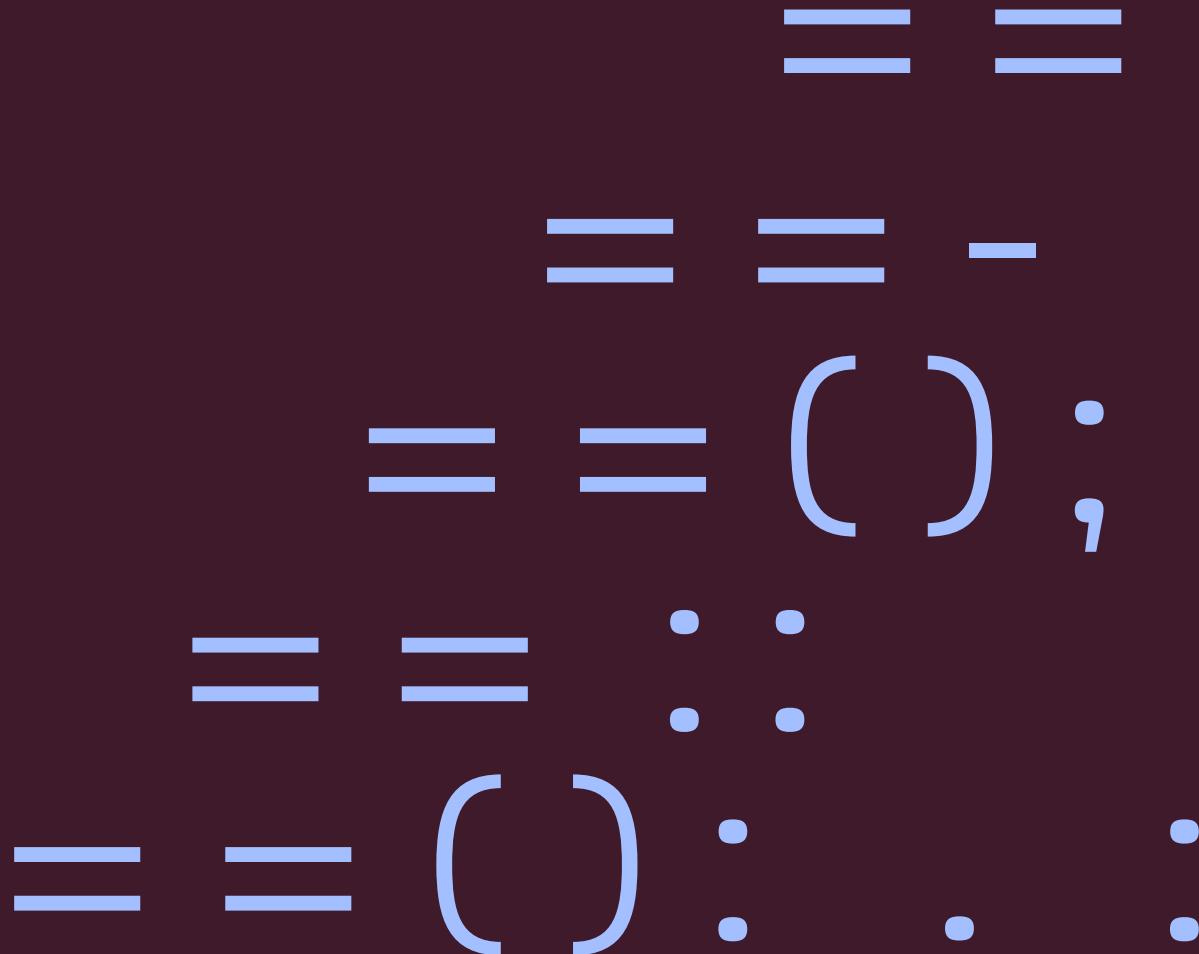


Version 8 – Draft Høringsversion

# Samlet offentlig certifikatpolitik for OCES og kvalificerede certifikater (Combined Public Certificate Policy for OCES and Qualified Certificates)



# Content

<b>1. Introduktion (Introduction) .....</b>	<b>11</b>
1.1 Overview .....	13
1.2 Document Name and Identification .....	14
1.2.1 Naming .....	14
1.2.2 Identification .....	14
1.3 PKI Participants .....	15
1.3.1 Certification Authorities.....	15
1.3.2 Registration Authorities.....	15
1.3.3 Subscribers .....	15
1.3.4 Relying Parties .....	16
1.3.5 Other Participants.....	16
1.4 Certificate Usage .....	16
1.4.1 Appropriate Certificate Uses .....	16
1.4.2 Prohibited Certificate Uses .....	16
1.5 Policy Administration .....	16
1.5.1 Organization Administering the Document.....	16
1.5.2 Contact Person .....	16
1.5.3 Person Determining CPS Suitability for the Policy.....	17
1.5.4 CPS Approval Procedures .....	17
1.6 Definitions and Acronyms .....	17
1.6.1 Definitions .....	17
1.6.2 Abbreviations .....	19
<b>2. Publication and Repository Responsibilities.....</b>	<b>21</b>
2.1 Repositories .....	21
2.2 Publication of Certification Information .....	21
2.3 Time or Frequency of Publication .....	21
2.4 Access Controls on Repositories .....	21
<b>3. Identification and Authentication .....</b>	<b>22</b>

3.1 Naming .....	22
3.1.1 Type of Names .....	22
3.1.2 Need for Names to be Meaningful .....	22
3.1.3 Anonymity or Pseudonymity of Subscribers.....	22
3.1.4 Rules for Interpreting Various Name Forms .....	22
3.1.5 Uniqueness of Names .....	22
3.1.6 Recognition, Authentication, and Role of Trademarks .....	23
3.2 Initial Identity Validation.....	23
3.2.1 Method to Prove Possession of Private Key .....	23
3.2.2 Authentication of Organization Identity.....	23
3.2.3 Authentication of Individual Identity.....	23
3.2.4 Non-Verified Subscriber Information.....	24
3.2.5 Validation of Authority .....	24
3.2.6 Criteria for Interoperation .....	24
3.3 Identification and Authentication for Re-Key Requests.....	24
3.3.1 Identification and Authentication for Routine Re-Key.....	24
3.3.2 Identification and Authentication for Re-Key After Revocation .....	24
3.4 Identification and Authentication for Revocation Request .....	24
<b>4. Certificate Life-Cycle Operational Requirements.....</b>	<b>25</b>
4.1 Certificate Application .....	25
4.1.1 Who Can Submit a Certificate Application .....	25
4.1.2 Enrollment Process and Responsibilities.....	25
4.2 Certificate Application Processing.....	25
4.2.1 Performing Identification and Authentication Functions .....	25
4.2.2 Approval or Rejection of Certificate Applications .....	25
4.2.3 Time to Process Certificate .....	25
4.3 Certificate Issuance.....	25
4.3.1 CA Actions During Certificate Issuance .....	25
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate .....	26
4.4 Certificate Acceptance .....	26
4.4.1 Conduct Constituting Certificate Acceptance .....	26
4.4.2 Publication of the Certificate by the CA.....	26

4.4.3 Notification of Certificate Issuance by the CA to Other Entities .....	26
<b>4.5 Key Pair and Certificate Usage .....</b>	<b>27</b>
4.5.1 Subscriber Private Key and Certificate Usage.....	27
4.5.2 Relying Party Public Key and Certificate Usage.....	27
<b>4.6 Certificate Renewal .....</b>	<b>27</b>
4.6.1 Circumstances for Certificate Renewal.....	27
4.6.2 Who May Request Renewal .....	27
4.6.3 Processing Certificate Renewal Requests .....	27
4.6.4 Notification of New Certificate Issuance to Subscriber .....	27
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate .....	28
4.6.6 Publication of the Renewal Certificate by the CA .....	28
4.6.7 Notification of Certificate Issuance by the CA to Other Entities .....	28
<b>4.7 Certificate Re-Key .....</b>	<b>28</b>
4.7.1 Circumstances for Certificate Re-Key .....	28
4.7.2 Who May Request Certification of a New Public Key .....	28
4.7.3 Processing Certificate Re-Keying Requests.....	28
4.7.4 Notification of New Certificate Issuance to Subscriber .....	28
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate.....	28
4.7.6 Publication of the Re-Keyed Certificate by the CA.....	28
4.7.7 Notification of Certificate Issuance by the CA to Other Entities .....	28
<b>4.8 Certificate Modification .....</b>	<b>28</b>
4.8.1 Circumstances for Certificate Modification .....	28
4.8.2 Who May Request Certificate Modification .....	29
4.8.3 Processing Certificate Modification Requests.....	29
4.8.4 Notification of New Certificate Issuance to Subscriber .....	29
4.8.5 Conduct Constituting Acceptance of Modified Certificate .....	29
4.8.6 Publication of the Modified Certificate by the CA.....	29
4.8.7 Notification of Certificate Issuance by the CA to Other Entities .....	29
<b>4.9 Certificate Revocation and Suspension.....</b>	<b>29</b>
4.9.1 Circumstances for Revocation.....	29
4.9.2 Who Can Request Revocation .....	29
4.9.3 Procedure for Revocation Request .....	30
4.9.4 Revocation Request Grace Period.....	30

4.9.5 Time Within Which CA Must Process the Revocation Request .....	30
4.9.6 Revocation Checking Requirements for Relying Parties.....	30
4.9.7 CRL Issuance Frequency.....	30
4.9.8 Maximum Latency for CRLs .....	30
4.9.9 On-Line Revocation/Status Checking Availability.....	30
4.9.10 On-Line Revocation Checking Requirements .....	31
4.9.11 Other Forms of Revocation Advertisements Available.....	31
4.9.12 Special Requirements related to Key Compromise .....	31
4.9.13 Circumstances for Suspension .....	31
4.9.14 Who Can Request Suspension .....	31
4.9.15 Procedure for Suspension Request .....	31
4.9.16 Limits on Suspension Period .....	31
<b>4.10 Certificate Status Services .....</b>	<b>31</b>
4.10.1 Operational Characteristics .....	31
4.10.2 Service Availability.....	31
4.10.3 Operational Features .....	31
<b>4.11 End of Subscription.....</b>	<b>32</b>
<b>4.12 Key Escrow and Recovery.....</b>	<b>32</b>
4.12.1 Key Escrow and Recovery Policy and Practices .....	32
4.12.2 Session Key Encapsulation and Recovery Policy and Practices .....	32
<b>5. Facility, Management, and Operational Controls ....</b>	<b>33</b>
<b>5.1 Physical Controls .....</b>	<b>33</b>
5.1.1 Site Location and Construction .....	33
5.1.2 Physical Access.....	33
5.1.3 Power and Air Conditioning.....	33
5.1.4 Water Exposures.....	33
5.1.5 Fire Prevention and Protection .....	33
5.1.6 Media Storage.....	33
5.1.7 Waste Disposal .....	33
5.1.8 Off-Site Backup .....	33
<b>5.2 Procedural Controls .....</b>	<b>34</b>
5.2.1 Trusted Roles .....	34

5.2.2 Number of Persons Required per Task.....	34
5.2.3 Identification and Authentication for Each Role.....	34
5.2.4 Roles Requiring Separation of Duties .....	34
<b>5.3 Personnel Controls .....</b>	<b>34</b>
5.3.1 Qualifications, Experience, and Clearance Requirements .....	34
5.3.2 Background Check Procedures .....	34
5.3.3 Training Requirements.....	34
5.3.4 Retraining Frequency and Requirements .....	35
5.3.5 Job Rotation Frequency and Sequence .....	35
5.3.6 Sanctions for Unauthorized Actions .....	35
5.3.7 Independent Contractor Requirements .....	35
5.3.8 Documentation Supplied to Personnel .....	35
<b>5.4 Audit Logging Procedures .....</b>	<b>35</b>
5.4.1 Types of Events Recorded.....	35
5.4.2 Frequency of Processing Log.....	35
5.4.3 Retention Period for Audit Log.....	35
5.4.4 Protection of Audit Log .....	35
5.4.5 Audit Log Backup Procedures.....	35
5.4.6 Audit Collection System (Internal vs. External).....	35
5.4.7 Notification to Event-Causing Subject.....	35
5.4.8 Vulnerability Assessments .....	35
<b>5.5 Records Archival .....</b>	<b>36</b>
5.5.1 Types of Records Archived .....	36
5.5.2 Retention Period for Archive .....	36
5.5.3 Protection of Archive .....	36
5.5.4 Archive Backup Procedures .....	36
5.5.5 Requirements for Time-Stamping of Records .....	36
5.5.6 Archive Collection System (Internal or External) .....	36
5.5.7 Procedures to Obtain and Verify Archive Information .....	36
<b>5.6 Key Changeover.....</b>	<b>36</b>
<b>5.7 Compromise and Disaster Recovery .....</b>	<b>36</b>
5.7.1 Incident and Compromise Handling Procedures.....	36
5.7.2 Computing Resources, Software, and/or Data Are Corrupted .....	37

