sikre, at det er et certificeret QSCD jf. eIDAS.

[KRAV 6.1.1-18] Hvis det kryptografiske modul til håndtering af certifikatholders nøgler håndteres på vegne af certifikatholder af en anden tillidstjeneste end CA, skal CA sikre, at denne anden tillidstjeneste opfylder krav jf. eIDAS, herunder at det er en kvalificeret tillidstjenesteudbyder.

[KRAV 6.1.1-19] Certifikatanmodningsprocessen skal sikre, at certifikatholders offentlige nøgle, der skal indgå i certifikatet, kommer fra et nøglepar genereret i et QSCD.

[KRAV 6.1.1-20] Hvis certifikatholderens nøglepar genereres af en kvalificeret tillidstjenesteudbyder og importeres til en QSCD til signering, skal de miljømæssige forudsætninger og sikkerhedsmål for det givne QSCD opfyldes af tillidstjenesteudbyderen.

[KRAV 6.1.1-21] Hvis certifikatholderens private nøgle flyttes mellem kryptografiske moduler, skal potentielle sårbarheder relateret til kompromittering af nøglen identificeres og mitigeres med tilstrækkelige mekanismer.

6.1.2 Levering af privat nøgle til certifikatholder

[KRAV 6.1.2-01] Hvis CA genererer certifikatholders nøgler, skal den private nøgle leveres til certifikatholders nøglebeskyttelsesmiddel eller til en tillidstjeneste, som håndterer certifikatholders private nøgle, på en sådan måde, at den private nøgles fortrolighed og integritet ikke kompromitteres. Eksempelvis må et kryptografisk modul og tilhørende aktiveringskode ikke leveres, så de ankommer i samme forsendelse.

[KRAV 6.1.2-02] Hvis CA genererer certifikatholders nøgler, og hvis CA eller en af dets udpegede RA'er bliver opmærksomme på, at en certifikatholders private nøgle er blevet kommunikeret til en uautoriseret person eller en organisation, der

ikke er tilknyttet certifikatholder, skal CA spærre alle certifikater, der indeholder den offentlige nøgle svarende til den kommunikerede private nøgle.

[KRAV 6.1.2-03] Hvis CA genererer certifikatholders nøgler, skal CA slette alle kopier certifikatholders privat nøgle efter levering af den private nøgle til certifikatholder.

[KRAV 6.1.2-04] Hvis CA genererer certifikatholders nøgler, skal CA sikre udstedelse af et kryptografisk modul til certifikatholder.

Særlig gælder at

> **[KRAV 6.1.2-05]** Hvis CA genererer certifikatholders nøgler, skal det kryptografiske modul initieres sikkert.
>
> Og
>
> **[KRAV 6.1.2-06]** Hvis CA genererer certifikatholders nøgler, skal det kryptografiske modul lagres og distribueres sikkert.

6.1.3 Levering af offentlig nøgle til certifikatudsteder

[KRAV 6.1.3-01] Hvis certifikatholder eller certifikatindehaver leverer certifikatholders offentlige nøgle til CA, skal dette ske med en mekanisme, der sikrer integriteten af nøglen.

6.1.4 Levering af CA's offentlige nøgle til modtagerparter

[KRAV 6.1.4-01] CA's (offentlige) nøgler skal være tilgængelige for at modtagerparter på en måde, der sikrer integriteten af CA-nøglen og autentificerer dens oprindelse.

[KRAV 6.1.4-02] Særligt skal CA give mulighed for verifikation af rodcertifikatet via anden kanal. Verifikation kan f.eks. ske ved anvendelse af et fingerprint for certifikatet.

6.1.5 Nøglelængder

Se afsnit 6.1.1.

6.1.6 Generering og kvalitetskontrol af offentlig nøgle parametre

N/A

6.1.7 Nøgleanvendelsesformål (X.509v3 keyUsage)

[KRAV 6.1.7-01] CA skal inkludere extension keyUsage i udstedte certifikater til certifikatholder og keyUsage skal efterleve krav i afsnit 4.3.2 Key usage i [ETSI EN 319 412-2].

6.2 Beskyttelse af private nøgler og anvendelse af kryptografiske moduler

[KRAV 6.2-01] CA skal sikre, at CA's rodnøgler ikke kompromitteres og til stadighed bevarer deres integritet.

6.2.1 Kryptografiske moduler – standarder og evalueringer

[KRAV 6.2.1-01] CA's nøglegenerering, herunder generering af nøgler, der anvendes ved spærrings- og registreringstjenester, skal ske i et kryptografisk modul, som udgør et troværdigt system der

a) er evalueret EAL 4 eller højere i overensstemmelse med ISO 15408 eller tilsvarende nationale eller internationalt anerkendte evalueringskriterier for it-sikkerhed, forudsat at dette er et sikkerhedsniveau eller en beskyttelsesprofil, der opfylder kravene i dette dokument baseret på en risikoanalyse og under hensyntagen til fysiske og andre ikke-tekniske sikkerhedsforanstaltninger eller

b) lever op til kravene identificeret i ISO/IEC 19790 eller FIPS 140-2 level 3.

Note: I takt med at produkter, der opfylder KRAV 6.2.1-01 a), bliver generelt tilgængelige forventes det, at KRAV 6.2.1-01 b) vil blive fjernet i kommende versioner af denne CP.

[KRAV 6.2.1-02] Det kryptografiske modul skal betjenes i sin konfiguration som beskrevet i den relevante certificeringsvejledningsdokumentation eller i en ækvivalent konfiguration, der opnår det samme sikkerhedsniveau.

[KRAV 6.2.1-03] CA skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering ikke er blevet kompromitteret inden installation.

[KRAV 6.2.1-04] CA skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering ikke bliver kompromitteret under brug.

[KRAV 6.2.1-05] 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 rolle i CA.

[KRAV 6.2.1-06] CA skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering altid fungerer korrekt.

[KRAV 6.2.1-07] CA private nøgle til signering skal opbevares og anvendes i et sikkert kryptografisk modul, der opfylder kravene ovenfor.

6.2.2 Privat nøgle (n ud af m) multi-person kontrol

Se KRAV 6.2.4-01.

6.2.3 Nøgledeponering

Se KRAV 4.12.1-01.

6.2.4 Sikkerhedskopiering af privat nøgle

[KRAV 6.2.4-01] CA's private nøgle til signering skal kun sikkerhedskopieres, opbevares og genetableres af personale i betroede roller under mindst dual kontrol i et fysisk sikret miljø jf. afsnit 5.1.

[KRAV 6.2.4-02] Antallet af personer, der er autoriseret til at lave sikkerhedskopier, opbevare og genetablere CA's private nøgle til signering skal holdes på et minimum og være i overensstemmelse med CA's CPS.

[KRAV 6.2.4-03] Kopier af CA's private nøgle til signering skal være underlagt samme eller højere sikkerhedsniveau som nøgler i brug.

6.2.5 Arkivering af privat nøgle

[KRAV 6.2.5-01] Når CA's private nøgle til signering opbevares uden for det sikre kryptografiske modul, skal denne nøgle beskyttes på en måde, der sikrer det samme beskyttelsesniveau som for det sikre kryptografiske modul.

6.2.6 Overførsel af privat nøgle til eller fra et kryptografisk modul

[KRAV 6.2.6-01] 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.

[KRAV 6.2.6-02] Transport af CA's rodnøgler og andre kritiske private nøgler skal ske under overvågning af to personer med hver sin betroede funktion i CA.

Note: Certifikatholderes private nøgler anses i denne sammenhæng som udgangspunkt ikke kritiske private nøgler, medmindre de fx anvendes i forbindelse med administration af CA's systemer.

6.2.7 Lagring af privat nøgle i kryptografisk modul

[KRAV 6.2.7-01] Når CA private nøgler til signering og eventuelle kopier er gemt i et dedikeret sikkert kryptografisk modul, skal der forefindes adgangskontroller der sikre, at nøglerne ikke er tilgængelige uden for dette modul.

[KRAV 6.2.7-02] Der må ikke manipuleres med det sikre kryptografiske modul under forsendelsen.

[KRAV 6.2.7-03] Der må ikke manipuleres med det sikre kryptografiske modul under opbevaring.

[KRAV 6.2.7-04] Det sikre kryptografiske modul skal fungere korrekt.

6.2.8 Aktivering af privat nøgle

[KRAV 6.2.8-01] CA skal sikre, at certifikatholders private nøgle ikke kan anvendes, uden at certifikatholderen i hvert tilfælde har autoriseret anvendelsen, således at certifikatholderen opretholder egenkontrol over sin private nøgle.

Dette kan ske:

- Gennem aftale der forpligter certifikatindehaver, hvis den private nøgle genereres og anvendes alene under certifikatindehavers kontrol.
- Ved hjælp af en kombination af tekniske kontroller og aftaler, der forpligter certifikatindehaver og andre relevante parter, hvis den private nøgle genereres og anvendes helt eller delvis af en tillidstjeneste.

