DIGITALISERINGSSTYRELSEN

Certificate Policy for OCES organizational certificates (Public Certificates for Electronic Services)

October 2019

Version 7.0

Contents

1. Introduction

This Certificate Policy (CP) has been produced by and is administered by the Danish Agency for Digitisation. The Danish Agency for Digitisation is a public authority that authorizes the issuance of OCES certificates to the selected certification authorities (CAs) and which authorizes the CAs in relation to the agency and subordinate CPs. The Danish Agency for Digitisation is also responsible for the content of this CP. The latest version of this CP and any previous versions, under which valid certificates still exist, are available on https://certifikat.gov.dk.

Advanced electronic signature and advanced electronic 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). OCES constitutes such a PKI. OCES means Public Certificates for Electronic Services. The Danish Agency for Digitisation has produced a set of OCES certificate policies, one for employee and business certificates, respectively. Historically, certificates have been issued to private persons through OCES CP for person certificates that are no longer used. As of version 7.0, OCES CP for business certificates and functional certificates have been combined under OCES CP for business certificates to simplify the OCES structure.

Together with qualified CPs, OCES CPs constitute a common public standard regulating the issuance and use of certificates for electronic signatures and electronic seals.

The requirements in the OCES CPs are in accordance with the requirements for *Normalized Certificate Policy*, abbreviated NCP, cf. the European standards ETSI EN 319 401 and ETSI EN 319 411-1. The OCES CPs does not address qualified certificates issued under the eIDAS regulation. A mapping of the requirements from this CP to ETSI EN 319 401 and ETSI EN 319 411-1 and is available in Annex A.

The requirements of this CP include:

1. Mandatory requirements which must be met. Such requirements use the term ‘shall/must’.
2. Requirements describing prohibitions in relation to the 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’.

Note that this English version is a courtesy translation, which might not be 100% accurate. In case of doubt, the Danish version should be regarded as the authoritative source.

1.1 Overview

This certificate policy outlines the general guidelines applicable to the issuance of

an OCES certificate, OCES being an abbreviation of Public Certificate for Electronic Services.

The basis of the CP is 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 ensure a high level of assurance that the subject has the identity specified in the certificate.

A certificate is only an OCES business certificate if it is issued according to a CP for OCES business certificates and is issued by a CA which is approved by the Danish Agency for Digitisation as issuer of OCES certificates. As part of the verification, a formal agreement is made between the CA and the Danish Agency for Digitisation in which the CA accepts to comply with the requirements of this CP, including requirements about auditing of the CA's discharge of its duties, cf. also clause 8.

This means that the trust of the subscriber and relying parties can be based on the certificate policy, the Danish Agency for Digitisation's approval of the CA and the agency's ongoing supervision.

Certification authorities that may issue OCES certificates are available on the website: https://certifikat.gov.dk.

1.2 Document name and identification

1.2.1 Naming

This document named "Certificate policy for OCES business certificates (Public Certificates for Electronic Services) version 7.0" abbreviated VOCES-CP describes the certificate policy for OCES business certificates.

1.2.2 Identification

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

OCES business certificate.

Iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) cp(1) nq(1) business(3) ver(7)

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

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] The CA organization must be reliable.

[REQ 1.3.1-02] The CA shall be a natural person or legal entity.

[REQ 1.3.1-03] The CA may make use of other parties to provide parts of the certification service. However, the CA always maintains overall responsibility and ensures that the policy requirements identified in the CA are met.

A PKI may include a hierarchy of CAs with the highest CA in the hierarchy being named the root CA. A root CA has a self-issued certificate named root certificate with a related key pair named public root key and private root key, respectively.

[REQ 1.3.1-04] The CA may sub-certify its public OCES root key under other parent CAs. The OCES root key of a CA may also sub-certify the public key of another subordinate CA if it is verified for OCES. The Root CA is responsible for ensuring that any subordinate CA complies with relevant OCES CPs.

The services required to issue and maintain certificates can be divided into the following:

- Registration: Verification of the identity and any related ID and registration data of the subject. The result of the registration is transferred to the certificate generation. This function is undertaken by the RA on behalf of the CA.
- Certificate generation: Generation and electronic signing of certificates based on the verified identity and any other ID and registration data from the registration. Certificate generation includes issuance, re-key and renewal of certificates
- Certificate distribution: Distribution of certificates to subjects.
- Catalogue service: Release of certificates, allowing relying parties to access the certificates.
- Publication of business terms etc.: Publication of terms and rules, including CP and CPS.
- Revocation of certificates: Receipt and processing of requests for revocation of certificates.
- Publication of revocation information: Publication of status information for certificates.