5.7.3 Entity Private Key Compromise Procedures .....	37
5.7.4 Business Continuity Capabilities After a Disaster .....	37
5.8 CA or RA Termination .....	37
<b>6. Technical Security Controls.....</b>	<b>38</b>
6.1 Key Pair Generation and Installation .....	38
6.1.1 Key Pair Generation.....	39
6.1.2 Private Key Delivery to Subscriber .....	39
6.1.3 Public Key Delivery to Certificate Issuer .....	39
6.1.4 CA Public Key Delivery to Relying Parties.....	39
6.1.5 Key Sizes .....	39
6.1.6 Public Key Parameters Generation and Quality Checking.....	39
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field).....	39
6.2 Private Key Protection and Cryptographic Module Engineering Controls .....	39
6.2.1 Cryptographic Module Standards and Controls .....	39
6.2.2 Private Key (n out of m) Multi-Person Control .....	39
6.2.3 Private Key Escrow .....	39
6.2.4 Private Key Backup .....	39
6.2.5 Private Key Archival.....	39
6.2.6 Private Key Transfer Into or From a Cryptographic Module.....	39
6.2.7 Private Key Storage on Cryptographic Module .....	40
6.2.8 Method of Activating Private Key.....	40
6.2.9 Method of Deactivating Private Key .....	40
6.2.10 Method of Destroying Private Key.....	40
6.2.11 Cryptographic Module Rating .....	40
6.3 Other Aspects of Key Pair Management.....	40
6.3.1 Public Key Archival .....	40
6.3.2 Certificate Operational Periods and Key Pair Usage Periods .....	40
6.4 Activation Data.....	40
6.4.1 Activation Data Generation and Installation.....	40
6.4.2 Activation Data Protection .....	40
6.4.3 Other Aspects of Activation Data.....	40

6.5 Computer Security Controls .....	40
6.5.1 Specific Computer Security Technical Requirements .....	40
6.5.2 Computer Security Rating .....	41
6.6 Life Cycle Technical Controls .....	41
6.6.1 System Development Controls .....	41
6.6.2 Security Management Controls .....	41
6.6.3 Life Cycle Security Controls .....	41
6.7 Network Security Controls .....	41
6.8 Time-Stamping .....	42
<b>7. Certificate, CRL, and OCSP Profiles .....</b>	<b>43</b>
7.1 Certificate Profile .....	43
7.1.1 Version Number(s) .....	43
7.1.2 Certificate Extensions .....	43
7.1.3 Algorithm Object Identifiers .....	44
7.1.4 Name Forms .....	44
7.1.5 Name Constraints .....	45
7.1.6 Certificate Policy Object Identifier .....	45
7.1.7 Usage of Policy Constraints Extension .....	46
7.1.8 Policy Qualifiers Syntax and Semantics .....	46
7.1.9 Processing Semantics for the Critical Certificate Policies Extension .....	46
7.2 CRL Profile .....	46
7.2.1 Version Number(s) .....	46
7.2.2 CRL and CRL Entry Extensions .....	46
7.3 OCSP Profile .....	46
7.3.1 Version Number(s) .....	46
7.3.2 OCSP Extensions .....	46
<b>8. Compliance Audit and Other Assessments .....</b>	<b>47</b>
8.1 Frequency and Circumstances of Assessment .....	47
8.2 Identity/Qualifications of Assessor .....	47
8.3 Assessor's Relationship to Assessed Entity .....	48
8.4 Topics Covered by Assessment .....	48

8.5 Actions Taken as a Result of Deficiency .....	48
8.6 Communications of Results.....	48
<b>9. Other Business and Legal Matters .....</b>	<b>50</b>
<b>9.1 Fees .....</b>	<b>50</b>
9.1.1 Certificate Issuance or Renewal Fees.....	50
9.1.2 Certificate Access Fees .....	50
9.1.3 Revocation or Status Information Access Fees.....	50
9.1.4 Fees for Other Services .....	50
9.1.5 Refund Policy .....	50
<b>9.2 Financial Responsibility.....</b>	<b>50</b>
9.2.1 Insurance Coverage.....	50
9.2.2 Other Assets.....	50
9.2.3 Insurance or Warranty Coverage for End-Entities .....	50
<b>9.3 Confidentiality of Business Information.....</b>	<b>50</b>
9.3.1 Scope of Confidential Information.....	50
9.3.2 Information Not Within the Scope of Confidential Information .....	50
9.3.3 Responsibility to Protect Confidential Information.....	51
<b>9.4 Privacy of Personal Information.....</b>	<b>51</b>
9.4.1 Privacy Plan.....	51
9.4.2 Information Treated as Private .....	51
9.4.3 Information Not Deemed Private.....	51
9.4.4 Responsibility to Protect Private Information .....	51
9.4.5 Notice and Consent to Use Private Information .....	51
9.4.6 Disclosure Pursuant to Judicial or Administrative Process.....	51
9.4.7 Other Information Disclosure Circumstances.....	51
<b>9.5 Intellectual Property rights .....</b>	<b>51</b>
<b>9.6 Representations and Warranties .....</b>	<b>51</b>
9.6.1 CA Representations and Warranties .....	51
9.6.2 RA Representations and Warranties .....	52
9.6.3 Subscriber Representations and Warranties .....	52
9.6.4 Relying Party Representations and Warranties.....	52
9.6.5 Representations and Warranties of Other Participants.....	52

9.7 Disclaimers of Warranties.....	52
9.8 Limitations of Liability .....	52
9.9 Indemnities .....	52
9.10 Term and Termination.....	52
9.10.1 Term .....	52
9.10.2 Termination.....	52
9.10.3 Effect of Termination and Survival.....	53
9.11 Individual Notices and Communications with Participants.....	53
9.12 Amendments .....	53
9.12.1 Procedure for Amendment .....	53
9.12.2 Notification Mechanism and Period.....	53
9.12.3 Circumstances Under Which OID Must be Changed .....	53
9.13 Dispute Resolution Provisions.....	53
9.14 Governing Law .....	53
9.15 Compliance with Applicable Law.....	53
9.16 Miscellaneous Provisions .....	53
9.16.1 Entire Agreement.....	53
9.16.2 Assignment .....	53
9.16.3 Severability .....	53
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) .....	54
9.16.5 Force Majeure .....	54
9.17 Other Provisions .....	54
9.17.1 Disabilities .....	54
9.17.2 Organizational.....	54
9.17.3 Additional testing.....	54

# 1. Introduktion (Introduction)

Note: This Danish introduction clause will follow in an English translation

(in Danish)

Denne certifikatpolitik (CP) er udarbejdet og administreres af Digitaliseringsstyrelsen, og har været i bred offentlig høring. Den seneste version af denne CP samt eventuelle tidligere versioner, under hvilke der stadig findes gyldige certifikater, kan findes på <https://certifikat.gov.dk> eller rekvisiteres hos Digitaliseringsstyrelsen.

Avancerede elektroniske signaturer og segl anvendes til at sikre ægthed og integritet af data i elektronisk form. I praksis kræver brugen af sådanne signaturer og segl etablering af en Public Key Infrastructure (PKI). Digitaliseringsstyrelsen har udarbejdet denne samlede certifikatpolitik for kvalificerede certifikater og OCES-certifikater (ikke-kvalificerede), der udstedes til private personer (betegnet fysiske personer), medarbejdere (betegnet fysiske personer tilknyttet juridiske personer), og organisationer (betegnet juridiske enheder).

OCES (dansk forkortelse for *Offentlige Certifikater til Elektroniske Services*) har siden 2003 udgjort en offentlig dansk standard for ikke-kvalificerede certifikater. Udstedelse af OCES-certifikater er reguleret som en ikke-kvalificeret tillidstjeneste jf. "Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet" (herefter benævnt eIDAS2 forordningen eller eIDAS2). Dette betyder, at eIDAS2 kræver mindst et passivt tilsyn med tillidstjenesteudbydere, der udsteder OCES-certifikater. OCES-rammeverket stiller dog krav om et aktivt tilsyn, som er sammenligneligt med det, der gælder for udbydere af kvalificerede certifikater. I denne politik er kravene til OCES-certifikater i overensstemmelse med kravene til NCP-certifikater i henhold til ETSI-standarderne.

Tillidstjenesteudbydere, der udsteder OCES-certifikater, skal anvende og opfylde kravene i denne CP eller en anden gyldig OCES-CP udarbejdet og administreret af Digitaliseringsstyrelsen. Et certifikat er således kun et OCES-certifikat, hvis det er udstedt efter en CP for OCES-certifikater og er udstedt af et CA, som er godkendt af Digitaliseringsstyrelsen som udsteder af OCES-certifikater. Som led i godkendelsen indgås en formel aftale mellem CA og Digitaliseringsstyrelsen, hvori CA bl.a. forpligter sig til at opfylde kravene i denne CP, herunder krav om revision af CA's opgavevaretagelse, jf. i øvrigt afsnit 8.

Kvalificerede certifikater er defineret og reguleret i eIDAS2 forordningen, som fastlægger rammerne for et aktivt tilsyn med tillidstjenesteudbydere, der udsteder kvalificerede certifikater.

Denne politik er en offentlig standard, der regulerer udstedelse og anvendelse af public key certifikater. eIDAS2 forordningens artikel 25 og artikel 35 omhandler retsvirkningen af elektroniske signaturer henholdsvis elektroniske segl.

Tillidstjenesteudbydere, der udsteder kvalificerede certifikater, kan anvende denne kvalificerede certifikatpolitik, som er udarbejdet og administreret af Digitaliseringsstyrelsen, eller alternativt anvende egne kvalificerede certifikatpolitiske, såfremt de overholder kravene i eIDAS2-forordningen og de tilhørende gennemførelsesretsakter.

Kravene i denne CP er i overensstemmelse med og henviser til følgende standarder:

- ETSI EN 319 401 V3.1.1 (herefter betegnet ETSI EN 319 401)
- ETSI EN 319 411-1 V1.5.1 (hereafter betegnet ETSI EN 319 411-1)
- ETSI EN 319 411-2 V2.6.1 (hereafter betegnet ETSI EN 319 411-2)

Denne CP omfatter følgende kravtyper:

1. Obligatoriske krav, som skal opfyldes. Disse krav anvender termene 'shall/must'.
2. Krav, der beskriver begrænsninger i relation til denne CP, anvender termen 'must not'.
3. Krav der bør opfyldes. Hvis et sådant krav ikke opfyldes, skal der gives en begrundelse. Denne type krav anvender termen 'should'.
4. Krav der kan opfyldes efter CA's skøn. Denne type krav anvender termen 'may'.

Denne certifikatpolitik træder i kraft den **XX.XX.XXXX**. Certifikater må ikke udstedes i henhold til tidligere certifikatpolitikker udstedt af Digitaliseringsstyrelsen senere end seks måneder efter, at denne politik er trådt i kraft.

Digitaliseringsstyrelsen er den offentlige myndighed, der fører tilsyn med tillidstjenesteudbydere i Danmark.

**(in English)**

This Certificate Policy (CP) has been produced by and is managed by the Danish Agency for Digital Government. The latest version of this CP and any previous versions, under which valid certificates still exist, can be found on <https://certifikat.gov.dk> or can be requested from the Agency for Digital Government.

Advanced electronic signature and seal are used to ensure authenticity and integrity of data in electronic form. In practice, the use of advanced electronic signature and seal requires the establishment of a Public Key Infrastructure (PKI). The Danish Agency for Digital Government has produced this combined certificate policy for qualified and OCES (non-qualified) certificates issued to private individuals (denoted natural persons), employees (denoted natural persons associated with a legal persons) and organisations (denoted legal persons).

OCES (the Danish abbreviation for *Public Certificates for Electronic Services*) has, since 2003, constituted a public Danish standard for non-qualified certificates. The issuance of OCES certificates is regulated as a non-qualified trust service pursuant to "Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework" (hereinafter denoted eIDAS2 regulation or eIDAS2). This means that eIDAS2 requires at least passive supervision of trust service providers issuing OCES certificates. However, the OCES framework imposes requirements for active supervision comparable to those applicable to providers of qualified certificates. Under this policy, the requirements for OCES certificates are aligned with the requirements for NCP certificates in accordance with ETSI standards.