6.2.9 Deaktivering af privat nøgle

N/A

6.2.10 Destruktion af privat nøgle

[KRAV 6.2.10-01] CA's private nøgler til signering, der er gemt på CA's sikre kryptografiske modul, skal destrueres når modulet ikke længere skal anvendes til håndtering af CA's private nøgler til signering.

6.2.11 Klassificering af kryptografisk modul

[KRAV 6.2.11-01] CA skal overvåge anvendte QSCD'ers (herunder certifikatholderes QSCD'er) certificeringsstatus indtil udløb af certifikater på QSCD'erne. CA skal foretage passende foranstaltninger ved ændring af denne status for et QSCD's. Disse foranstaltninger skal dokumenteres i CPS.

6.3 Andre aspekter af nøglehåndtering

[KRAV 6.3-01] CA skal udelukkende anvende CA's private nøgler til signering på passende måde, herunder

- CA må ikke anvende private nøgler til signering efter afslutning på nøglernes livscyklus.
- CA's private nøgler, der anvendes til at generere kvalificerede certifikater og/eller udstedelse af spærrestatusoplysninger, må ikke anvendes til andre formål.
- CA's private nøgler, der anvendes til at generere certifikater, må kun anvendes inden for de fysisk sikrede lokaler.
- Brugen af CA's private nøgle skal være i overensstemmelse med hash-algoritmen, signaturalgoritmen og nøglelængden, der anvendes til generering af certifikater, i overensstemmelse med den nuværende praksis som i krav afsnit 6.1.
- Alle kopier af CA's private nøgler til signering skal destrueres, når de er nået slutningen af deres livscyklus.
- Hvis CA har udstedt et selvsigneret certifikat, skal certifikatets attributter være i overensstemmelse med den definerede nøglebrug som defineret i Recommendation ITU-T X.509 og krav i afsnit 6.1.

Note: CA kan udstede interne driftsrelaterede certifikater.

[KRAV 6.3-02] Hvis certifikatholders nøgler håndteres af CA, skal det fremgå af CPS, hvorvidt CA sikrer sig, at certifikatet er gyldigt i forbindelse med brug af certifikatholders private nøgle.

6.3.1 Lagring af offentlige nøgler

N/A

6.3.2 Anvendelsesperiode for certifikat og nøglepar

N/A

6.4 Aktiveringsdata

6.4.1 Generering og installation af aktiveringsdata

[KRAV 6.4.1-01] Hvis CA udsteder et sikkert kryptografisk modul (fx et smartcard), skal deaktivering og reaktivering af det kryptografiske modul ske sikkert.

[KRAV 6.4.1-02] CA skal gennem aftale og/eller tekniske kontroller sikre, at certifikatholders private nøgle er effektivt beskyttet mod uautoriseret anvendelse med brug af aktiveringsdata eller andre mekanismer, der giver tilsvarende eller højere beskyttelse.

[KRAV 6.4.1-03] Hvis certifikatholders private nøgle er placeret på udstyr, hvor andre har adgang, skal aktiveringsdata bestå af mindst 2 forskellige uafhængige faktorer (blandt "noget certifikatindehaver ved", "noget certifikatindehaver har" og "noget certifikatindehaver er") og der skal være effektiv beskyttelse mod udtømmende søgning af gyldige aktiveringsdata.

Note: Biometri ("noget certifikatindehaver er") er primært relevant, hvis certifikatindehaver er identisk med en fysisk person.

[KRAV 6.4.1-04] Hvis certifikatholders private nøgle er placeret på udstyr, hvor kun certifikatindehaver har adgang men uden effektiv beskyttelse mod udtømmende søgning, skal aktiveringsdata have en sikkerhed, der mindst svarer til en adgangskode, som består af mindst 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal og hvor adgangskoden er svær at gætte. Alternativt kan anvendes andre mekanismer, der giver tilsvarende eller højere beskyttelse. Anvendes en adgangskode i miljøer, der effektivt kan spærre for udtømmende søgninger, kan adgangskode dog vælges fra et udfaldsrum på mindst 9.800 mulige koder.

6.4.2 Beskyttelse af aktiveringsdata

[KRAV 6.4.2-01] Hvis CA udsteder et sikkert personaliseret kryptografisk modul (fx et smartcard) med tilhørende brugeraktiveringsdata (fx PIN-kode), skal aktiveringsdataene genereres sikkert og distribueres separat fra det kryptografiske modul.

6.4.3 Andre aspekter ved aktiveringsdata

[KRAV 6.4.3-01] Installation og geninstallation af CA's nøglepar i et sikkert kryptografisk modul skal kræve samtidig kontrol af mindst to betroede medarbejdere.

[KRAV 6.4.3-02] CA skal håndhæve multifaktorautentificering for alle konti, der er i stand til direkte at forårsage certifikatudstedelse.

6.5 IT-sikkerhedskontroller

6.5.1 Særlige tekniske krav til IT-sikkerhed

[KRAV 6.5.1-01] CA's driftssystemer skal implementere en tilstrækkelig IT-sikkerhed til at understøtte adskillelse af betroede roller identificeret i CA's CSP, herunder adskillelse af sikkerhedsadministration og operationelle roller. Særligt skal anvendelse af utility programmer begrænses og kontrolleres til det nødvendige.

[KRAV 6.5.1-02] CA skal implementere dokumenterede processer til release- og ændringshåndtering af software-, hardware- og konfigurationsændringer. CA skal desuden have dokumenterede processer for sikkerhedsopdatering af egenudviklet og standardsoftware og -firmware. Processerne skal inkludere dokumentation for gennemført ændringer.

[KRAV 6.5.1-03] Integriteten i CA's systemer og data skal beskyttes mod vira, malware og uautoriseret software herunder skal CA implementere processer, der sikre, at

- sikkerhedsopdateringer installeres i rimelig tid efter at de bliver tilgængelige,
- sikkerhedsopdateringer ikke installeres, hvis det vurderes, at de introducerer nye uacceptable sårbarheder eller ustabilitet, der ikke opvejer fordelene ved opdateringerne og
- årsager til at undlade eller udskyde en sikkerhedsopdatering er dokumenteret.

[KRAV 6.5.1-04] CA's systemer skal håndhæve adgangskontrol ved forsøg på at tilføje eller slette certifikater og ændre andre tilknyttede oplysninger.

[KRAV 6.5.1-05] CA's systermer skal håndhæve adgangskontrol ved forsøg på at ændre spærringsstatusoplysninger.

[KRAV 6.5.1-06] CA skal implementere kontinuerlige overvågnings- og alarmfaciliteter for at gøre det muligt for CA at detektere, registrere og reagere i tide på uautoriserede og/eller uregelmæssige forsøg på at få adgang til ressourcer.

6.5.2 Klassificering af IT-sikkerhed

N/A

6.6 Tekniske kontroller for livscyklus

6.6.1 Kontroller relateret til systemudvikling

[KRAV 6.6.1-01] CA skal benytte anerkendte systemer og produkter, som er beskyttet mod ændringer. Produkterne skal overholde en tilstrækkelig beskyttelsesprofil i henhold til ISO 15408 eller tilsvarende.

[KRAV 6.6.1-02] CA skal sikre, at der forud for enhver systemudvikling (dvs. egenudvikling eller udvikling hos tredjepart) foreligger en ledelsesgodkendt plan for indbygning af sikkerhed i systemerne. Planen skal indeholde en analyse af, at sikkerhedskrav er opfyldt for at kunne opretholde et tilstrækkeligt sikkerhedsniveau.

6.6.2 Kontroller relateret til informationssikkerhedsledelse

[KRAV 6.6.2-01] CA skal leve op til kravene i standard for informationssikkerhed ISO 27001 og kunne dokumentere efterlevelse fx igennem certificering.

[KRAV 6.6.2-02] CA skal have en ledelsesgodkendt politik for informationssikkerhed, der fastlægger organisationens informationssikkerhedsledelse.

[KRAV 6.6.2-03] Ændringer i politik for informationssikkerhed skal kommunikeres til tredjeparter, hvor det er relevant. Dette kan inkludere abonnenter, overensstemmelsesvurderingsorgan, tilsyn og andre myndigheder.

[KRAV 6.6.2-04] CA's politik for informationssikkerhed skal dokumenteres, implementeres og vedligeholdes herunder sikkerhedskontrol og driftsprocedurer for CA's faciliteter, systemer og informationsaktiver for leverede tjenester.

[KRAV 6.6.2-05] CA skal kommunikere politik for informationssikkerhed til alle medarbejdere herunder medarbejdere hos underleverandører, der udfører arbejde for CA.

Note: Medarbejdere, der er ansat i CA's organisation, men som ikke udfører arbejde relateret til organisationens rolle som CA, er ikke omfattet af ovenstående krav.

[KRAV 6.6.2-06] CA's politik og aktiver for informationssikkerhed skal revideres årligt og ved væsentlige ændringer med henblik på at sikre kontinuitet, egnethed, tilstrækkelighed og effektivitet.

[KRAV 6.6.2-07] Alle ændringer, der kan påvirke det leverede sikkerhedsniveau skal godkendes af CA's ledelse.