Trust service providers issuing OCES certificates shall apply and comply with the requirements set out in this CP or another valid OCES CP prepared and administered by the Danish Agency for Digital

Government. A certificate is therefore only an OCES certificate if it is issued in accordance with a CP for OCES certificates and is issued by a CA that has been approved by the Danish Agency for Digital Government as an issuer of OCES certificates. As part of the approval, a formal agreement is entered into between the CA and the Danish Agency for Digital Government, under which the CA, *inter alia*, undertakes to comply with the requirements of this CP, including requirements for audits of the CA's performance of its duties, cf. section 8.

Qualified certificates are defined and regulated via the eIDAS2 regulation, which set the framework for an active supervisory of trust service providers issuing qualified certificates.

This policy constitutes a common public standard regulating the issuance and use of public key certificates. The legal effect of electronic signatures and electronic seals based on qualified certificates and OCES certificates issued under this policy is defined in eIDAS2 article 25 and article 35.

Trust service providers issuing qualified certificates may use this qualified certificate policy produced and managed by the Danish Agency for Digital Government but may also use proprietary qualified certificate policies if they comply with the requirements of the eIDAS Regulation, including related implementing regulation.

The requirements of this CP are compliant with and refers to the requirements in standards

- ETSI EN 319 401 V3.1.1 (hereafter denoted ETSI EN 319 401),
- ETSI EN 319 411-1 V1.5.1 (hereafter denoted ETSI EN 319 411-1) and
- ETSI EN 319 411-2 V2.6.1 (hereafter denoted ETSI EN 319 411-2).

The requirements in this CP include:

1. Mandatory requirements, which must be met. Such requirements use the term 'shall/must'.
2. Requirements describing prohibitions in relation to compliance with this CP use the wording 'must not'.
3. Requirements that should be met. If such requirements are not met, reasons must be given. Such requirements use the term 'should'.
4. Requirements that may be met if requested by the CA. Such requirements use the term 'may'.

This certificate policy will be effective from **XX.XX.XXXX**. Certificates shall not be issued from previous certificate policies issued by the Agency for Digital Government six month after this policy being effective.

The Danish Agency for Digital Government is the public supervisory body with regards to trust service providers in Denmark.

## 1.1 Overview

This CP describes the requirements for the issuance of an OCES or a qualified certificate to natural persons, natural persons associated with a legal person and legal persons. Requirements which are only applied to some certificate types are marked as follows

- “[POCES]” OCES certificates issued to natural persons
- “[MOCES]” OCES certificates issued to natural persons associated with a legal person

- “[VOCES]” OCES certificates issued to legal persons
- “[OCES]” All OCES certificate types
- “[QP]” Qualified certificates issued to natural persons
- “[QE]” Qualified certificates issued to natural persons associated with a legal person
- “[QO]” Qualified certificates issued to legal persons
- “[Q]” All qualified certificate types

The structure of this CP is compliant with RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

The provisions of the Certificate Policy on how the CA must act shall ensure a high level of assurance that the subject has the identity specified in the certificate.

This means that the trust of the subscriber and relying parties can be based on the Certificate Policy and the related EU regulation, including the ongoing supervision with the CA performed by the Danish Agency for Digital Government, trust service supervisory body.

Certification authorities subject to Danish supervision issuing OCES or qualified certificates are available on request to the Danish supervisory body.

## 1.2 Document Name and Identification

### 1.2.1 Naming

This document named "Combined Public Certificate Policy for OCES and Qualified Certificates Version 8.0".

### 1.2.2 Identification

This CP is identified by the following object identifier (OID):

iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) general(3) major-ver(8) minor-ver(0)

Certificates issued under this CP is identified by the following object identifiers (OIDs):

- [POCES] iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) person(1) major-ver(8) minor-ver(0)
- [MOCES] iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) medarbejder(2) major-ver(8) minor-ver(0)
- [VOCES] iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) virksomhed(3) major-ver(8) minor-ver(0)
- [QP] iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) person(1) major-ver(8) minor-ver(0)

- [QE] iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) medarbejder(2) major-ver(8) minor-ver(0)
- [QO] iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) virksomhed(3) major-ver(8) minor-ver(0)

The OIDs are registered in Danish Standards in accordance with DS 2391:1995, parts 1 and 3.

[QP][QE][QO] Certificates with the latter three OIDs included are qualified certificates and they require the use of QSCD to protect the subjects' private key cf. eIDAS2.

## 1.3 PKI Participants

### 1.3.1 Certification Authorities

A certification authority (CA) is a natural person or legal entity trusted by both subscribers and relying parties to generate, issue and administer electronic certificates. The CA has the overall responsibility for providing the services required to issue and maintain certificates. The CA's own keys are used to sign issued certificates, and the CA is identified in the certificate as issuer.

[REQ 1.3.1-01] Requirement REQ-7.1.1-01 in [ETSI EN 319 401] shall apply.

[REQ 1.3.1-02] Requirement REQ-7.1.1-02 in [ETSI EN 319 401] shall apply.

[REQ 1.3.1-03] Requirement REQ-7.1.1-03 in [ETSI EN 319 401] shall apply.

[REQ 1.3.1-04] Requirement OVR-5.4.1-01 in [ETSI EN 319 411-1] shall apply.

[REQ 1.3.1-05] Requirement OVR-5.4.1-02 in [ETSI EN 319 411-1] shall apply.

[REQ 1.3.1-06] Requirement OVR-5.4.1-03 in [ETSI EN 319 411-1] shall apply.

### 1.3.2 Registration Authorities

The registration authorities (RA) undertake the identification and registration of subjects on behalf of the CA before issuance and re-key of a certificate.

The RA may either be closely linked to the CA, or it may be an independent function, e.g. an identity proofing service provider. In any circumstances, the CA is liable for the RA's compliance with the applicable requirements and obligations in the exact same way as for its own affairs. It is the responsibility of the CA to ensure that the RA follows the provisions set out in this CP.

### 1.3.3 Subscribers

Prior to the issuance of certificates, the CA enters into an agreement with the subscriber.

Certificates are issued to subject. Subscribers and subjects may be the same natural person e.g. if the subscriber represents herself or himself as a private citizen or it may be different entities e.g. if the subject is a natural person associated with the subscriber.

This CP uses the terms subscriber and subject to distinguish between the entity entering into an agreement with a CA and the entity identified in the certificate.

The subscriber has the final responsibility for the use of the certificate and the related private keys, even though the subject has control of the private key.

### 1.3.4 Relying Parties

A relying party is the party relying on a certificate issued by the CA. This is typically a natural person or legal entity receiving an electronically signed document or authenticating a subject through the use of a PKI.

### 1.3.5 Other Participants

The supervisory body for CA issuing certificates according to this CP is the Danish Agency for Digital Government.

**[REQ 1.3.5-01]** Requirement OVR-5.4.3-01 in [ETSI EN 319 411-1] shall apply.

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Uses

**[REQ 1.4.1-01]** A certificate may be used to secure sender and message authenticity, including electronic signature and message integrity. It may also be used to ensure confidentiality (encryption).

Note: Please note the limitations in clause 1.4.2.

**[REQ 1.4.1-02]** Certificates issued under this CP may be valid for a period of maximum 4 years.

### 1.4.2 Prohibited Certificate Uses

**[REQ 1.4.2-01]** [OCES] OCES certificates are not qualified certificates, i.e. they must not be used in situations where qualified certificates are required.

**[REQ 1.4.2-02]** Certificates issued under this CP must not be used to sign other certificates.

**[REQ 1.4.2-03]** [POCES] [MOCES] [QP] [QE] The subject's private key must not be used without being authorized in each individual case by the subject through the use of activation data. This means that storing keys in automated systems which use them on behalf of the subject is not allowed.

**[REQ 1.4.2-04]** The subject's private key may not be used beyond what is specified in the certificate keyUsage, cf. clause 7.1.2.

## 1.5 Policy Administration

### 1.5.1 Organization Administering the Document

This CP is owned and maintained by Danish Agency for Digital Government.

### 1.5.2 Contact Person

Inquiries regarding this CP can be addressed to:

Agency for Digital Government  
Landgreven 4  
1301 Copenhagen K  
Denmark

Phone +45 3392 5200  
Email: [digst@digst.dk](mailto:digst@digst.dk)

### 1.5.3 Person Determining CPS Suitability for the Policy

[REQ 1.5.3-01] [OCES] The CA may issue OCES certificates under this CP if the CA

- has entered into a written agreement with the Danish Agency for Digital Government to this effect; and
- has submitted a CA report, cf. below, to the Danish Agency for Digital Government; and
- has received a declaration of compliance from the Danish Agency for Digital Government confirming that the Danish Agency for Digital Government has approved the submitted report and considers the requirements of this CP to be met.

Note: If CA is the Agency for Digital Government on behalf of the Danish state no written agreement shall be entered cf. first bullet in the above.

[REQ 1.5.3-02] [OCES] An updated CA report must be submitted at least once a year to the Danish Agency for Digital Government.

[REQ 1.5.3-03] [OCES] The report must include:

- CAs, CPS;
- Auditor's records from conformity assessment body;
- a declaration from the CA's management specifying whether the CA's overall data, system and operational security can be considered adequate and that the CPS addresses all requirements of this CP and that the CA complies with its own CPS;
- a declaration from the conformity assessment body specifying whether the CA's overall data, system and operational security – in the opinion of the body – can be considered adequate and that the CPS addresses all requirements of this CP and that the CA complies with its own CPS; and
- documentation of liability insurance covering CA's liability.

[REQ 1.5.3-04] [OCES] The report and its content must be in Danish or English. The Danish Agency for Digital Government may grant an exemption for this requirement.

### 1.5.4 CPS Approval Procedures

[REQ 1.5.4-01] All requirements in [ETSI EN 319 401] clause 6.1 "Trust Service Practice statement" shall apply.

[REQ 1.5.4-02] Requirement OVR-5.2-02 in [ETSI EN 319 411-1] shall apply.

[REQ 1.5.4-03] Requirement OVR-5.2-10 in [ETSI EN 319 411-1] shall apply.

[REQ 1.5.4-04] The CPS must be in Danish or English.

## 1.6 Definitions and Acronyms

### 1.6.1 Definitions

This clause provides definitions of the special terms used in this CP.

**Activation data:** Data that can activate the use of the subject's private key(s). This may be a password.

**Authorized person/entity:** Person or logical entity given authority by a management representative with the required power of procuration from the sub-scriber to register any subjects and administer certificates for subscriber on behalf of the business.

**Certification authority – CA:** A natural person or legal entity generating, issuing and administering certificates in its capacity as trust service provider. The eIDAS Regulation uses the term certification-service-provider for this entity.

**Certification Practice Statement – CPS:** A specification of the principles and procedures used by the CA when issuing certificates to comply with related CPs. See the description in RFC 3647 clause 3.4.

**Public key certificate:** An electronic certificate specifying the subscriber's public key as well as additional information which uniquely links the public key to the identification of the subscriber. A public key certificate must be signed by a Certification Authority (CA) which thus confirms the validity of the certificate.

**Subject:** A natural person or entity with a subscriber who/which, in the certificate, is identified as the proper user of the private key that belongs to the public key, which is granted in the certificate, and to whom an OCES certificate is either being issued or has already been issued.

**Subscriber:** A natural person or legal entity who/which concludes an agreement with the issuing Certification Authority (CA) on the issuance of certificates to one or more subjects.

**Certificate Policy:** A set of rules that sets out requirements for the issuance and use of certificates or several specific contexts with common security requirements. See the description in RFC 3647 clause 3.1.

**Danish Data Protection Act:** Act no. 502 of 23 May 2018 on additional provision on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

**Digital signature:** Data in electronic form used for authentication of other electronic data to which the digital signature is attached or logically connected.

**Sole control:** Property which uses up-to-date technical and administrative measures to ensure that a given entity solely controls the use of a resource.

Examples:

A subject (entity) may have sole control of a private signature key (resource) by placing the private key securely on a cryptographic hardware module where the activation of the key is based on something held and known only by the subject.

**ISO 27001:** "ISO/IEC 27001:2022 - Information technology -- Security techniques – Information security management systems" as well as subsequent amendments.

**ISO 27002:** "ISO/IEC 27002:2013 - Information technology -- Security techniques – Code of practice for information security controls" as well as subsequent amendments.

**Cryptographic module:** Hardware unit which independently of the operating system can generate and store keys and use the digital signature with appropriate certification e.g. SSCD-PP Type 3.