[KRAV 6.6.2-08] CA skal gennemgå konfiguration af CA's systemer med faste intervaller og mindst en gang årligt for ændringer, der ikke lever op til CA's politik for informationssikkerhed.

[KRAV 6.6.2-09] CA skal gennemgå konfiguration af CA's systemer for ændringer, der ikke lever op til CA's politik for informationssikkerhed ved væsentlige organisatoriske eller driftsmæssige forandringer.

[KRAV 6.6.2-10] Det maksimale interval mellem to af ovenstående gennemgange skal dokumenteres i CPS.

6.6.3 Kontroller relateret til systemer sikkerhedslivscyklus

[KRAV 6.6.3-01] CA skal implementere en effektiv brugeradministration herunder administration af adgange for operatører, administratorer og systemauditorer.

[KRAV 6.6.3-02] Brugerkonti skal regelmæssigt gennemgås for at sikre at brugere til stadighed kun har nødvendige rettigheder jf. politik for adgangsrettigheder.

[KRAV 6.6.3-03] Adgang til informations- og applikationssystemfunktioner skal begrænses i overensstemmelse med adgangskontrolpolitikken.

[KRAV 6.6.3-04] CA's personale skal identificeres og autentificeres inden der gives adgang til kritiske systemer og applikationer

[KRAV 6.6.3-05] CA's personale skal være ansvarlig for deres aktiviteter fx gennem effektiv hændelseslogning.

[KRAV 6.6.3-06] CA skal overvåge og planlægge kapacitetsbehov for at sikre, at der er tilstrækkelig beregnings- og lagerplads til rådighed for at opretholde en passende service.

6.7 Sikkerhedskontroller for netværk

[KRAV 6.7-01] CA's interne netværk og systemer skal beskyttes mod angreb og uautoriseret adgang, herunder adgang fra certifikatindehavere, certifikatholdere og modtagerparter.

[KRAV 6.7-02] CA skal segmentere sine netværk i zoner i forhold til en risikovurdering under hensyntagen til kritikaliteten af de enkelte delsystemer og den fysiske placering.

[KRAV 6.7-03] CA skal opretholde og beskytte alle CA-systemer som minimum i en sikker zone og skal implementere og konfigurere sikkerhedsprocedurer, som beskytter systemer og kommunikation mellem systemer inden for sikre zoner og særligt sikrede zoner.

[KRAV 6.7-04] CA skal konfigurere alle CA-systemer ved at fjerne eller deaktivere alle konti, applikationer, tjenester, protokoller og porte, der ikke skal anvendes til CA's drift.

[KRAV 6.7-05] Lokale netværkskomponenter (fx routere) skal opbevares i et fysisk og logisk sikkert miljø.

[KRAV 6.7-06] Konfigurationen af lokale netværkskomponenter (fx routere) skal kontrolleres periodisk for overensstemmelse med CA's krav dokumenteret i CSP.

[KRAV 6.7-07] Alle systemer i en zone skal underlægges samme sikkerhedskontroller.

[KRAV 6.7-08] Særligt kritiske systemer herunder rod-CA skal placeres i særligt sikrede zoner.

[KRAV 6.7-09] CA skal kun giver adgang til sikre zoner og særligt sikrede zoner til personale med betroede roller.

[KRAV 6.7-10] CA skal adskille dedikeret netværk til administration af it-systemer og CA driftsnetværk.

[KRAV 6.7-11] CA må ikke anvende systemer, der anvendes til administration af implementeringen af sikkerhedspolitikken til andre formål.

[KRAV 6.7-12] CA skal holde driftssystemer adskilt fra udviklings- og testsystemer.

[KRAV 6.7-13] Firewalls skal være konfigureret til kun at tillade relevante protokoller og kommunikationsparter og kommunikation mellem zoner skal begrænses til det nødvendige. CA skal eksplicit blokere eller deaktivere forbindelser og services, der ikke skal anvendes.

[KRAV 6.7-14] CA skal sikre at kommunikation mellem kritiske systemer udelukkende sker gennem sikrede kanaler, der er fysisk eller logisk adskilt fra andre kommunikationskanaler og giver fortrolighed, integritet og autenticitet mellem systemerne.

[KRAV 6.7-15] CA skal regelmæssigt gennemgå fastlagte netværks- og firewallregler.

[KRAV 6.7-16] CA skal sikre ekstern netværksredundans for systemer med høje krav til tilgængelighed fra eksterne kilder.

[KRAV 6.7-17] Mindst én gang hvert kvartal skal CA udføre sårbarhedsscanning fra eksterne og interne IP-adresser. Scanningerne gennemføres af en part med færdigheder, værktøjer, etisk kodeks og uafhængighed, som er nødvendig for at kunne give en pålidelig rapport. Scanninger skal dokumenteres.

[KRAV 6.7-18] Mindst én gang årligt, efter etablering og ved væsentlige ændringer og opdateringer i infrastrukturen eller i de anvendte applikationer skal CA udføre penetrationstest. Penetrationstesten gennemføres af en part med færdigheder, værktøjer, etisk kodeks og uafhængighed, som er nødvendig for at kunne give en pålidelig rapport. Penetrationstesten skal dokumenteres.

6.8 Tidsstempling

[KRAV 6.8-01] CA skal anvende en pålidelig tidskilde, der skal synkroniseres med UTC mindst en gang dagligt. Kilden til synkronisering skal dokumenteres i den offentlige del af CA's CPS.

[KRAV 6.8-02] Det nøjagtige tidspunkt for væsentlige hændelser i forhold til driftsmiljø, nøglehåndtering og tidssynkronisering skal registreres.

7. Profiler for certifikater, spærrelister og OCSP

7.1 Certifikatprofil

[KRAV 7.1-01] Alle udstedte certifikater skal opfylde kravene i Recommendation ITU-T X.509 eller IETF RFC 5280.

[KRAV 7.1-02] Certifikater skal opfylde krav i ETSI EN 319 412-2.

7.1.1 Versionsnummer

[KRAV 7.1.1-01] Certifikaters versionsnummer skal være angivet og sættes til "v3" (0x2).

7.1.2 Certifikat-extensions

[KRAV 7.1.2-01] Alle certifikater udstedt under denne CP skal indeholde alle relevante qcStatements som beskrevet i ETSI EN 319 412-5 afsnit 5 herunder esi4-qcStatement-4.

[KRAV 7.1.2-02] Alle certifikater udstedt under denne CP skal indeholde en ikke-kritisk extension qcStatements med den i RFC 3739 prædefinerede qcStatement-2, hvor værdier i sematicsInformation skal være

- semanticsIdentifier: id-etsi-qcs-semanticsId-Legal
- nameRegistrationAuthorities: https://uid.gov.dk (af typen URI generalName)

[KRAV 7.1.2-03] Alle certifikater udstedt under denne CP skal indeholde en ikke-kritisk extension authorityKeyIdentifier og skal indeholde identifier for udstedende CA's offentlige nøgle.

[KRAV 7.1.2-04] Alle certifikater udstedt under denne CP skal indeholde præcis én kritisk eller ikke-kritisk extension keyUsage med en af profilerne beskrevet i ETSI EN 319 412-2 afsnit 4.3.2.

[KRAV 7.1.2-05] Hvis et certifikat udstedt under denne CP indeholder extension subjectAlternativeName, skal denne markeres som ikke-kritisk.

[KRAV 7.1.2-06] Hvis et certifikat udstedt efter denne CP indeholder extension issuerAlternativeName, skal denne markeres som ikke-kritisk.

[KRAV 7.1.2-07] Alle certifikater udstedt under denne CP skal indeholde en ikke-kritisk extension cRLDistributionPoints, der indeholder mindst én reference til en offentlig tilgængelig spærreliste og mindst en reference skal være baseret på http-protokollen (http://) IETF RFC 7230-7235.

[KRAV 7.1.2-08] Alle certifikater udstedt under denne CP og CA-certifikater, der ikke er rodcertifikater, skal indeholde en ikke-kritisk extension authorityInformationAccess (AIA). AIA skal indeholde mindst én accessMethod, id-ad-caIssuers, med accessLocation, der henviser til det udstedende CA's gyldige certifikat baseret

på enten http- eller https-protokollen. Desuden skal AIA indeholde mindst én accessMethod, id-ad-ocsp, med accessLocation, der henviser til en offentlig tilgængelig OCSP-responder, der kan give gyldige svar på certifikatets status baseret på enten http- eller https-protokollen og som accepterer ikke-signerede og ikke-autentificerede status-anmodninger.

[KRAV 7.1.2-09] Ingen certifikater udstedt under denne CP må indeholde følgende extensions

- policyMapping
- subjectDirectoryAttributes
- nameConstraints
- policyConstraints
- inhibitAnyPolicy

Note: Se herunder for yderligere krav til extensions.

7.1.3 Algoritme object identifiers

N/A

7.1.4 Navneformer

[KRAV 7.1.4-01] Betegnelsen "Kvalificeret" eller "Qualified" skal indgå i CA-certifikaters commonName.