**Qualified certificate:** "Qualified Certificate for Electronic Signature" or a "Qualified Certificate for Electronic Seal" as defined in eIDAS Article 3(15) and Article 3(30), respectively.

**Employee:** Person associated with the organization specified in the certificate.

**Relying party:** a natural person or legal entity relying on a CA as a trusted service.

**Key Escrow:** Storing of keys with a view to making them available to a third party in order for such third party to decrypt data.

**Conformity assessment body:** Legal entity that audits the CA's compliance with this certificate policy. See clause 8 for requirements for the conformity assessment body.

**Private key:** The subject's key for provision of digital signature or for decryption. The private key is personal and must not be disclosed by the subject.

**Registration authority —RA:** The natural person or legal entity responsible for identifying and authenticating a (coming) subject.

**Root CA:** Highest CA in a hierarchy of CAs.

**Root certificate:** A public certificate issued by a CA for validating other certificates. A root certificate is signed with its own signing key ("self-signed").

**Root key:** The root CA's private and public keys used for signing certificates and certificate revocation lists.

**Level of Assurance (LoA):** The degree of trust in an authenticated electronic identity.

**Certificate Revocation List:** List of certificates that are no longer considered valid because they have been permanently revoked.

## 1.6.2 Abbreviations

AIA	Authority Information Access
BCP	Business Continuity Plan
CA	Certification Authority
CEN	European Committee for Standardization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CVR	Central Business Register
eIDAS2	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
ENISA	The European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
GDPR	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
KSC	Key Signing Ceremony
LDAP	Lightweight Directory Access Protocol
MOCES	Employee OCES
NCP	Normalized Certificate Policy
NSIS	National Standard for Identity Assurance Levels
OCES	Public Certificates for Electronic Services
OCSP	Online Certificate Status Protocol
OID	Object identifier, cf. ITU-T's ASN.1 standard
PKI	Public Key Infrastructure
POCES	Personal OCES
RA	Registration Authority
TSP	Trust Service Provider
UTC	Universal Time Coordinated
UUID	Universally Unique Identifier
VOCES	Organisational OCES

## 2. Publication and Repository Responsibilities

### 2.1 Repositories

**[REQ 2.1-01]** All requirements in [ETSI EN 319 401] clause 6.2 “Terms and Conditions” shall apply.

**[REQ 2.1-02]** All non-marked requirements in [ETSI EN 319 411-1] clause 6.9.4 “Terms and Conditions” shall apply.

**[REQ 2.1-03]** Requirement OVR-7.2-01 in [ETSI EN 319 411-1] shall apply.

**[REQ 2.1-04]** Requirement OVR-5.2-04 in [ETSI EN 319 411-1] shall apply.

**[REQ 2.1-05]** Requirement OVR-5.2-05 in [ETSI EN 319 411-1] shall apply.

**[REQ 2.1-06]** Requirement DIS-6.1-04 in [ETSI EN 319 411-1] shall apply.

**[REQ 2.1-07]** Requirement DIS-6.1-05 in [ETSI EN 319 411-1] shall apply.

**[REQ 2.1-08]** Requirement DIS-6.1-08 in [ETSI EN 319 411-1] shall apply.

**[REQ 2.1-09]** Requirement DIS-6.1-09 in [ETSI EN 319 411-1] shall apply.

### 2.2 Publication of Certification Information

**[REQ 2.2-01]** Requirement DIS-6.1-01A in [ETSI EN 319 411-1] shall apply.

**[REQ 2.2-02]** Requirement DIS-6.1-01B in [ETSI EN 319 411-1] shall apply.

**[REQ 2.2-03]** Requirement DIS-6.1-01C in [ETSI EN 319 411-1] shall apply.

**[REQ 2.2-04]** Requirement DIS-6.1-02A in [ETSI EN 319 411-1] shall apply.

**[REQ 2.2-05]** Requirement DIS-6.1-07A in [ETSI EN 319 411-1] shall apply.

**[REQ 2.2-06]** Requirement DIS-6.1-10 in [ETSI EN 319 411-1] shall apply.

### 2.3 Time or Frequency of Publication

N/A

### 2.4 Access Controls on Repositories

N/A

# 3. Identification and Authentication

## 3.1 Naming

### 3.1.1 Type of Names

**[REQ 3.1.1-01]** [MOCES] [VOCES] [QE] [QO] The subscriber shall be identified by a name registered in the CVR. However, deviations are allowed, cf. clause 3.1.2.

**[REQ 3.1.1-02]** The subject shall be identified by a registered name or a pseudonym. However, deviations are allowed, cf. clause 3.1.2. It must be recorded whether a name or pseudonym has been used.

Note: Regardless of whether the CA enters the name or pseudonym of the subject, the CA must, possibly via a third party, be able to identify the subject as a natural person.

### 3.1.2 Need for Names to be Meaningful

**[REQ 3.1.2-01]** [MOCES] [VOCES] [QE] [QO] The name of the subscriber shall be the name or secondary name registered in the CVR. However, corporate forms in the name, e.g. 'ApS', 'A/S' and 'Fonden' may be left out. Danish letters and special characters may be re-placed unless this causes obvious misunderstandings, and long names may be abbreviated unless this causes obvious misunderstandings.

**[REQ 3.1.2-02]** [POCES] [QP] The name of the subject shall be verified via an authoritative source.

Note: An authoritative source may be the Civil Registration system, eIDAS nodes (cf. Article 12 of eIDAS) or a valid passport.

**[REQ 3.1.2-03]** [POCES] [MOCES] [QP] [QE] If the subject is registered with a name, such name shall as a minimum consist of a registered first name and last name. Any middle name may be omitted, and the name must not include words not forming part of a subject's name such as pet names.

**[REQ 3.1.2-04]** If the subject is registered with a pseudonym, such pseudonym may not be of a nature that may cause obvious misunderstandings and must not be identical or confusingly like a trademark. Moreover, the CA may reject the use of pseudonyms.

Note: The CA may reject a pseudonym if it may be perceived as offensive or un-ethical.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

**[REQ 3.1.3-01]** The subscriber shall be able to select that the name of the subject does not appear from issued certificates.

### 3.1.4 Rules for Interpreting Various Name Forms

N/A

### 3.1.5 Uniqueness of Names

**[REQ 3.1.5-01]** The uniqueness of the subject shall be ensured by using serial-Number in subject distinguishedName.

### 3.1.6 Recognition, Authentication, and Role of Trademarks

N/A

## 3.2 Initial Identity Validation

[REQ 3.2-01] Requirement REG-6.2.2-01 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2-02] Requirement REG-6.2.2-02A in [ETSI EN 319 411-1] shall apply.

[REQ 3.2-03] Requirement REG-6.2.2-02AB in [ETSI EN 319 411-1] shall apply.

[REQ 3.2-04] Requirement REG-6.2.2-02AC in [ETSI EN 319 411-1] shall apply.

[REQ 3.2-05] Requirement REG-6.2.2-02B in [ETSI EN 319 411-1] shall apply.

[REQ 3.2-06] Requirement REG-6.2.2-25 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2-07] Requirement REG-6.2.2-26 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2-08] [QP][QE] Requirement REG-6.2.2-02 in [ETSI EN 319 411-2] shall apply.

[REQ 3.2-09] [QO] Requirement REG-6.2.2-03 in [ETSI EN 319 411-2] shall apply.

### 3.2.1 Method to Prove Possession of Private Key

[REQ 3.2.1-01] Requirement REG-6.3.1-01 in [ETSI EN 319 411-1] shall apply.

### 3.2.2 Authentication of Organization Identity

[REQ 3.2.2-01] [VOCES][QO] Requirement REG-6.2.2-10 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-02] [VOCES][QO] Requirement REG-6.2.2-10A in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-03] [VOCES][QO] Requirement REG-6.2.2-12 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-04] [VOCES] [QO] Requirement REG-6.2.2-13 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-05] [VOCES] [QO] Requirement REG-6.2.2-13A in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-06] [VOCES] [QO] Requirement REG-6.2.2-15A in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-07] [VOCES] [QO] Requirement REG-6.2.2-16 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-08] [VOCES] [QO] Requirement REG-6.2.2-16A in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-09] [VOCES] [QO] Requirement REG-6.2.2-16B in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.2-10] [VOCES] [QO] Requirement REG-6.2.2-17A in [ETSI EN 319 411-1] shall apply.

### 3.2.3 Authentication of Individual Identity

[REQ 3.2.3-01] [POCES][MOCES][QP][QE] Requirement REG-6.2.2-05 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.3-02] [POCES][MOCES][QP][QE] Requirement REG-6.2.2-05A in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.3-03] [POCES][MOCES][QP][QE] Requirement REG-6.2.2-05B in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.3-04] [POCES][MOCES][QP][QE] Requirement REG-6.2.2-05C in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.3-05] [POCES][MOCES][QP][QE] Requirement REG-6.2.2-06 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.3-06] [POCES][MOCES][QP][QE] Requirement REG-6.2.2-07 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.3-07] [MOCES][QE] Requirement REG-6.2.2-08 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.3-08] [MOCES][QE] Requirement REG-6.2.2-08A in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.3-09] [MOCES][QE] Requirement REG-6.2.2-09 in [ETSI EN 319 411-1] shall apply.

### 3.2.4 Non-Verified Subscriber Information

[REQ 3.2.4-01] Requirement REG-6.2.2-21 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.4-02] Requirement REG-6.2.2-22 in [ETSI EN 319 411-1] shall apply.

[REQ 3.2.4-03] Requirement REG-6.2.2-23 in [ETSI EN 319 411-1] shall apply.

### 3.2.5 Validation of Authority

Cf. clause 3.2.2 and clause 3.2.3

### 3.2.6 Criteria for Interoperation

N/A

## 3.3 Identification and Authentication for Re-Key Requests

### 3.3.1 Identification and Authentication for Routine Re-Key

N/A

### 3.3.2 Identification and Authentication for Re-Key After Revocation

N/A

## 3.4 Identification and Authentication for Revocation Request

See clause 4.9

# 4. Certificate Life-Cycle Operational Requirements

## 4.1 Certificate Application

### 4.1.1 Who Can Submit a Certificate Application

[REQ 4.1.1-01] Requirement REG-6.3.1-00F in [ETSI EN 319 411-1] shall apply.

### 4.1.2 Enrollment Process and Responsibilities

[REQ 4.1.2-01] Application for certificates shall be made through an RA according to a defined enrollment process.

Note: The RA may be part of the CA's organization and/or one or more external business partners.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

[REQ 4.2.1-01] [OCES] Before a certificate is issued to a registered subject, the subject shall be identified and authenticated at NSIS assurance level 'substantial' or 'high', eIDAS assurance level 'substantial' or 'high' or ETSI TS 119 461 LoIP 'Baseline' or 'Extended'.

[REQ 4.2.1-01] Requirement REG-6.3.1-00A in [ETSI EN 319 411-1] shall apply.

[REQ 4.2.1-02] Requirement REG-6.3.1-00B in [ETSI EN 319 411-1] shall apply.

[REQ 4.2.1-03] Requirement REG-6.3.1-00C in [ETSI EN 319 411-1] shall apply.

[REQ 4.2.1-04] Requirement REG-6.3.1-00D in [ETSI EN 319 411-1] shall apply.

[REQ 4.2.1-05] Requirement REG-6.3.1-00E in [ETSI EN 319 411-1] shall apply.

### 4.2.2 Approval or Rejection of Certificate Applications

[REQ 4.2.2-01] Requirement REG-6.3.2-00B in [ETSI EN 319 411-1] shall apply.

### 4.2.3 Time to Process Certificate

[REQ 4.2.3-01] The CA should process certificate applications without undue delay.

## 4.3 Certificate Issuance

### 4.3.1 CA Actions During Certificate Issuance

[REQ 4.3.1-01] Requirement REG-6.3.2-00A in [ETSI EN 319 411-1] shall apply.

[REQ 4.3.1-02] Requirement REG-6.3.2-01 in [ETSI EN 319 411-1] shall apply.

[REQ 4.3.1-03] Requirement REG-6.3.2-02 in [ETSI EN 319 411-1] shall apply.

[REQ 4.3.1-04] All non-marked requirements and requirements marked with "[NCP]" in [ETSI EN 319 411-1] clause 6.3.3 "Certificate issuance" shall apply.

[REQ 4.3.1-05] [Q] Requirement REG-6.3.3-09A in [ETSI EN 319 411-1] shall apply.