[KRAV 7.1.4-02] Alle certifikater udstedt under denne CP skal indeholde et subject-felt, der som minimum skal indeholde

- countryName,
- organizationName,
- organizationIdentifier,
- commonName og
- serialNumber.

Dette indhold skal sikre certifikatholders unikke identifikation.

[KRAV 7.1.4-03] countryName skal have værdien "DK".

[KRAV 7.1.4-04] commonName skal indeholde et navn på certifikatholder. Dette kan være i certifikatholders eller CA foretrukne format for navn eller et andet format. Navne med stavemåde andet end defineret af det registrerede navn kan anvendes.

[KRAV 7.1.4-05] serialNumber skal have følgende semantik:

UI:DK-xxxxxxxxxxxxxxxx,

hvor "xxxxxxxxxxxxxxxx" er certifikatholderens UUID registreret i Digitaliseringsstyrelsens UUID-nummereringstjeneste.

[KRAV 7.1.4-06] organizationIdentifier skal have følgende semantik:

NTRDK-xxxxxxxx

hvor "xxxxxxxx" er certifikatindehaverens CVR-nummer.

[KRAV 7.1.4-07] organizationName skal indeholde certifikatindehavers registrerede navn. Det er tilladt at udelade eventuelle virksomhedsformer fx "ApS" og "Fonden" og det er tilladt at anvende registrerede binavne. Endelig er det tilladt at foretage forkortelser af registreret navn, hvis dette ikke med rimelighed giver anledning til misforståelser.

7.1.5 Navnebegrænsninger

[KRAV 7.1.5-01] Der må kun være én instans af commonName, organizationIdentifier, organizationName og countryName i subject-feltet.

7.1.6 Certifikat politik object identifier

[KRAV 7.1.6-01] Alle certifikater udstedt under denne CP skal referere hertil ved at angive den relevante OID fra afsnit 1.2.2 i certificatePolicies extension.

[KRAV 7.1.6-02] OID'er for kvalificerede CP'er udarbejdet af Digitaliseringsstyrelsen må kun refereres i et certifikat efter skriftlig aftale med Digitaliseringsstyrelsen.

[KRAV 7.1.6-03] Alle certifikater udstedt under denne CP skal referere til QCP-l-qscd ved at angive OID:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers (1) qcp-legal-qscd (3)

i certificatePolicies extension.

[KRAV 7.1.6-04] certificatePolicies extension bør ikke markers som kritisk.

7.1.7 Extension for politikanvendelsesbegrænsninger

Se KRAV 7.1.2-08.

7.1.8 Policy qualifiers - syntaks and semantic

N/A

7.1.9 Semantik for processering af kritisk certifikatpolitik extension

N/A

7.2 Spærrelisteprofil

[KRAV 7.2-01] Spærrelister skal følge krav fastlagt i ISO 9594-8, Recommendation ITU-T X.509 eller IETF RFC 5280.

[KRAV 7.2-02] **thisUpdate** og **nextUpdate** skal angives i **UTCTime** format YYMMDDHHMMSSz.

[KRAV 7.2-03] Hvis CA ophører med udstedelse af spærrelister, skal CA udstede en sidste spærreliste, der placeres på rette CRL distributionspunkt med det nextUpdate felt, der indeholder en værdien "99991231235959Z"

7.2.1 Versionsnummer

[KRAV 7.2.1-01] Spærrelistens versionsnummer skal være angivet og sættes til "v2" (0x1).

7.2.2 CRL og CRL entry extensions

[KRAV 7.2.2-01] Hvis CA ikke fjerner spærrede certifikater fra spærreliste, skal spærrelister indeholde extension "expiredCertsOnCRL" som defineret i ISO/IEC 9594-8/Recommendation ITU-T X.509.

[KRAV 7.2.2-02] Hvis CA fjerner spærrede certifikater fra spærreliste, må spærrelister ikke indeholde extension "expiredCertsOnCRL" som defineret i ISO/IEC 9594-8/Recommendation ITU-T X.509.

7.3 OCSP-profile

[KRAV 7.3-01] OCSP skal følge krav fastlagt i IETF RFC 6960.

[KRAV 7.3-02] OCSP skal benytte en profil i overensstemmelse med IETF RFC 5019. Dog kan SHA1 erstattes af mere sikre algoritmer fx SHA256.

[KRAV 7.3-03] Hvis OCSP-responderen modtager en anmodning om status for et certifikat, der ikke er udstedt, må OCSP-responderen ikke svare med en "good"-status som angivet i afsnit 2.2 i IETF RFC 6960.

[KRAV 7.3-04] CA bør overvåge OCSP-anmodninger vedrørende ikke-udstedte certifikater på OCSP-responderen som en del af sine sikkerhedsprocedurer for at kontrollere, om dette er et tegn på et angreb.

7.3.1 Versionsnummer

[KRAV 7.3.1-01] OCSP responder skal understøtte versionsnummer "v1" (0x0).

7.3.2 OCSP extension

[KRAV 7.3.2-01] OCSP-svar bør indeholde archiveCutOff extension som specificeret i IETF RFC 6960 med datoen sat til CA-certifikatets "notBefore"-værdi.

Se i øvrigt KRAV 7.3-02.

8. Overensstemmelsesvurdering og andre vurderinger

8.1 Frekvens og baggrund for systemrevision

[KRAV 8.1-01] Der skal foretages løbende dokumenteret intern systemrevision af CA's samlede system.

[KRAV 8.1-02] Der skal foretages ekstern overensstemmelsesvurdering af CA's samlede system af et overensstemmelsesvurderingsorgan jf. KRAV 8.2-01 mindst én gang årlig.

8.2 Systemrevisors identitet og kvalifikationer

[KRAV 8.2-01] CA skal vælge et eksternt overensstemmelsesvurderingsorgan til varetagelse af systemrevisionen hos CA. Overensstemmelsesvurderingsorganet skal være et overensstemmelsesvurderingsorgan defineret i eIDAS artikel 3 litra 18).

8.3 Systemrevisors relation til den reviderede part

[KRAV 8.3-01] Det valgte overensstemmelsesvurderingsorgan skal samarbejde med den interne revision hos CA'en.

8.4 Emner omfattet af systemrevision

[KRAV 8.4-01] Overensstemmelsesvurderingsorganet skal tilse at CA opfylder krav til kvalificerede tillidstjenesteudbydere jf. eIDAS og krav i denne CP.

[KRAV 8.4-05] CA skal kunne dokumentere opfyldelse af gældende lovgivning. Særligt i forhold til eIDAS, GDPR og Databeskyttelsesloven.

8.5 Krævede handlinger som følge af fundne mangler

[KRAV 8.5-01] I det omfang det valgte overensstemmelsesvurderingsorgan konstaterer væsentlige svagheder eller uregelmæssigheder, skal CA's ledelse behandle sagen på næstkommende ledelsesmøde og inden for rimelig tid.

8.6 Rapportering af resultater

[KRAV 8.6-01] CA og overensstemmelsesvurderingsorgan skal straks oplyse Digitaliseringsstyrelsen om forhold, der er af afgørende betydning for CA's fortsatte virksomhed.

[KRAV 8.6-02] Ved afslutningen af CA's regnskabsår udarbejder det valgte overensstemmelsesvurderingsorgan et protokollat til CA's ledelse.

[KRAV 8.6-03] Protokollatet skal indeholde erklæringer om, hvorvidt

- systemrevisionen er blevet udført i overensstemmelse med god revisionsskik,
- det valgte overensstemmelsesvurderingsorgan opfylder de i lovgivningen indeholdte habilitetsbetingelser,

- det valgte overensstemmelsesvurderingsorgan har fået alle de oplysninger, som det valgte overensstemmelsesvurderingsorgan har anmodet om,
- de anførte systemrevisionsopgaver er udført ifølge denne CP's krav, herunder om der er forhold, som har givet anledning til væsentlige bemærkninger,
- den samlede data-, system- og driftssikkerhed må anses for betryggende.

9. Andre forretningsmæssige og juridiske anliggender

[KRAV 9-01] CA-organisationen skal agere pålidelig og ikke-diskriminerende.

[KRAV 9-02] CA bør gøre sine tjenester tilgængelige for alle, hvis aktiviteter falder inden for det angivne driftsområde, og at de overholder deres forpligtelser som angivet i CA's vilkår og betingelser.

[KRAV 9-03] Tjenester og slutbrugerprodukter leveret af CA skal være tilgængelige for personer med handicap, når det er muligt og der bør tages hensyn til gældende standarder for tilgængelighed som fx ETSI EN 301 549.

[KRAV 9-04] CA skal understøtte en "PKI disclosure statement" jf. ETSI EN 319 411-1. Dette statement skal være struktureret som Annex A i ETSI EN 319 411-1.

9.1 Vederlag

9.1.1 Vederlag for udstedelse og fornyelse af certifikater

N/A

9.1.2 Vederlag for adgang til certifikat

N/A

9.1.3 Vederlag for adgang til spærrings- og statusinformation

N/A

9.1.4 Vederlag for andre services

[KRAV 9.1.4-01] CA skal afholde alle udgifter i forbindelse med systemrevision, herunder tillige systemrevision pålagt af Digitaliseringsstyrelsen som tilsynsmyndighed.