**[REQ 4.3.1-06]** [POCES] The allocated OID referred in requirement GEN-6.3.3-12 in [EN 319 411-1] shall be

iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) person(1) major-ver(8) minor-ver(0)

**[REQ 4.3.1-07]** [MOCES] The allocated OID referred in requirement GEN-6.3.3-12 in [EN 319 411-1] shall be

iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) medarbejder(2) major-ver(8) minor-ver(0)

**[REQ 4.3.1-08]** [VOCES] The allocated OID referred in requirement GEN-6.3.3-12 in [EN 319 411-1] shall be

iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) virksomhed(3) major-ver(8) minor-ver(0)

**[REQ 4.3.1-09]** [QP] The allocated OID referred in requirement GEN-6.3.3-12 in [EN 319 411-1] shall be

iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) person(1) major-ver(8) minor-ver(0)

**[REQ 4.3.1-10]** [QE] The allocated OID referred in requirement GEN-6.3.3-12 in [EN 319 411-1] shall be

iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) medarbejder(2) major-ver(8) minor-ver(0)

**[REQ 4.3.1-11]** [QO] The allocated OID referred in requirement GEN-6.3.3-12 in [EN 319 411-1] shall be

iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) q(2) virksomhed(3) major-ver(8) minor-ver(0)

#### 4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

**[REQ 4.3.2-01]** The CA may notify the subject and/or subscriber of issuance of certificate.

### 4.4 Certificate Acceptance

#### 4.4.1 Conduct Constituting Certificate Acceptance

**[REQ 4.4.1-01]** All requirements in [ETSI EN 319 411-1] clause 6.3.4 “Certificate acceptance” shall apply.

**[REQ 4.4.1-02]** [Q] Requirement OVR-6.3.4-02 in [ETSI EN 319 411-2] shall apply.

#### 4.4.2 Publication of the Certificate by the CA

**[REQ 4.4.2-01]** The CA shall publish the certificate, cf. clause 2.2 with due regard to clause 4.4.1.

#### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

**[REQ 4.4.3-01]** The CA may notify other participants of the issuance of a certificate with due regard to clause 4.4.1.

## 4.5 Key Pair and Certificate Usage

### 4.5.1 Subscriber Private Key and Certificate Usage

**[REQ 4.5.1-01]** All non-marked requirements and requirements marked with “[NCP]” in [ETSI EN 319 411-1] clause 6.3.5 “Key pair and certificate usage” shall apply.

**[REQ 4.5.1-02]** [Q] f) and g) of requirement OVR-6.3.5-01 in [ETSI EN 319 411-1] shall apply.

**[REQ 4.5.1-03]** [Q] Requirement SDP-6.3.5-02 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-04]** [QP][QE] Requirement SDP-6.3.5-03 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-05]** [QO] Requirement SDP-6.3.5-04 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-06]** [QP][QE] Requirement SDP-6.3.5-05 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-07]** [QO] Requirement SDP-6.3.5-06 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-08]** [Q] Requirement SDP-6.3.5-07 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-09]** [QP][QE] Requirement SDP-6.3.5-08 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-10]** [QO] Requirement SDP-6.3.5-09 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-11]** [QP][QE] Requirement SDP-6.3.5-10 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-12]** [QO] Requirement SDP-6.3.5-11 in [ETSI EN 319 411-2] shall apply.

**[REQ 4.5.1-13]** [Q] Requirement SDP-6.3.5-12 in [ETSI EN 319 411-2] shall apply.

### 4.5.2 Relying Party Public Key and Certificate Usage

N/A

## 4.6 Certificate Renewal

Renewal of a subject’s certificate means issuance of a new certificate according to this Certificate Policy to the same subject with the same public key as a previously issued certificate, but with a new validity period, a new certificate serial number and the current Policy OID.

**[REQ 4.6-01]** All non-marked requirements in [ETSI EN 319 411-1] clause 6.3.6 “Certificate renewal” shall apply.

### 4.6.1 Circumstances for Certificate Renewal

See REQ 4.6-01.

### 4.6.2 Who May Request Renewal

**[REQ 4.6.2-01]** The subscriber may apply for a certificate renewal for a subject.

### 4.6.3 Processing Certificate Renewal Requests

See REQ 4.6-01.

### 4.6.4 Notification of New Certificate Issuance to Subscriber

See REQ 4.6-01.

#### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See REQ 4.6-01.

#### 4.6.6 Publication of the Renewal Certificate by the CA

See REQ 4.6-01.

#### 4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See REQ 4.6-01.

### 4.7 Certificate Re-Key

Re-key of a subject's certificate means issuance of a new certificate according to this Certificate Policy to a previously registered subject with a new key pair, new validity period, a new certificate serial number and the current Policy OID.

**[REQ 4.7-01]** All non-marked requirements in [ETSI EN 319 411-1] clause 6.3.7 "Certificate Re-key" shall apply.

#### 4.7.1 Circumstances for Certificate Re-Key

See REQ 4.7-01.

#### 4.7.2 Who May Request Certification of a New Public Key

See REQ 4.7-01.

#### 4.7.3 Processing Certificate Re-Keying Requests

See REQ 4.7-01.

#### 4.7.4 Notification of New Certificate Issuance to Subscriber

See REQ 4.7-01.

#### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See REQ 4.7-01.

#### 4.7.6 Publication of the Re-Keyed Certificate by the CA

See REQ 4.7-01.

#### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See REQ 4.7-01.

### 4.8 Certificate Modification

**[REQ 4.8-01]** All requirements in [ETSI EN 319 411-1] clause 6.3.7 "Certificate modification" shall apply.

#### 4.8.1 Circumstances for Certificate Modification

See REQ 4.8-01.

#### 4.8.2 Who May Request Certificate Modification

See REQ 4.8-01.

#### 4.8.3 Processing Certificate Modification Requests

See REQ 4.8-01.

#### 4.8.4 Notification of New Certificate Issuance to Subscriber

See REQ 4.8-01.

#### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

See REQ 4.8-01.

#### 4.8.6 Publication of the Modified Certificate by the CA

See REQ 4.8-01.

#### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See REQ 4.8-01.

### 4.9 Certificate Revocation and Suspension

**[REQ 4.9-01]** Requirement REV-6.2.4-01 in [ETSI EN 319 411-1] shall apply.

**[REQ 4.9-02]** Requirement REV-6.3.9-15 in [ETSI EN 319 411-1] shall apply.

**[REQ 4.9-03]** Requirement REV-6.3.9-15A in [ETSI EN 319 411-1] shall apply.

**[REQ 4.9-04]** Requirement REV-6.3.9-16 in [ETSI EN 319 411-1] shall apply.

**[REQ 4.9-05]** Requirement REV-6.3.9-17 in [ETSI EN 319 411-1] shall apply.

**[REQ 4.9-06]** Requirement REV-6.3.9-18 in [ETSI EN 319 411-1] shall apply.

**[REQ 4.9-07]** Requirement REV-6.3.9-19 in [ETSI EN 319 411-1] shall apply.

#### 4.9.1 Circumstances for Revocation

**[REQ 4.9.1-01]** Requirement REV-6.3.9-01 in [ETSI EN 319 411-1] shall apply.

**[REQ 4.9.1-02]** Requirement REV-6.3.9-02 in [ETSI EN 319 411-1] shall apply.

**[REQ 4.9.1-03]** If the subscriber changes its name, the CA shall immediately notify the subscriber that the certificate must be renewed within 120 days. If the certificate is not renewed, the CA shall revoke the certificate.

#### 4.9.2 Who Can Request Revocation

**[REQ 4.9.2-01]** The following parties may request revocation of a certificate:

- Subject
- Authorized person/entity
- The CA if the rules of this CP have not been complied with or if other circumstances so warrant

- The authorized signatory of the company against proper documentation
- Supervisor or trustee in bankruptcy if the subscriber has filed for suspension of payments or becomes subject to bankruptcy proceedings.

#### 4.9.3 Procedure for Revocation Request

[REQ 4.9.3-01] Requirement REV-6.2.4-09 in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.3-02] Requirement REV-6.3.9-03 in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.3-03] Requirement REV-6.3.9-04 in [ETSI EN 319 411-1] shall apply.

#### 4.9.4 Revocation Request Grace Period

N/A

#### 4.9.5 Time Within Which CA Must Process the Revocation Request

[REQ 4.9.5-01] Requirement REV-6.2.4-03A in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.5-02] Requirement REV-6.2.4-03BA in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.5-03] Requirement REV-6.2.4-03BB in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.5-04] Requirement REV-6.2.4-03C in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.5-05] Requirement REV-6.2.4-05A in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.5-06] Requirement REV-6.2.4-06A in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.5-07] Requirement REV-6.2.4-07 in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.5-08] Requirement REV-6.2.4-08 in [ETSI EN 319 411-1] shall apply.

#### 4.9.6 Revocation Checking Requirements for Relying Parties

N/A

#### 4.9.7 CRL Issuance Frequency

[REQ 4.9.7-01] Requirement CSS-6.3.9-05 in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.7-02] Requirement CSS-6.3.9-06 in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.7-03] Requirement CSS-6.3.9-07 in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.7-04] Requirement CSS-6.3.9-12 in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.7-05] Requirement CSS-6.3.9-13 in [ETSI EN 319 411-1] shall apply.

[REQ 4.9.7-06] Requirement CSS-6.3.9-14 in [ETSI EN 319 411-1] shall apply.

#### 4.9.8 Maximum Latency for CRLs

N/A

#### 4.9.9 On-Line Revocation/Status Checking Availability

[REQ 4.9.9-01] The CA should offer online status check via the Online Certificate Status Protocol, OCSP.

#### 4.9.10 On-Line Revocation Checking Requirements

N/A

#### 4.9.11 Other Forms of Revocation Advertisements Available

N/A

#### 4.9.12 Special Requirements related to Key Compromise

N/A

#### 4.9.13 Circumstances for Suspension

[REQ 4.9.13-01] A certificate issued under this CP must not be suspended.

#### 4.9.14 Who Can Request Suspension

N/A

#### 4.9.15 Procedure for Suspension Request

N/A

#### 4.9.16 Limits on Suspension Period

N/A

### 4.10 Certificate Status Services

#### 4.10.1 Operational Characteristics

[REQ 4.10.1-01] Requirement CSS-6.3.10-01 in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.1-02] Requirement CSS-6.3.10-01A in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.1-03] Requirement CSS-6.3.10-03 in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.1-04] Requirement CSS-6.3.10-08 in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.1-05] Requirement CSS-6.3.10-09 in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.1-06] Requirement CSS-6.3.10-09A in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.1-08] Requirement CSS-6.3.10-02A in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.1-09] [Q] Requirement CSS-6.3.10-07 in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.1-10] [Q] Requirement CSS-6.3.10-08 in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.1-11] [Q] Requirement CSS-6.3.10-09 in [ETSI EN 319 411-2] shall apply.

#### 4.10.2 Service Availability

[REQ 4.10.2-01] Requirement CSS-6.3.10-02 in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.2-02] Requirement CSS-6.3.10-10 in [ETSI EN 319 411-1] shall apply.

#### 4.10.3 Operational Features

[REQ 4.10.3-01] Requirement CSS-6.3.10-04 in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.3-02] Requirement CSS-6.3.10-05 in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.3-03] Requirement CSS-6.3.10-06 in [ETSI EN 319 411-1] shall apply.

[REQ 4.10.3-04] [Q] Requirement CSS-6.3.10-02 in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.3-05] [Q] Requirement CSS-6.3.10-03 in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.3-06] [Q] Requirement CSS-6.3.10-04 in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.3-07] [Q] Requirement CSS-6.3.10-10 in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.3-08] [Q] Requirement CSS-6.3.10-11 in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.3-09] [Q] Requirement CSS-6.3.10-12 in [ETSI EN 319 411-2] shall apply.

[REQ 4.10.3-10] [Q] Requirement CSS-6.3.10-13 in [ETSI EN 319 411-2] shall apply.

## 4.11 End of Subscription

N/A

## 4.12 Key Escrow and Recovery

### 4.12.1 Key Escrow and Recovery Policy and Practices

[REQ 4.12.1-01] Key escrow shall not be done for subject's keys.

### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices

N/A

# 5. Facility, Management, and Operational Controls

[REQ 5-01] All requirements in [ETSI EN 319 401] clause 5 “Risk Assessment” shall apply.

[REQ 5-02] Requirement REQ-7. 3.1-01 in [ETSI EN 319 401] shall apply.

[REQ 5-03] Requirement REQ-7.3.1-02X in [ETSI EN 319 401] shall apply.

## 5.1 Physical Controls

[REQ 5.1-01] Requirement REQ-7.6-03 in [ETSI EN 319 401] shall apply.

[REQ 5.1-02] Requirement REQ-7.6-04 in [ETSI EN 319 401] shall apply.