9.1.5 Vilkår for tilbagebetaling

N/A

9.2 Økonomisk ansvar

9.2.1 Forsikringsdækning

[KRAV 9.2.1-01] CA skal opretholde tilstrækkelige finansielle ressourcer og/eller tegne en passende ansvarsforsikring i overensstemmelse med gældende lov, herunder eIDAS, til dækning af forpligtelser som følge af dets aktiviteter.

[KRAV 9.2.1-02] Hvis CA er en privat virksomhed eller en fysisk person, skal CA tegne og opretholde en ansvarsforsikring jf. KRAV 9.2.1-01. Forsikringen skal som minimum have en dækning på kr. 25 millioner pr. år.

9.2.2 Øvrige aktiver

[KRAV 9.2.2-01] CA skal have den finansielle stabilitet og ressourcer, der kræves for at fungere i overensstemmelse med denne politik.

Note: Ovenstående krav skal vurderes i forhold til den kontekst CA opererer, herunder men ikke begrænset til antallet af certifikatindehaver og den finansielle risiko som CA påtager sig i forhold til de udstedte certifikater.

9.2.3 Forsikringsdækning eller garanti for slutbrugere

Se KRAV 9.2.1-01.

9.3 Fortrolighed i forhold til forretningsdata

9.3.1 Omfang af fortrolighed

N/A

9.3.2 Hvad er ikke omfattet af fortrolighed

N/A

9.3.3 Ansvar for beskyttelse af fortrolig information

N/A

9.4 Behandling af personoplysninger

9.4.1 Plan for privatlivsbeskyttelse

[KRAV 9.4.1-01] CA skal træffes passende tekniske og organisatoriske foranstaltninger mod uautoriseret eller ulovlig behandling af personoplysninger og imod utilsigtet tab eller ødelæggelse eller beskadigelse af personoplysninger.

[KRAV 9.4.1-02] Herunder skal registreringsdatas fortrolighed og integritet beskyttes, især når de udveksles med certifikatindehaveren og/eller certifikatholderen eller mellem distribuerede CA systemkomponenter.

[KRAV 9.4.1-03] Det kan være nødvendigt at behandle og herunder opbevare visse data for at opfylde lovmæssige krav samt at understøtte væsentlige forretningsaktiviteter. Disse data skal behandles og opbevares sikkert.

9.4.2 Persondata, der betragtes som fortrolige

N/A

9.4.3 Persondata, der ikke betragtes som fortrolige

N/A

9.4.4 Ansvar for beskyttelse af fortrolige persondata

[KRAV 9.4.4-01] 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'en.

[KRAV 9.4.4-02] CA og RA skal sikre, at statistiske oplysninger om anvendelse af certifikater ikke kan henføres til det enkelte certifikat.

9.4.5 Underretning og samtykke

[KRAV 9.4.5-01] Opbevaringstid af persondata jf. afsnit 5.5.2 skal oplyses som en del af CA's vilkår og betingelser.

9.4.6 Videregivelse i henhold til retslige eller administrative processer

N/A

9.4.7 Andre årsager til videregivelse

N/A

9.5 Rettigheder

[KRAV 9.5-01] Digitaliseringsstyrelsen har alle rettigheder til denne certifikatpolitik. Brug af denne CP's policy-OID i certifikater er kun tilladt efter skriftlig aftale med Digitaliseringsstyrelsen.

9.6 Garantier

9.6.1 CA's garantier

[KRAV 9.6.1-01] CA har det overordnede ansvar for overholdelse af certifikatpolitikken og informationssikkerhedspolitikken uanset anvendelse af eventuelle underleverandører herunder RA. CA skal fastlægge og sikre en effektiv implementering af relevante kontroller hos underleverandører.

[KRAV 9.6.1-02] CA skal levere alle sine tjenester relateret til udstedelse af certifikater i overensstemmelse med CA's CPS.

[KRAV 9.6.1-03] CA skal, i forhold til den der med rimelighed forlader sig på certifikatet, påtage sig erstatningsansvar efter dansk rets almindelige regler.

[KRAV 9.6.1-04] CA skal desuden påtage sig erstatningsansvar for tab hos certifikatindehavere og modtagerparter, 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 7.1,
- manglende spærring af certifikatet, jf. afsnit 4.9,
- manglende eller fejlagtig information om, at certifikatet er spærret, hvilken udløbsdato certifikatet har, eller om certifikatet indeholder formåls- eller beløbsbegrænsninger, jf. afsnit 4.10 og afsnit 7.1, eller
- CA's tilsidesættelse af krav i afsnit 3.2, afsnit 3.3, afsnit 3.4 og afsnit 6.1. medmindre CA kan godtgøre, at CA ikke har handlet uagtsomt eller forsætligt.

9.6.2 RA's garantier

N/A

9.6.3 Certifikatholder/-indehavers garantier

N/A

9.6.4 Modtagerparts garantier

N/A

9.6.5 Andre parters garantier

N/A

9.7 Begrænset hæftelse

N/A

9.8 Ansvarsbegrænsninger

[KRAV 9.8-01] 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.

[KRAV 9.8-02] CA er desuden berettiget til at fraskrive sig ansvar overfor medkontrahenter for tab af den i artikel 13 stk. 2 i eIDAS-forordningen beskrevne art.

9.9 Skadesløsholdelse

N/A

9.10 Varighed og ophør

9.10.1 Varighed

N/A

9.10.2 Opsigelse

N/A

9.10.3 Ophør

N/A

9.11 Personlige meddelelser og kommunikation mellem parterne

[KRAV 9.11-01] CA skal sikre, at der foreligger politikker og procedurer for håndtering af kundehenvendelser eller henvendelser fra modtagerparter.

9.12 Tillæg

9.12.1 Ændringshåndtering

N/A

9.12.2 Notifikationsmekanisme og -varsler

N/A

9.12.3 Situationer, der betinger ændring af OID

N/A

9.13 Tvistligheder

[KRAV 9.13-01] CA skal have politikker og procedurer til løsning af klager og tvister modtaget fra kunder eller andre afhængige parter om leveringen af ydelserne eller andre relaterede forhold og skal være i overensstemmelse med CA's vilkår og betingelser jf. afsnit 2.1.

9.14 Lovvalg

[KRAV 9.14-01] 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.

9.15 Overholdelse af gældende lovgivning

[KRAV 9.15-01] CA og RA skal sikre overensstemmelse med lovgivning, herunder særligt relevante love vedrørende behandling af personoplysninger og eIDAS forordningen.

[KRAV 9.15-02] Særligt skal CA dokumentere hvorledes love vedrørende behandling af personoplysninger efterleves i forbindelse med CA's registreringsproces.

9.16 Diverse bestemmelser

9.16.1 Aftalens elementer

N/A

9.16.2 Overdragelse

N/A

9.16.3 Fortolkning

N/A

9.16.4 Håndhævelse

N/A

9.16.5 Force Majeure

N/A

9.17 Øvrige bestemmelser

[KRAV 9.17-01] CA skal have skriftlig dokumenteret aftale- og kontraktforhold på plads, hvor levering af tjenesteydelser omfatter underleverancer, outsourcing eller andre tredjepartsordninger.

[KRAV 9.17-02] De dele af CA, der beskæftiger sig med certifikatgenerering og spærring, skal være uafhængige af andre organisationer for sine beslutninger vedrørende etablering, levering og vedligeholdelse og lukning af tjenester i overensstemmelse med gældende certifikatpolitik.

[KRAV 9.17-03] Særlig skal CA's øverste ledelse, andre ledende medarbejdere og medarbejdere i betroede roller, der beskæftiger sig med certifikatgenerering og spærring, være fri for ethvert kommercielt, finansielt og andet pres, som kan have negativ indflydelse på tilliden til de leverede ydelser.

[KRAV 9.17-04] De dele af CA's organisation, der beskæftiger sig med certifikatgenerering og -spærring, skal have en dokumenteret struktur, som sikrer driftens upartiskhed.

[KRAV 9.17-05] CA sikre mulighed for, at tredjeparter kan kontrollere og teste alle de certifikattyper, som CA udsteder.

[KRAV 9.17-06] Det skal tydeligt fremgå i certifikater, hvis de er til testformål.

Note: Fx kan det anvendte CA, der udsteder certifikater til testformål indeholde ordet "test" i commonName.

[KRAV 9.17-07] Certifikater til testformål må ikke være udstedt af under samme rod-CA som certifikater til certifikatholdere.

Bilag A

Denne CP's opfyldelse af krav til QCP-l-qscd fastlagt i ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1, ETSI EN 319 412-2 og ETSI EN 319 412-3.

VQ CP	ETSI EN 319 401	ETSI EN 319 411-1	ETSI EN 319 411-2	ETSI EN 319 412-1	ETSI EN 319 412-2	ETSI EN 319 412-3
KRAV 1.3.1-01						
KRAV 1.3.1-02						
KRAV 1.3.1-03		OVR-5.4.1-01				
KRAV 1.3.1-04		OVR-5.4.1-02 OVR-5.4.1-03				
KRAV 1.3.2-01						
KRAV 1.4.1-01						
KRAV 1.4.1-02						
KRAV 1.4.2-02						
KRAV 1.4.2-03						
KRAV 1.4.2-04						
KRAV 1.5.3-01						
KRAV 1.5.3-02						
KRAV 1.5.4-01	REQ-6.1-01 REQ-6.1-03 REQ-6.1-04 REQ-6.1-05					
KRAV 1.5.4-02						
KRAV 1.5.4-03		OVR-5.2-03				

KRAV 1.5.4-04		OVR-5.2-02				
KRAV 1.5.4-05						
KRAV 1.5.4-06		OVR-5.2-04 OVR-5.2-10				
KRAV 1.5.4-07	REQ-6.1-02 REQ-6.1-06 REQ-6.1-07					
KRAV 1.5.4-08	REQ-6.1-08 REQ-6.1-09					
KRAV 2.1-01						
KRAV 2.1-02	REQ-6.1-02 REQ-6.1-10 REQ-6.2-06	OVR-5.2-05				
KRAV 2.1-03	REQ-6.2-01 REQ-6.2-02					
KRAV 2.1-04		OVR-6.9.4-02				
KRAV 2.1-05						
KRAV 2.1-06	REQ-6.2-04					
KRAV 2.1-07	REQ-6.2-05	DIS-6.1-05 DIS-6.1-07				
KRAV 2.1-08	REQ-6.2-06					
KRAV 2.2-01		DIS-6.1-01 DIS-6.1-03				
KRAV 2.2-02		DIS-6.1-02				

KRAV 2.2-03						
KRAV 2.2-04						
KRAV 2.2-05						
KRAV 2.3-01	REQ-6.1-10					
KRAV 2.4-01		DIS-6.1-09				
KRAV 3.1.1-01						
KRAV 3.1.1-02						
KRAV 3.1.2-01						
KRAV 3.1.2-02						
KRAV 3.1.2-03						
KRAV 3.1.5-01						
KRAV 3.2-01		REG-6.2.2-01				
KRAV 3.2-02		REG-6.2.2-02				
KRAV 3.2-03		REG-6.2.2-18				
KRAV 3.2-04		REG-6.2.2-23				
KRAV 3.2.05		REG-6.2.2-24				
KRAV 3.2.1-01						
KRAV 3.2.1-02						
KRAV 3.2.2-01		REG-6.2.2-10 REG-6.2.2-12				
KRAV 3.2.2-02						
KRAV 3.2.2-03						
KRAV 3.2.2-04		REG-6.2.2-13 REG-6.2.2-15				

KRAV 3.2.2-05		REG-6.2.2-16 REG-6.2.2-17				
KRAV 3.2.4-01		REG-6.2.2-21				
KRAV 3.3-01		REG-6.2.3-01				
KRAV 3.3-02		REG-6.2.3-08				
KRAV 3.3-03		REG-6.2.3-09				
KRAV 3.3.1-01		REG-6.2.3-02				
KRAV 3.3.2-01		REG-6.2.3-02				
KRAV 3.4-01		REV-6.2.4-09				
KRAV 3.4-02		REV-6.2.4-01				
KRAV 4.1.1-01						
KRAV 4.1.2-01		REG-6.3.2-01				
KRAV 4.1.2-02		REG-6.3.2-02				
KRAV 4.1.2-03	REQ-6.2-01 REQ-6.2-03					
KRAV 4.1.2-04		REG-6.3.1-01				
KRAV 4.2.1-01						
KRAV 4.2.2-01						
KRAV 4.2.3-01						
KRAV 4.3.1-01		GEN-6.3.3-01				
KRAV 4.3.1-02		GEN-6.3.3-02				
KRAV 4.3.1-03		GEN-6.3.3-03				
KRAV 4.3.1-04		GEN-6.3.3-04				
KRAV 4.3.1-05		GEN-6.3.3-05				

		GEN-6.3.3-06				
KRAV 4.3.1-06		GEN-6.3.3-07				
KRAV 4.3.1-07		SDP-6.3.3-08				
KRAV 4.3.1-08		GEN-6.3.3-10				
KRAV 4.3.1-10		GEN-6.3.3-12				
KRAV 4.3.2-01						
KRAV 4.4.1-01		OVR-6.3.4-01				
KRAV 4.4.1-02		REG-6.3.4-02				
KRAV 4.4.1-04		OVR-6.3.4-04				
KRAV 4.4.1-05		OVR-6.3.4-05				
KRAV 4.4.1-06		OVR-6.3.4-06				
KRAV 4.4.1-08		REG-6.3.4-08				
KRAV 4.4.1-09		REG-6.3.4-12 REG-6.3.4-13				
KRAV 4.4.1-12		REG-6.3.4-16				
KRAV 4.4.1-13		REG-6.3.4-17				
KRAV 4.4.2-01						
KRAV 4.4.3-01						
KRAV 4.5.1-01		OVR-6.3.5-01				
KRAV 4.5.1-03			SDP-6.3.5-02			
KRAV 4.5.1-04			SDP-6.3.5-03			
KRAV 4.5.1-05			SDP-6.3.5-05			
KRAV 4.5.1-06			SDP-6.3.5-06			
KRAV 4.5.1-07			OVR-6.3.5-07			

			SDP-6.3.5-08 SDP-6.3.5-10			
KRAV 4.5.2-01		OVR-6.3.5-03				
KRAV 4.6.2-01						
KRAV 4.6.3-01		REG-6.3.6-01				
KRAV 4.6.3-02		REG-6.3.6-02				
KRAV 4.6.3-03		REG-6.3.6-08				
KRAV 4.6.3-04		REG-6.3.6-09				
KRAV 4.6.3-05		GEN-6.3.6-10				
KRAV 4.6.4-01						
KRAV 4.6.5-01						
KRAV 4.6.6-01						
KRAV 4.6.7-01						
KRAV 4.7.1-01						
KRAV 4.7.1-02						
KRAV 4.7.1-03						
KRAV 4.7.1-04						
KRAV 4.7.2-01						
KRAV 4.7.3-01						
KRAV 4.7.3-02						
KRAV 4.7.4-01						
KRAV 4.7.5-01						
KRAV 4.7.6-01						
KRAV 4.7.7-01						

KRAV 4.8.1-01		REG-6.3.8-01				
KRAV 4.8.2-01						
KRAV 4.8.3-01		REG-6.3.8-02				
KRAV 4.8.4-01						
KRAV 4.8.5-01						
KRAV 4.8.6-01						
KRAV 4.8.7-01						
KRAV 4.9.1-01		REV-6.2.4-03				
KRAV 4.9.1-02						
KRAV 4.9.1-03						
KRAV 4.9.1-04		REV-6.3.9-03				
KRAV 4.9.2-01						
KRAV 4.9.3-01		REV-6.3.9-01				
KRAV 4.9.3-02						
KRAV 4.9.3-03		REV-6.3.9-02				
KRAV 4.9.3-04						
KRAV 4.9.3-05						
KRAV 4.9.4-01						
KRAV 4.9.5-01		REV-6.2.4-08				
KRAV 4.9.5-02						
KRAV 4.9.5-03		REV-6.2.4-05				
KRAV 4.9.5-04		REV-6.2.4-06				
KRAV 4.9.5-05		REV-6.2.4-07				
KRAV 4.9.7-01		CSS-6.3.9-04				

KRAV 4.9.7-02		CSS-6.3.9-05				
KRAV 4.9.7-03		CSS-6.3.9-11				
KRAV 4.9.7-04		CSS-6.3.9-12				
KRAV 4.9.7-05		CSS-6.3.9-06				
KRAV 4.9.7-06		CSS-6.3.9-13				
KRAV 4.9.8-01						
KRAV 4.9.9-01						
KRAV 4.9.11-01						
KRAV 4.9.13-01						
KRAV 4.10-01		CSS-6.3.10-01				
KRAV 4.10-02			CSS-6.3.10-12			
KRAV 4.10.1-01			CSS-6.3.10-02			
KRAV 4.10.1-02		CSS-6.3.10-03				
KRAV 4.10.1-03		CSS-6.3.10-05				
KRAV 4.10.1-04		CSS-6.3.10-04	CSS-6.3.10-03			
KRAV 4.10.1-05			CSS-6.3.10-08			
KRAV 4.10.1-06			CSS-6.3.10-09			
KRAV 4.10.1-07		CSS-6.3.10-07				
KRAV 4.10.1-08						
KRAV 4.10.1-09		CSS-6.3.10-08 CSS-6.3.10-09				
KRAV 4.10.1-10						
KRAV 4.10.1-11						
KRAV 4.10.1-12						