[REQ 5.1-03] All requirements in [ETSI EN 319 411-1] clause 6.4.2 “Physical security controls” shall apply.

### 5.1.1 Site Location and Construction

[REQ 5.1.1-01] Requirement REQ-7.6-05 in [ETSI EN 319 401] shall apply.

[REQ 5.1.1-02] The requirements in this CP apply regardless of whether the CA locates all or parts of the operating environment outside Denmark. This means that it must be possible to carry out the regular control set out in the CP regardless of where the CA is geographically located.

### 5.1.2 Physical Access

[REQ 5.1.2-01] Requirement REQ-7.6-01 in [ETSI EN 319 401] shall apply.

[REQ 5.1.2-02] Requirement REQ-7.6-02 in [ETSI EN 319 401] shall apply.

### 5.1.3 Power and Air Conditioning

See clause 5.1.

### 5.1.4 Water Exposures

See clause 5.1.

### 5.1.5 Fire Prevention and Protection

See clause 5.1.

### 5.1.6 Media Storage

[REQ 5.1.6-01] All requirements in [ETSI EN 319 401] clause 7.3.3 “Storage media handling” shall apply.

### 5.1.7 Waste Disposal

See clause 5.1.6.

### 5.1.8 Off-Site Backup

[REQ 5.1.8-01] If data is stored or processed at another location, the CA shall ensure that such storage or processing complies with the same security requirements as the CA's main systems.

## 5.2 Procedural Controls

[REQ 5.2-01] All requirements in [ETSI EN 319 401] clause 7.3.2 “Assets inventory and classification” shall apply.

[REQ 5.2-02] All requirements in [ETSI EN 319 411-1] clause 6.4.3 “Procedural controls” shall apply.

### 5.2.1 Trusted Roles

[REQ 5.2.1-01] Requirement REQ-7. 2-08X in [ETSI EN 319 401] shall apply.

[REQ 5.2.1-02] Requirement REQ-7.2-11X in [ETSI EN 319 401] shall apply.

[REQ 5.2.1-03] Requirement REQ-7.2-13X in [ETSI EN 319 401] shall apply.

[REQ 5.2.1-04] Requirement REQ-7.2-14X in [ETSI EN 319 401] shall apply.

[REQ 5.2.1-05] Requirement REQ-7.2-15X in [ETSI EN 319 401] shall apply.

[REQ 5.2.1-06] Requirement REQ-7.2-16X in [ETSI EN 319 401] shall apply.

[REQ 5.2.1-07] Requirement REQ-7.2-17 in [ETSI EN 319 401] shall apply.

### 5.2.2 Number of Persons Required per Task

See REQ 5.2-03.

### 5.2.3 Identification and Authentication for Each Role

See clause 5.2.1.

### 5.2.4 Roles Requiring Separation of Duties

[REQ 5.2.4-01] Requirement REQ-7.1.2-01 in [ETSI EN 319 401] shall apply.

## 5.3 Personnel Controls

[REQ 5.3-01] Requirement REQ-7.2-01X in [ETSI EN 319 401] shall apply.

[REQ 5.3-02] Requirement REQ-7.2-07X in [ETSI EN 319 401] shall apply.

[REQ 5.3-03] Requirement REQ-7.2-09X in [ETSI EN 319 401] shall apply.

[REQ 5.3-04] Requirement REQ-7.2-10X in [ETSI EN 319 401] shall apply.

[REQ 5.3-05] All requirements in [ETSI EN 319 411-1] clause 6.4.4 “Personnel controls” shall apply.

### 5.3.1 Qualifications, Experience, and Clearance Requirements

[REQ 5.3.1-01] Requirement REQ-7.2-02 in [ETSI EN 319 401] shall apply.

[REQ 5.3.1-02] Requirement REQ-7.2-03X in [ETSI EN 319 401] shall apply.

[REQ 5.3.1-03] Requirement REQ-7.2-12X in [ETSI EN 319 401] shall apply.

### 5.3.2 Background Check Procedures

See clause 6.6.3.

### 5.3.3 Training Requirements

[REQ 5.3.3-01] Requirement REQ-7. 2-04X in [ETSI EN 319 401] shall apply.

### 5.3.4 Retraining Frequency and Requirements

[REQ 5.3.4-01] Requirement REQ-7. 2-05X in [ETSI EN 319 401] shall apply.

### 5.3.5 Job Rotation Frequency and Sequence

N/A

### 5.3.6 Sanctions for Unauthorized Actions

[REQ 5.3.6-01] Requirement REQ-7. 2-05X in [ETSI EN 319 401] shall apply.

### 5.3.7 Independent Contractor Requirements

See clause 6.6.3.

### 5.3.8 Documentation Supplied to Personnel

N/A

## 5.4 Audit Logging Procedures

[REQ 5.4-01] All non-marked requirements in [ETSI EN 319 411-1] clause 6.4.5 “Audit logging procedures” shall apply.

[REQ 5.4-02] [Q] Requirement SDP-6.4.5-10 in [ETSI EN 319 411-1] shall apply.

[REQ 5.4-03] [Q] Requirement OVR-6.4.5-03 in [ETSI EN 319 411-2] shall apply.

### 5.4.1 Types of Events Recorded

See clause 5.4.

### 5.4.2 Frequency of Processing Log

See clause 5.4.

### 5.4.3 Retention Period for Audit Log

See clause 5.4.

### 5.4.4 Protection of Audit Log

See clause 5.4.

### 5.4.5 Audit Log Backup Procedures

See clause 5.4.

### 5.4.6 Audit Collection System (Internal vs. External)

N/A

### 5.4.7 Notification to Event-Causing Subject

N/A

### 5.4.8 Vulnerability Assessments

N/A

## 5.5 Records Archival

[REQ 5.5-01] Requirement REQ-7.10-01 in [ETSI EN 319 401] shall apply.

[REQ 5.5-02] All requirements in [ETSI EN 319 411-1] clause 6.4.6 “Records archival” shall apply.

### 5.5.1 Types of Records Archived

See clause 5.5.

### 5.5.2 Retention Period for Archive

[REQ 5.5.2-01] Requirement REQ-7.10-07 in [ETSI EN 319 401] shall apply.

### 5.5.3 Protection of Archive

[REQ 5.5.3-01] Requirement REQ-7.10-02 in [ETSI EN 319 401] shall apply.

[REQ 5.5.3-02] Requirement REQ-7.10-03 in [ETSI EN 319 401] shall apply.

[REQ 5.5.3-03] Requirement REQ-7.10-08 in [ETSI EN 319 401] shall apply.

### 5.5.4 Archive Backup Procedures

[REQ 5.5.4-01] All requirements in [ETSI EN 319 401] clause 7.11.2 “Back up” shall apply.

### 5.5.5 Requirements for Time-Stamping of Records

[REQ 5.5.5-01] Requirement REQ-7.10-05 in [ETSI EN 319 401] shall apply.

[REQ 5.5.5-02] Requirement REQ-7.10-06 in [ETSI EN 319 401] shall apply.

### 5.5.6 Archive Collection System (Internal or External)

N/A

### 5.5.7 Procedures to Obtain and Verify Archive Information

[REQ 5.5.7-01] Requirement REQ-7.10-04 in [ETSI EN 319 401] shall apply.

## 5.6 Key Changeover

[REQ 5.6-01] The CA must ensure that, before expiry of the private key, a new CA key pair is generated that can be utilized for issuance of certificates.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling Procedures

[REQ 5.7.1-01] All requirements in [ETSI EN 319 401] clause 7.9.1 “Monitoring and logging” shall apply.

[REQ 5.7.1-02] All requirements in [ETSI EN 319 401] clause 7.9.2 “Incident response” shall apply.

[REQ 5.7.1-03] All requirements in [ETSI EN 319 401] clause 7.9.3 “Reporting” shall apply.

[REQ 5.7.1-04] All requirements in [ETSI EN 319 401] clause 7.9.4 “Event assessment and classification” shall apply.

**[REQ 5.7.1-05]** All requirements in [ETSI EN 319 401] clause 7.9.5 “Post-incident reviews” shall apply.

**[REQ 5.7.1-06]** All requirements in [ETSI EN 319 411-1] clause 6.4.8 “Compromise and disaster recovery” shall apply.

## 5.7.2 Computing Resources, Software, and/or Data Are Corrupted

See clause 5.7.1.

## 5.7.3 Entity Private Key Compromise Procedures

See clause 5.7.1.

## 5.7.4 Business Continuity Capabilities After a Disaster

**[REQ 5.7.4-01]** All requirements in [ETSI EN 319 401] clause 7.11.1 “General” shall apply.

**[REQ 5.7.4-02]** All requirements in [ETSI EN 319 401] clause 7.11.3 “Crisis management” shall apply.

# 5.8 CA or RA Termination

**[REQ 5.8-01]** All requirements in [ETSI EN 319 401] clause 7.12 “TSP termination and termination plans” shall apply.

**[REQ 5.8-02]** All requirements in [ETSI EN 319 411-1] clause 6.4.9 “Certification Authority or Registration Authority termination” shall apply.

# 6. Technical Security Controls

[REQ 6-01] Requirement REQ-7.5-01X in [ETSI EN 319 401] shall apply.

## 6.1 Key Pair Generation and Installation

[REQ 6.1-01] All non-marked requirements in [ETSI EN 319 411-1] clause 6.5.1 “Key pair generation and installation” shall apply.

[REQ 6.1-02] [Q] Requirement SDP-6.5.1-23 in [ETSI EN 319 411-1] shall apply.

[REQ 6.1-03] [Q] Requirement SDP-6.5.1-02 in [ETSI EN 319 411-2] shall apply.

[REQ 6.1-04] [Q] Requirement SDP-6.5.1-03 in [ETSI EN 319 411-2] shall apply.

[REQ 6.1-05] [Q] Requirement SDP-6.5.1-04 in [ETSI EN 319 411-2] shall apply.

[REQ 6.1-06] [Q] Requirement SDP-6.5.1-05 in [ETSI EN 319 411-2] shall apply.

[REQ 6.1-07] [Q] Requirement SDP-6.5.1-06 in [ETSI EN 319 411-2] shall apply.

[REQ 6.1-08] [Q] Requirement SDP-6.5.1-07A in [ETSI EN 319 411-2] shall apply.

[REQ 6.1-09] [Q] Requirement SDP-6.5.1-07B in [ETSI EN 319 411-2] shall apply.

### 6.1.1 Key Pair Generation

[REQ 6.1.1-01] The certificate issuer's certificates shall be valid for at least 5 years.

### 6.1.2 Private Key Delivery to Subscriber

See clause 6.1.

### 6.1.3 Public Key Delivery to Certificate Issuer

See clause 6.1.

### 6.1.4 CA Public Key Delivery to Relying Parties

See clause 6.1.

### 6.1.5 Key Sizes

See clause 6.1.

### 6.1.6 Public Key Parameters Generation and Quality Checking

See clause 6.1.

### 6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

See clause 6.1.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

[REQ 6.2-01] All requirements in [ETSI EN 319 411-1] clause 6.5.2 "Private key protection and cryptographic module engineering controls" shall apply.

### 6.2.1 Cryptographic Module Standards and Controls

See clause 6.2.

### 6.2.2 Private Key (n out of m) Multi-Person Control

See clause 6.2.

### 6.2.3 Private Key Escrow

See clause 6.2.

### 6.2.4 Private Key Backup

See clause 6.2.

### 6.2.5 Private Key Archival

See clause 6.2.

### 6.2.6 Private Key Transfer Into or From a Cryptographic Module

See clause 6.2.

## 6.2.7 Private Key Storage on Cryptographic Module

See clause 6.2.

## 6.2.8 Method of Activating Private Key

See clause 6.2.

## 6.2.9 Method of Deactivating Private Key

N/A

## 6.2.10 Method of Destroying Private Key

See clause 6.2.

## 6.2.11 Cryptographic Module Rating

See clause 6.2.

# 6.3 Other Aspects of Key Pair Management

**[REQ 6.3-01]** All requirements in [ETSI EN 319 411-1] clause 6.5.3 “Other aspects of key pair management” shall apply.

## 6.3.1 Public Key Archival

N/A

## 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

N/A

# 6.4 Activation Data

**[REQ 6.4-01]** All requirements in [ETSI EN 319 411-1] clause 6.5.4 “Activation data” shall apply.

## 6.4.1 Activation Data Generation and Installation

See clause 6.4.

## 6.4.2 Activation Data Protection

See clause 6.4.

## 6.4.3 Other Aspects of Activation Data

See clause 6.4.