KRAV 4.10.1-13						
KRAV 4.10.1-14			CSS-6.3.10-11			
KRAV 4.10.2-01		CSS-6.3.10-02				
KRAV 4.10.2-02						
KRAV 4.10.2-03		CSS-6.3.10-10				
KRAV 4.12.1-01						
KRAV 5-01	REQ-7.13-01					
KRAV 5-02	REQ-5-01					
KRAV 5-03	REQ-5-02					
KRAV 5-04	REQ-5-03					
KRAV 5-05	REQ-5-04					
KRAV 5-06	REQ-5-05					
KRAV 5-07	REQ-7.3.1-01 REQ-7.3.1-02					
KRAV 5-08	REQ-7.4-01					
KRAV 5.1-01	REQ-7.6-01					
KRAV 5.1-02	REQ-7.6-03 REQ-7.6-04					
KRAV 5.1-03		OVR-6.4.2-07				
KRAV 5.1-04		OVR-6.4.2-08				
KRAV 5.1-05		OVR-6.4.2-09				
KRAV 5.1.1-01						
KRAV 5.1.1-02	REQ-7.6-02					
KRAV 5.1.1-03	REQ-7.8-02					

KRAV 5.1.1-04						
KRAV 5.1.2-01						
KRAV 5.1.2-02	REQ-7.6-05					
KRAV 5.1.2-03		OVR-6.4.2-05				
KRAV 5.1.2-04		OVR-6.4.2-02				
KRAV 5.1.2-05	REQ-7.8-04					
KRAV 5.1.2-06						
KRAV 5.1.2-07		OVR-6.4.2-10				
KRAV 5.1.2-08		OVR-6.4.2-06				
KRAV 5.1.2-09						
KRAV 5.1.2-10						
KRAV 5.1.2-11		OVR-6.4.2-03				
KRAV 5.1.2-12		OVR-6.4.2-11				
KRAV 5.1.2-13		OVR-6.4.2-04				
KRAV 5.1.6-01	REQ-7.3.2-01 REQ-7.4-10 REQ-7.7-06	OVR-6.4.3-01				
KRAV 5.1.6-02	REQ-7.7-07					
KRAV 5.1.7-01	REQ-7.3.2-01					
KRAV 5.1.8-01						
KRAV 5.2.1-01	REQ-7.2-07 REQ-7.2-08					
KRAV 5.2.1-02	REQ-7.7-08					
KRAV 5.2.1-03	REQ-7.2-14					

KRAV 5.2.1-04	REQ-7.2-15	OVR-6.4.4-02				
KRAV 5.2.1-05	REQ-7.1.2-01					
KRAV 5.2.2-01		GEN-6.4.3-02				
KRAV 5.2.3-01	REQ-7.2-16					
KRAV 5.2.3-02	REQ-7.2-09					
KRAV 5.2.3-03	REQ-7.2-10					
KRAV 5.2.3-04	REQ-7.2-11					
KRAV 5.2.3-05	REQ-7.2-17					
KRAV 5.2.4-01						
KRAV 5.3-01	REQ-7.2-01					
KRAV 5.3.1-01	REQ-7.2-02					
KRAV 5.3.1-02	REQ-7.2-13					
KRAV 5.3.1-03	REQ-7.2-06					
KRAV 5.3.2-01	REQ-7.4-08					
KRAV 5.3.2-02						
KRAV 5.3.3.-01	REQ-7.2-03					
KRAV 5.3.3.-02						
KRAV 5.3.4-01	REQ-7.2-04					
KRAV 5.3.6-01	REQ-7.2-12					
KRAV 5.3.6-02	REQ-7.2-05					
KRAV 5.3.7-01						
KRAV 5.4.1-01		OVR-6.4.5-02				
KRAV 5.4.1-02		REG-6.4.5-03				
KRAV 5.4.1-03		GEN-6.4.5-06				

KRAV 5.4.1-04		GEN-6.4.5-07	OVR-6.4.5-02			
KRAV 5.4.1-05		GEN-6.4.5-08				
KRAV 5.4.1-06		REV-6.4.5-09				
KRAV 5.4.1-07						
KRAV 5.4.1-08			SDP-6.4.5-06			
KRAV 5.4.2-01						
KRAV 5.4.3-01		OVR-6.4.6-01				
KRAV 5.4.3-02						
KRAV 5.4.4-01	REQ-7.10-02 REQ-7.10-08					
KRAV 5.4.4-02		REG-6.4.5-05				
KRAV 5.4.4-03			OVR-6.4.5-03			
KRAV 5.4.4-04			OVR-6.4.5-04 OVR-6.4.5-05			
KRAV 5.4.5-01						
KRAV 5.5-01						
KRAV 5.5.-02						
KRAV 5.5.1-01	REQ-7.10-01					
KRAV 5.5.1-02		REG-6.4.5-04				
KRAV 5.5.1-03						
KRAV 5.5.1-04						
KRAV 5.5.2-01	REQ-7.10-07					
KRAV 5.5.2-02		OVR-6.4.6-01				

KRAV 5.5.3-01	REQ-7.10-02					
KRAV 5.5.3-02	REQ-7.10-03					
KRAV 5.5.4-01		OVR-6.4.8-03				
KRAV 5.5.4-02		OVR-6.4.8-04				
KRAV 5.5.4-03		OVR-6.4.8-02				
KRAV 5.5.4-04		OVR-6.4.8-05				
KRAV 5.5.4-05		OVR-6.4.8-06				
KRAV 5.5.4-06		OVR-6.4.8-07				
KRAV 5.5.7-01	REQ-7.10-04					
KRAV 5.6-01						
KRAV 5.7-01						
KRAV 5.7.1-01	REQ-7.9-01					
KRAV 5.7.1-02	REQ-7.9-02					
KRAV 5.7.1-03	REQ-7.9-03					
KRAV 5.7.1-04	REQ-7.9-04					
KRAV 5.7.1-05	REQ-7.9-05					
KRAV 5.7.1-06	REQ-7.9-06					
KRAV 5.7.1-07	REQ-7.9-07					
KRAV 5.7.1-08	REQ-7.9-08					
KRAV 5.7.1-09	REQ-7.9-09					
KRAV 5.7.1-10	REQ-7.9-10					
KRAV 5.7.1-11	REQ-7.9-11					
KRAV 5.7.1-12	REQ-7.9-12					
KRAV 5.7.2-01						

KRAV 5.7.2-02						
KRAV 5.7.3-01		OVR-6.4.8-08				
KRAV 5.7.3-02		OVR-6.4.8-09				
KRAV 5.7.3-03		OVR-6.4.8-11 OVR-6.4.8-12 OVR-6.4.8-13 OVR-6.4.8-14				
KRAV 5.7.3-04		OVR-6.4.8-15				
KRAV 5.7.3-05		OVR-6.4.8-16				
KRAV 5.7.3-06						
KRAV 5.7.4-01	REQ-7.11-01					
KRAV 5.7.4-02	REQ-7.11-02					
KRAV 5.7.4-03		OVR-6.4.8-10				
KRAV 5.8-01	REQ-7.12-02					
KRAV 5.8-02	REQ-6.1-11 REQ-7.12-10	OVR-6.4.9-03				
KRAV 5.8-03	REQ-7.12-03 REQ-7.12-04					
KRAV 5.8-04						
KRAV 5.8-05	REQ-7.12-01 REQ-7.12-11					
KRAV 5.8-06	REQ-7.12-06	OVR-6.4.9-02				
KRAV 5.8-07	REQ-7.12-05					
KRAV 5.8-08	REQ-7.12-07					

KRAV 5.8-09	REQ-7.12-08					
KRAV 5.8-10		OVR-6.4.9-04				
KRAV 5.8-11	REQ-7.12-09					
KRAV 6.1.1-01						
KRAV 6.1.1-02	REQ-7.5-01					
KRAV 6.1.1-03						
KRAV 6.1.1-04		GEN-6.5.1-02				
KRAV 6.1.1-05		GEN-6.5.1-03 GEN-6.5.1-04 GEN-6.5.1-05 GEN-6.5.1-06 GEN-6.5.1-07				
KRAV 6.1.1-06		GEN-6.5.1-08				
KRAV 6.1.1-07		GEN-6.5.1-09				
KRAV 6.1.1-08		GEN-6.5.1-10				
KRAV 6.1.1-09		GEN-6.5.1-11				
KRAV 6.1.1-10		GEN-6.5.1-12				
KRAV 6.1.1-11		GEN-6.5.1-13				
KRAV 6.1.1-12		GEN-6.5.1-14				
KRAV 6.1.1-13						
KRAV 6.1.1-14		SDP-6.5.1-17				
KRAV 6.1.1-15		SDP-6.5.1-18				
KRAV 6.1.1-16		SDP-6.5.1-19				
KRAV 6.1.1-17			SDP-6.5.1-02			