# 6.5 Computer Security Controls

**[REQ 6.5-01]** All requirements in [ETSI EN 319 411-1] clause 6.5.4 “Computer security controls” shall apply.

## 6.5.1 Specific Computer Security Technical Requirements

See clause 6.5.

## 6.5.2 Computer Security Rating

See clause 6.5.

# 6.6 Life Cycle Technical Controls

**[REQ 6.6-01]** Requirement REQ-7.7-01 in [ETSI EN 319 401] shall apply.

**[REQ 6.6-02]** Requirement REQ-7.7-03 in [ETSI EN 319 401] shall apply.

**[REQ 6.6-03]** Requirement REQ-7.7-04 in [ETSI EN 319 401] shall apply.

**[REQ 6.6-04]** Requirement REQ-7.7-05 in [ETSI EN 319 401] shall apply.

**[REQ 6.6-05]** Requirement REQ-7.7-06X in [ETSI EN 319 401] shall apply.

**[REQ 6.6-06]** All non-marked requirements in [ETSI EN 319 411-1] clause 6.5.6 “Life cycle security controls” shall apply.

**[REQ 6.6-07]** All requirements marked with “[NCP]” in [ETSI EN 319 411-1] clause 6.5.6 “Life cycle security controls” shall apply.

## 6.6.1 System Development Controls

**[REQ 6.6.1-01]** Requirement REQ-7.7-02 in [ETSI EN 319 401] shall apply.

## 6.6.2 Security Management Controls

**[REQ 6.6.2-01]** All requirements in [ETSI EN 319 401] clause 6.3 “Information security policy” shall apply.

**[REQ 6.6.2-02]** Requirement REQ-7.7-07X in [ETSI EN 319 401] shall apply.

**[REQ 6.6.2-03]** Requirement REQ-7.7-08X in [ETSI EN 319 401] shall apply.

**[REQ 6.6.2-04]** Requirement REQ-7.7-09X in [ETSI EN 319 401] shall apply.

**[REQ 6.6.2-05]** Requirement REQ-7.7-10X in [ETSI EN 319 401] shall apply.

## 6.6.3 Life Cycle Security Controls

**[REQ 6.6.3-01]** All requirements in [ETSI EN 319 401] clause 7.4 “Access control” shall apply.

**[REQ 6.6.3-02]** All requirements in [ETSI EN 319 401] clause 7.14.1 “Supply chain policy” shall apply.

**[REQ 6.6.3-03]** All requirements in [ETSI EN 319 401] clause 7.14.2 “Supply chain procedures and processes” shall apply.

**[REQ 6.6.3-04]** All requirements in [ETSI EN 319 401] clause 7.14.3 “Responsibility, third parties agreements and SLA” shall apply.

# 6.7 Network Security Controls

**[REQ 6.7-01]** Requirement REQ-7.2-18X in [ETSI EN 319 401] shall apply.

**[REQ 6.7-02]** Requirement REQ-7.2-19X in [ETSI EN 319 401] shall apply.

**[REQ 6.7-03]** All requirements in [ETSI EN 319 401] clause 7.8 “Network security” shall apply.

**[REQ 6.7-04]** All requirements in [ETSI EN 319 411-1] clause 6.5.7 “Network security controls” shall apply.

## 6.8 Time-Stamping

See clause 5.5.5

# 7. Certificate, CRL, and OCSP Profiles

## 7.1 Certificate Profile

[REQ 7.1-01] Requirement GEN-6.6.1-01 in [ETSI EN 319 411-1] shall apply.

[REQ 7.1-02] Requirement GEN-6.6.1-02 in [ETSI EN 319 411-1] shall apply.

[REQ 7.1-03] Requirement GEN-4.1-1 in [ETSI EN 319 412-2] shall apply.

[REQ 7.1-04] Requirement GEN-4.2.2-1 in [ETSI EN 319 412-2] shall apply.

[REQ 7.1-05] All requirements in [ETSI EN 319 412-2] clause 4.2.3 “Issuer” shall apply

### 7.1.1 Version Number(s)

[REQ 7.1.1-01] Requirement GEN-4.2.1-1 in [ETSI EN 319 412-2] shall apply.

### 7.1.2 Certificate Extensions

[REQ 7.1.2-01] Requirement CSS-6.3.10-01B in [ETSI EN 319 411-1] shall apply.

[REQ 7.1.2-02] [Q] Requirement CSS-6.3.10-02B in [ETSI EN 319 411-2] shall apply.

[REQ 7.1.2-03] Requirement GEN-6.6.1-03 in [ETSI EN 319 411-1] shall apply.

[REQ 7.1.2-04] Requirement GEN-6.6.1-04 in [ETSI EN 319 411-1] shall apply.

[REQ 7.1.2-05] Requirement GEN-6.6.1-05 in [ETSI EN 319 411-1] shall apply.

[REQ 7.1.2-06] [Q] Requirement GEN-6.6.1-02 in [ETSI EN 319 411-2] shall apply.

[REQ 7.1.2-07] [Q] Requirement GEN-6.6.1-03 in [ETSI EN 319 411-2] shall apply.

[REQ 7.1.2-08] [OCES] Requirement GEN-6.6.1-04 in [ETSI EN 319 411-2] shall apply.

[REQ 7.1.2-09] [Q] Requirement GEN-6.6.1-05 in [ETSI EN 319 411-2] shall apply.

[REQ 7.1.2-10] [Q] Requirement GEN-6.6.1-07 in [ETSI EN 319 411-2] shall apply.

[REQ 7.1.2-11] [POCES] [MOCES] [QP] [QE] Requirement GEN-5.1.2-01 in [ETSI EN 319 412-1] shall apply where the semantic identifier shall be id-etsi-qcs-semanticsId-Natural and the nameRegistrationAuthorities shall be <https://uid.gov.dk> of type URI general-Name.

[REQ 7.1.2-12] [VOCES] [QO] Requirement GEN-5.1.2-01 in [ETSI EN 319 412-1] shall apply where the semantic identifier shall be id-etsi-qcs-SemanticsId-Legal and the nameRegistrationAuthorities shall be <https://uid.gov.dk> of type URI general-Name.

[REQ 7.1.2-13] Requirement GEN-5.2.3-01 in [ETSI EN 319 412-1] shall apply for Validity Assured Certificates.

[REQ 7.1.2-14] Requirement GEN-4.3.1-1 in [ETSI EN 319 412-2] shall apply.

[REQ 7.1.2-15] Requirement NAT-4.3.2-1 in [ETSI EN 319 412-2] shall apply.

[REQ 7.1.2-16] [POCES] [MOCES] [QP] [QE] Requirement NAT-4.3.2-2 in [ETSI EN 319 412-2] shall apply.

[REQ 7.1.2-17] [POCES] [MOCES] [QP] [QE] Requirement NAT-4.3.2-3 in [ETSI EN 319 412-2] shall apply.

**[REQ 7.1.2-18]** [VOCES] [QO] Requirement LEG-4.3.1-3 in [ETSI EN 319 412-3] shall apply.

**[REQ 7.1.2-19]** [VOCES] [QO] Requirement LEG-4.3.1-4 in [ETSI EN 319 412-3] shall apply.

**[REQ 7.1.2-20]** All requirements in [ETSI EN 319 412-2] clause 4.3.3 “Certificate policies” through clause 4.3.12 “Inhibit any-policy” shall apply.

**[REQ 7.1.2-21]** All requirements in [ETSI EN 319 412-2] clause 4.4.1 “Authority Information Access” shall apply.

**[REQ 7.1.2-22]** [QP] [QE] [QO] All requirements in [ETSI EN 319 412-2] clause 5.1 “EU QCStatements” shall apply.

**[REQ 7.1.2-23]** [QP] [QE] [QO] All requirements in [ETSI EN 319 412-2] clause 5.2 “Certificate policies” shall apply.

### 7.1.3 Algorithm Object Identifiers

**[REQ 7.1.3-01]** Requirement GEN-4.2.5-1 in [ETSI EN 319 412-2] shall apply.

### 7.1.4 Name Forms

**[REQ 7.1.4-01]** [POCES] [QP] The subject field shall include the following attributes as specified in Recommendation ITU-T X.520

- countryName;
- choice of (givenName and surname) or pseudonym;
- commonName and
- serialNumber

**[REQ 7.1.4-02]** [MOCES] [QE] The subject field shall include the following attributes as specified in Recommendation ITU-T X.520

- countryName;
- choice of (givenName and surname) or pseudonym;
- commonName;
- serialNumber;
- organizationName and
- organizationIdentifier

**[REQ 7.1.4-03]** [VOCES] [QO] The subject field shall include the following attributes as specified in Recommendation ITU-T X.520

- countryName;
- commonName;
- serialNumber;
- organizationName and
- organizationIdentifier

**[REQ 7.1.4-04]** Only one instance of each of the attributes above shall be present. Additional attributes may be present.

**[REQ 7.1.4-05]** The pseudonym attribute shall not be present if the givenName and/or surname attribute are present.

**[REQ 7.1.4-06]** [POCES] [MOCES] [QP] [QE] Requirement NAT-4.2.4-12A in [ETSI EN 319 412-2] shall apply.

**[REQ 7.1.4-07]** [POCES] [MOCES] [QP] [QE] Requirement NAT-4.2.4-12A in [ETSI EN 319 412-2] shall apply.

**[REQ 7.1.4-08]** countryName in end user certificates shall have the value "DK".

**[REQ 7.1.4-09]** serialNumber shall have the following semantics:

UI:DK-xxxxxxxxxxxx..xx,

where "xxxxxxxxxxxx..xx" is the subjects UUID registered in The Agency for Digital Government's UUID numbering service and shall assure that it is sufficient to resolve any subject name collisions.

**[REQ 7.1.4-10]** The commonName shall contain a name of the subject. This can be the subject's or CA's preferred format for the name. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used.

**[REQ 7.1.4-11]** Requirement NAT-4.2.4-18 in [ETSI EN 319 412-2] shall apply.

**[REQ 7.1.4-12]** Requirement LEG-4.2.1-9 in [ETSI EN 319 412-3] shall apply.

**[REQ 7.1.4-13]** Requirement NAT-4.2.4-19 in [ETSI EN 319 412-2] shall apply.

**[REQ 7.1.4-14]** Requirement NAT-4.2.4-20 in [ETSI EN 319 412-2] shall apply.

**[REQ 7.1.4-15]** [MOCES] [VOCES] [QE] [QO] Requirement LEG-4.2.1-5 in [ETSI EN 319 412-3] shall apply but business forms in the name e.g. "ApS" or "Fonden" can be omitted.

**[REQ 7.1.4-16]** [MOCES] [VOCES] [QE] [QO] The organizationIdentifier shall have the following semantics:

NTRDK-xxxxxxx,

where "xxxxxxx" is the subjects CVR number registered in Danish Central Business Register, CVR.

## 7.1.5 Name Constraints

**[REQ 7.1.5-01]** Requirement OVR-5.2-11 in [ETSI EN 319 411-1] shall apply.

## 7.1.6 Certificate Policy Object Identifier

**[REQ 7.1.6-01]** All certificates issued under this CP shall refer to this CP by stating the relevant OID from clause 1.2.2 in the certificatePolicies extension.

**[REQ 7.1.6-02]** [OCES] OCES related OIDs may only be referenced in a certificate or written agreement with the Danish Agency for Digital Government, cf. clause 1.1.

**[REQ 7.1.6-03]** [QP] [QE] Qualified certificates issued to natural persons under this CP shall refer to QCP-n-qscd by stating OID:

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)

in certificatePolicies extension.

**[REQ 7.1.6-04]** [Q0] Qualified certificates issued to legal persons under this CP shall refer to QCP-I-qscd by stating OID:

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

in certificatePolicies extension.

**[REQ 7.1.6-05]** [OCES] OCES certificates issued under this CP shall refer to NCP by stating OID:

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)

in certificatePolicies extension.

## 7.1.7 Usage of Policy Constraints Extension

See clause 7.1.2.

## 7.1.8 Policy Qualifiers Syntax and Semantics

N/A

## 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

N/A

# 7.2 CRL Profile

**[REQ 7.2-01]** Requirement GEN-6.6.2-01 in [ETSI EN 319 411-1] shall apply.

**[REQ 7.2-02]** Requirement CSS-6.3.9-08 in [ETSI EN 319 411-1] shall apply.

**[REQ 7.2-03]** thisUpdate and nextUpdate shall be stated in UTCTime format YYMMDDHHMMSSz.

## 7.2.1 Version Number(s)

**[REQ 7.2.1-01]** The CRL's version number(s) shall be stated and provided as 'v2' (0x1).

## 7.2.2 CRL and CRL Entry Extensions

**[REQ 7.2.2-01]** [Q] Requirement CSS-6.3.10-05 in [ETSI EN 319 411-2] shall apply.

**[REQ 7.2.2-02]** [Q] Requirement CSS-6.3.10-06 in [ETSI EN 319 411-2] shall apply.

# 7.3 OCSP Profile

**[REQ 7.3-01]** All requirements in [ETSI EN 319 411-1] clause 6.6.3 "OCSP profile" shall apply.

## 7.3.1 Version Number(s)

**[REQ 7.3.1-01]** The OCSP responder shall support version number 'v1' (0x0).

## 7.3.2 OCSP Extensions

See clause 7.3

# 8. Compliance Audit and Other Assessments

[REQ 8-01] Requirement REQ-7.13-01 in [ETSI EN 319 401] shall apply.

[REQ 8-02] Requirement REQ-7.13-02 in [ETSI EN 319 401] shall apply.

[REQ 8-03] [OCES] The CA except for the Danish State acting as CA shall enter into an OCES agreement with the Agency of Digital Government before issuing OCES certificates.

## 8.1 Frequency and Circumstances of Assessment

[REQ 8.1-01] Regular, documented internal system audits of the CA's overall system shall be undertaken.

[REQ 8.1-02] [OCES] An external conformity assessment shall be undertaken of the CA's overall system by a conformity assessment body, cf. REQ 8.2-01, at least once a year.

## 8.2 Identity/Qualifications of Assessor

[REQ 8.2-01] [OCES] The CA shall select an external conformity assessment body for undertaking the assessment at the CA. The conformity assessment body must either be a conformity assessment body defined in eIDAS article 3 letter 18) or a state-authorised auditor that can document to the Danish Agency for Digital Government that it possesses the requisite resources to perform an adequate system audit of the CA. The Danish Agency for Digital Government may in special circumstances grant an exemption from the requirement that the conformity assessment body must be a state-authorised auditor. The CA must at the latest one month after selection of the conformity assessment body report this to the Danish Agency for Digital Government.

[REQ 8.2-02] [OCES] The CA must make the selected conformity assessment body aware that in accordance with good auditing practices must perform system audits, including making sure that:

- The CA's systems are in compliance with the requirements in this CP.
- The CA's security, checking and auditing needs are addressed to a sufficient scope by development, maintenance and operation of the CA's systems.
- The CA's business procedures, both IT-based as well as manual procedures, are reliable as regards security and checking considerations and in accordance with the CA's CPS.

System audits may use the audit instructions for public certificate policies published by the Danish Agency for Digital Government if available.

[REQ 8.2-03] [OCES] The CA must make the selected conformity assessment body aware that it is obligated to report a condition or the conditions to the Danish Agency for Digital Government if the conformity assessment body continues to be of the opinion, that significant weaknesses or irregularities are occurring. The CA must in addition make the conformity assessment body aware that upon inquiry by the Danish Agency for Digital Government it is obligated to give information on the CA's circumstances that have or may have an influence on the CA's administration of its task as the issuer of OCES certificates, without prior acceptance by the CA. The conformity assessment body is however obligated to orient the CA on the inquiry.

**[REQ 8.2-04]** [OCES] The Danish Agency for Digital Government may order the CA to within an established deadline select a new conformity assessment body if the functioning conformity assessment body is found to be obviously unsuited for its duties.

**[REQ 8.2-05]** [OCES] Upon changing the conformity assessment body, the CA and the withdrawing conformity assessment bodies must each give an explanation to the Danish Agency for Digital Government.

## 8.3 Assessor's Relationship to Assessed Entity

**[REQ 8.3-01]** [OCES] The selected conformity assessment body shall co-operate with the internal assessment function at the CA.

## 8.4 Topics Covered by Assessment

**[REQ 8.4-01]** [OCES] The CA must deliver the information that is necessary for the system audit at the CA. In this regard the CA must give the conformity assessment body access to the management records.

**[REQ 8.4-02]** [OCES] The CA must give the selected conformity assessment body access to management meetings during the processing of matters that are of significance to the system audit. What is to be understood by a management meeting is a meeting of the senior management of the CA, in practice often called a board meeting. What is to be understood in this context by the expression 'the CA's management' is the senior management of the CA, i.e. the board or an equivalent management body depending upon how the CA has been organized. The CA must ensure that the selected conformity assessment body participates in the processing of applicable matters, if it is desired by just one management member.

**[REQ 8.4-03]** [OCES] At CAs where an annual general assembly is held, the provisions of the Danish Company Accounts Act concerning the auditor's obligation to answer questions at a company's annual general meeting applies equivalently for the selected conformity assessment body.

**[REQ 8.4-04]** [OCES] The CA must be able to document its fulfilment of the applicable legal requirements. Particularly in respect of eIDAS, GDPR and the Danish Data Protection Act.

## 8.5 Actions Taken as a Result of Deficiency

**[REQ 8.5-01]** [OCES] To the extent that the selected conformity assessment body discovers significant weaknesses or irregularities, the CA's management shall consider the matter at its next meeting and within a reasonable time period.

## 8.6 Communications of Results

**[REQ 8.6-01]** [OCES] The CA and the conformity assessment body shall immediately inform the Danish Agency for Digital Government about any matters that are decisive to the CA's continued operations.

**[REQ 8.6-02]** [OCES] At least once a year, the selected conformity assessment body will prepare a report for the CA's management.

**[REQ 8.6-03]** [OCES] This report shall include declarations as to whether

- the assessment has been carried out in accordance with generally accepted auditing practice;

- the selected conformity assessment body complies with the competency requirements given under the law;
- the selected conformity assessment body has been given all the information it has requested;
- the stated assessment tasks have been undertaken in accordance with the requirements of this CP, including whether there are any matters that have given rise to significant remarks and
- the overall data, system and operational security should be considered as adequate.

# 9. Other Business and Legal Matters

## 9.1 Fees

### 9.1.1 Certificate Issuance or Renewal Fees

N/A

### 9.1.2 Certificate Access Fees

N/A

### 9.1.3 Revocation or Status Information Access Fees

N/A

### 9.1.4 Fees for Other Services

**[REQ 9.1.4-01]** The CA shall defray all expenses related to system auditing, also including any system auditing ordered by the Danish Agency for Digital Government.

### 9.1.5 Refund Policy

N/A

## 9.2 Financial Responsibility

**[REQ 9.2-01]** Requirement REQ-7.1.1-04 in [ETSI EN 319 401] shall apply.

**[REQ 9.2-02]** Requirement REQ-7.1.1-05 in [ETSI EN 319 401] shall apply.

### 9.2.1 Insurance Coverage

**[REQ 9.2.1-01]** [OCES] If the CA is a private enterprise or a natural person, the CA shall subscribe to and maintain liability insurance. Such insurance shall as a minimum provide a coverage of DKK 25 million per year.

### 9.2.2 Other Assets

N/A

### 9.2.3 Insurance or Warranty Coverage for End-Entities

See clause 9.2.1.

## 9.3 Confidentiality of Business Information

### 9.3.1 Scope of Confidential Information

N/A

### 9.3.2 Information Not Within the Scope of Confidential Information

N/A

### 9.3.3 Responsibility to Protect Confidential Information

N/A

## 9.4 Privacy of Personal Information

### 9.4.1 Privacy Plan

**[REQ 9.4.1-01]** Requirement REQ-7.13-05 in [ETSI EN 319 401] shall apply.

**[REQ 9.4.1-02]** All requirements in [ETSI EN 319 411-1] clause 6.8.4 “Privacy of personal information” shall apply.

### 9.4.2 Information Treated as Private

N/A

### 9.4.3 Information Not Deemed Private

N/A

### 9.4.4 Responsibility to Protect Private Information

N/A

### 9.4.5 Notice and Consent to Use Private Information

**[REQ 9.4.5-01]** Retention time of personal data, cf. clause 5.5.2, shall be specified as part of the CA's terms and conditions.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

N/A

### 9.4.7 Other Information Disclosure Circumstances

N/A

## 9.5 Intellectual Property rights

**[REQ 9.5-01]** The Danish Agency for Digital Government holds all rights to this certificate policy, the OCES name and OCES-OID. Use of OCES-OID for other parties in certificates and use of the designation OCES in connection with issuance of certificates is only permitted pursuant to a written agreement with the Danish Agency for Digital Government.

## 9.6 Representations and Warranties

**[REQ 9.6-01]** All requirements in [ETSI EN 319 411-1] clause 6.8.6 “Representations and warranties” shall apply.

### 9.6.1 CA Representations and Warranties

**[REQ 9.6.1-01]** The CA shall in respect of any party reasonably relying on the certificate accept liability according to the general rules of Danish law.

**[REQ 9.6.1-02]** [OCES] The CA shall also accept liability for the loss of subscribers and relying parties, who reasonably rely on the certificate when such loss is due to:

- the information specified in the certificate not being correct at the time of its issuance;
- the certificate not containing all information as required in clause 7.1;
- failure to revoke the certificate, cf. clause 4.9;
- lack of or wrong information about revocation of the certificate, the expiry date of the certificate or whether the certificate contains purpose or amount restrictions, cf. clause 4.10 or 7.1; or
- the CA's non-observance of the requirements in clause 3.2, clause 3.3, clause 3.4 and clause 6.1.

unless the CA can establish that the CA has not acted negligently or willfully.

## 9.6.2 RA Representations and Warranties

N/A

## 9.6.3 Subscriber Representations and Warranties

N/A

## 9.6.4 Relying Party Representations and Warranties

N/A

## 9.6.5 Representations and Warranties of Other Participants

N/A

## 9.7 Disclaimers of Warranties

N/A

## 9.8 Limitations of Liability

**[REQ 9.8-01]** The CA is entitled to try to limit its liability in the relationship between itself and its co-contractors to the extent that such co-contractors are businesses or public authorities. Accordingly, the CA is not entitled to try to limit its liability in relation to private citizens who are co-contractors.

**[REQ 9.8-02]** The CA is also entitled to disclaim liability to co-contractors for any loss described in article 13(2) of the eIDAS Regulation.

## 9.9 Indemnities

N/A

## 9.10 Term and Termination

### 9.10.1 Term

**[REQ 9.10.1-01]** [Q] Requirement OVR-6.9.4-03 in [ETSI EN 319 411-2] shall apply.

**[REQ 9.10.1-02]** [Q] Requirement OVR-6.9.4-04 in [ETSI EN 319 411-2] shall apply.

### 9.10.2 Termination

N/A

### 9.10.3 Effect of Termination and Survival

N/A

## 9.11 Individual Notices and Communications with Participants

[REQ 9.11-01] The CA shall ensure that policies and procedures are in place to handle customer inquiries and inquiries from relying parties.

## 9.12 Amendments

### 9.12.1 Procedure for Amendment

N/A

### 9.12.2 Notification Mechanism and Period

N/A

### 9.12.3 Circumstances Under Which OID Must be Changed

N/A

## 9.13 Dispute Resolution Provisions

[REQ 9.13-01] Requirement REQ-7.1.1-06 in [ETSI EN 319 401] shall apply.

[REQ 9.13-02] Requirement REQ-6.8.13-01 in [ETSI EN 319 411-1] shall apply.

## 9.14 Governing Law

[REQ 9.14-01] [OCES] If a dispute cannot be resolved out of court, either party may choose to bring the dispute before the ordinary courts of law. The venue is the City of Copenhagen. Subject to Danish law.

## 9.15 Compliance with Applicable Law

[REQ 9.15-01] Requirement REQ-6.8.15-01 in [ETSI EN 319 411-1] shall apply.

## 9.16 Miscellaneous Provisions

### 9.16.1 Entire Agreement

N/A

### 9.16.2 Assignment

N/A

### 9.16.3 Severability

N/A

#### 9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

N/A

#### 9.16.5 Force Majeure

N/A

### 9.17 Other Provisions

#### 9.17.1 Disabilities

[REQ 9.17.1-01] Requirement REQ-7.13-03 in [ETSI EN 319 401] shall apply.

[REQ 9.17.1-02] Requirement REQ-7.13-04 in [ETSI EN 319 401] shall apply.

#### 9.17.2 Organizational

[REQ 9.17.2-01] All requirements in [ETSI EN 319 411-1] clause 6.9.1 “Organizational” shall apply.

#### 9.17.3 Additional testing

[REQ 9.17.3-01] All requirements in [ETSI EN 319 411-1] clause 6.9.2 “Additional testing” shall apply.