KRAV 6.1.1-18			SDP-6.5.1-03			
KRAV 6.1.1-19			SDP-6.5.1-04			
KRAV 6.1.1-20			SDP-6.5.1-05			
KRAV 6.1.1-21			SDP-6.5.1-06			
KRAV 6.1.2-01		SDP-6.5.1-20				
KRAV 6.1.2-02		SDP-6.5.1-21				
KRAV 6.1.2-03		SDP-6.5.1-22				
KRAV 6.1.2-04		SDP-6.5.1-23				
KRAV 6.1.2-05		SDP-6.5.1-24				
KRAV 6.1.2-06		SDP-6.5.1-25				
KRAV 6.1.3-01						
KRAV 6.1.4-01		DIS-6.5.1-16				
KRAV 6.1.4-02						
KRAV 6.1.7-01						
KRAV 6.2-01						
KRAV 6.2.1-01		OVR-6.5.2-01 OVR-6.5.2-03				
KRAV 6.2.1-02		OVR-6.5.2-02				
KRAV 6.2.1-03						
KRAV 6.2.1-04						
KRAV 6.2.1-05						
KRAV 6.2.1-06						
KRAV 6.2.1-07		GEN-6.5.2-04				
KRAV 6.2.4-01		GEN-6.5.2-06				

KRAV 6.2.4-02		GEN-6.5.2-07				
KRAV 6.2.4-03		GEN-6.5.2-08				
KRAV 6.2.5-01		GEN-6.5.2-05				
KRAV 6.2.6-01						
KRAV 6.2.6-02						
KRAV 6.2.7-01		GEN-6.5.2-09				
KRAV 6.2.7-02		OVR-6.5.2-10				
KRAV 6.2.7-03		OVR-6.5.2-11				
KRAV 6.2.7-04		OVR-6.5.2-12				
KRAV 6.2.8-01						
KRAV 6.2.10-01		GEN-6.5.2-13				
KRAV 6.2.11-01			SDP-6.5.1-07			
KRAV 6.3-01		OVR-6.5.3-01 OVR-6.5.3-02 GEN-6.5.3-03 GEN-6.5.3-04 GEN-6.5.3-05 GEN-6.5.3-06 GEN-6.5.3-07				
KRAV 6.3-02			CSS-6.3.10-13			
KRAV 6.4.1-01		SDP-6.5.4-02				
KRAV 6.4.1-02						
KRAV 6.4.1-03						
KRAV 6.4.1-04						

KRAV 6.4.2-01		SDP-6.5.4-03				
KRAV 6.4.3-01		GEN-6.5.4-01				
KRAV 6.4.3-02		GEN-6.5.5-04				
KRAV 6.5.1-01	REQ-7.4-07					
KRAV 6.5.1-02	REQ-7.7-03 REQ-7.7-04					
KRAV 6.5.1-03	REQ-7.7-05 REQ-7.7-09					
KRAV 6.5.1-04		DIS-6.5.5-05				
KRAV 6.5.1-05		CSS-6.5.5-06				
KRAV 6.5.1-06		OVR-6.5.5-07				
KRAV 6.6.1-01	REQ-7.7-01					
KRAV 6.6.1-02	REQ-7.7-02					
KRAV 6.6.2-01						
KRAV 6.6.2-02	REQ-6.3-01					
KRAV 6.6.2-03	REQ-6.3-02					
KRAV 6.6.2-04	REQ-6.3-03					
KRAV 6.6.2-05	REQ-6.3-04					
KRAV 6.6.2-06	REQ-6.3-07					
KRAV 6.6.2-07	REQ-6.3-08					
KRAV 6.6.2-08	REQ-6.3-09					
KRAV 6.6.2-09						
KRAV 6.6.2-10	REQ-6.3-10					
KRAV 6.6.3-01	REQ-7.4-04					

KRAV 6.6.3-02	REQ-7.4-05					
KRAV 6.6.3-03	REQ-7.4-06					
KRAV 6.6.3-04	REQ-7.4-08					
KRAV 6.6.3-05	REQ-7.4-09					
KRAV 6.6.3-06		OVR-6.5.6-02				
KRAV 6.7-01	REQ-7.4-02 REQ-7.8-01					
KRAV 6.7-02	REQ-7.8-02					
KRAV 6.7-03		OVR-6.5.7-02				
KRAV 6.7-04		OVR-6.5.7-03				
KRAV 6.7-05		GEN-6.5.5-02				
KRAV 6.7-06		GEN-6.5.5-03				
KRAV 6.7-07	REQ-7.8-03					
KRAV 6.7-08	REQ-7.8-07	OVR-6.5.7-05				
KRAV 6.7-09		OVR-6.5.7-04				
KRAV 6.7-10	REQ-7.8-08					
KRAV 6.7-11	REQ-7.8-09					
KRAV 6.7-12	REQ-7.8-10					
KRAV 6.7-13	REQ-7.4-03 REQ-7.8-04 REQ-7.8-05					
KRAV 6.7-14	REQ-7.8-11					
KRAV 6.7-15	REQ-7.8-06					

KRAV 6.7-16	REQ-7.8-12					
KRAV 6.7-17	REQ-7.8-13					
KRAV 6.7-18	REQ-7.8-14 REQ-7.8-15					
KRAV 6.8-01	REQ-7.10-06					
KRAV 6.8-02	REQ-7.10-05					
KRAV 7.1-01		GEN-6.6.1-01				
KRAV 7.1-02		GEN-6.6.1-02				
KRAV 7.1.1-01						
KRAV 7.1.2-01			GEN-6.6.1-02 GEN-6.6.1-03			
KRAV 7.1.2-02				Afsnit 5.1.4		
KRAV 7.1.2-03					Afsnit 4.3.1	
KRAV 7.1.2-04					Afsnit 4.3.2	
KRAV 7.1.2-05					Afsnit 4.3.5	
KRAV 7.1.2-06					Afsnit 4.3.6	
KRAV 7.1.2-07					Afsnit 4.3.11	
KRAV 7.1.2-08					Afsnit 4.4.1	
KRAV 7.1.2-09					Afsnit 4.3.4 + 4.3.7 + 4.3.8 + 4.3.9 + 4.3.12	
KRAV 7.1.4-01						
KRAV 7.1.4-02						Afsnit 4.2.1
KRAV 7.1.4-03						Afsnit 4.2.1
KRAV 7.1.4-04						Afsnit 4.2.1

KRAV 7.1.4-05				Afsnit 5.1.3		
KRAV 7.1.4-06				Afsnit 5.1.4	Afsnit 4.2.4	Afsnit 4.2.1
KRAV 7.1.4-07						Afsnit 4.2.1
KRAV 7.1.5-01						Afsnit 4.2.1
KRAV 7.1.6-01						
KRAV 7.1.6-02						
KRAV 7.1.6-03						
KRAV 7.1.6-04					Afsnit 4.3.3	
KRAV 7.2-01		OVR-6.6.2-01				
KRAV 7.2-02						
KRAV 7.2-03			CSS-6.3.20-07			
KRAV 7.2.1-01						
KRAV 7.2.2-01			CSS-6.3.10-05			
KRAV 7.2.2-02			CSS-6.3.10-06			
KRAV 7.3-01		OVR-6.6.3-01				
KRAV 7.3-02						
KRAV 7.3-03		OVR-6.6.3-02				
KRAV 7.3-04		OVR-6.6.3-03				
KRAV 7.3.1-01						
KRAV 7.3.2-01			CSS-6.3.10-10			
KRAV 8.1-01						
KRAV 8.1-02						
KRAV 8.2-01						
KRAV 8.3-01						

KRAV 8.4-01						
KRAV 8.4-05	REQ-7.13-02					
KRAV 8.5-01						
KRAV 8.6-01						
KRAV 8.6-02						
KRAV 8.6-03						
KRAV 9-01	REQ-7.1.1-01 REQ-7.1.1-02					
KRAV 9-02	REQ-7.1.1-03					
KRAV 9-03	REQ-7.13-03 REQ-7.13-04					
KRAV 9-04			OVR-6.9.4-03 OVR-6.9.4-04			
KRAV 9.1.4-01						
KRAV 9.2.1-01	REQ-7.1.1-04					
KRAV 9.2.1-02						
KRAV 9.2.2-01	REQ-7.1.1-05					
KRAV 9.4.1-01	REQ-7.13-05					
KRAV 9.4.1-02		OVR-6.8.4-02				
KRAV 9.4.1-03		OVR-6.8.4-03				
KRAV 9.4.4-01						
KRAV 9.4.4-02						
KRAV 9.4.5-01						
KRAV 9.5-01						

KRAV 9.6.1-01	REQ-6.3-05 REQ-6.3-06					
KRAV 9.6.1-02		OVR-6.8.6-02				
KRAV 9.6.1-03						
KRAV 9.6.1-04						
KRAV 9.8-01						
KRAV 9.8-02						
KRAV 9.11-01						
KRAV 9.13-01	REQ-7.1.1-06	OVR-6.8.13-01				
KRAV 9.14-01						
KRAV 9.15-01						
KRAV 9.15-02		REG-6.2.2-22				
KRAV 9.17-01	REQ-7.1.1-07					
KRAV 9.17-02		OVR-6.9.1-02				
KRAV 9.17-03		OVR-6.9.1-03				
KRAV 9.17-04		OVR-6.9.1-04				
KRAV 9.17-05		OVR-6.9.2-01				
KRAV 9.17-06		OVR-6.9.2-02				
KRAV 9.17-07						