1.3.2 Registration authorities

The registration authorities (RA) undertakes 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. 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.

[REQ 1.3.2-01] The CA shall ensure that the RA:

- verifies the applicant's identity and details and
- maintains a technical operating environment conforming to the requirements of this CP.

Note: The CA shall ensure only that the part of the RA's technical operating environmental which is related to the CA's service is maintained in conformity with the requirements of this CP. This includes terminals used for the registration of subjects, but not operating assets that do not influence the RA's services for the CA.

1.3.3 Subscribers

Prior to the issuance of certificates, the CA enters into an agreement with the subscriber in its capacity as the business (legal entity) which wants certificates for natural persons or logical entities associated with the subscriber. The entity associated with the subscriber who is registered and to whom a certificate is issued is named the subject.

This CP uses the terms subscriber and subject to distinguish between the entity entering into an agreement with a CA and the natural person or logical 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 handles 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

CAs issuing certificates under this CP are trust service providers, cf. eIDAS, and are in this context covered by supervision as described in eIDAS Chapter III. In Denmark, the Danish Agency for Digitisation is the supervisory authority in relation to eIDAS.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

[REQ 1.4.1-01] An OCES business certificate may be used to secure sender and message authenticity, including electronic seal 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 certificates are not qualified certificates, i.e. they must not be used in situation 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] The subject's private key must not be used without being authorized in each individual case by the subject.

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

1.5 Policy administration

1.5.1 Organization administering the document

This CP is owned and maintained by the Danish Agency for Digitisation.

1.5.2 Contact person

Inquiries regarding this CP can be addressed to:

The Danish Agency for Digitisation

Landgreven 4

DK-1301 Copenhagen K

Telephone: +45 3392 5200

Email: digst@digst.dk

1.5.3 Entity determining CPS suitability for the policy

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

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

[REQ 1.5.3-02] An updated CA report must be submitted once a year to the Danish Agency for Digitisation. The report must be submitted three months after the end of the CA's accounting year at the latest. The period of the report must follow the accounting year of the CA.

[REQ 1.5.3-03] 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 the CA's liability.

[REQ 1.5.3-04] The report and its content must be in Danish. According to clause 1.5.4, however, the CPS may be in Danish or English. The Danish Agency for Digitisation may grant an exemption for this requirement.

1.5.4 CPS approval procedures

[REQ 1.5.4-01] The CA shall prepare a Certification Practice Statement (CPS) addressing all requirements of this CP. The CPS must also include all external organizations supporting the CA's service and must be in compliance with this CP. The CPS may be divided into a public and private part, with the public part of the CPS being published.

Note: External organizations in the above requirements include any subcontractors, including external RA.

[REQ 1.5.4-02] The CPS must be designed with a view to allowing specific measurements of efficiency, quality and security on an ongoing basis.

[REQ 1.5.4-03] The CPS shall include the complete CA hierarchy, including root and subordinate CAs.

[REQ 1.5.4-04] The CPS must be structured according to the guidelines in RFC 3647.

[REQ 1.5.4-05] The CPS must be in Danish or English.

[REQ 1.5.4-06] The CPS must describe the signature algorithms used and related parameters in the public part. Moreover, the public part of the CPS must describe the practice regarding the use of CA keys for signing certificates, CRL and OCSP.

[REQ 1.5.4-07] The management of the CA shall be responsible for and approve the entire CPS and ensure correct implementation, including that the CPS is communicated to relevant employees and partners.

[REQ 1.5.4-08] The CPS must be reviewed and revised on a regular basis at least once a year. The responsibility for maintaining the CPS must be determined and documented. Changes in the CPS must be documented.

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 subscriber 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 issuing 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 provisions 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 they key securely on a cryptographic hardware module where the activation of the key is based on something only held and known by the subject.

ISO 27001: "ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems" as well as subsequent amendments such as Cor 1:2014 and Cor 2:2015.

ISO 27002: "ISO/IEC 27002:2013 - Information technology -- Security techniques – Code of practice for information security controls" as well as subsequent amendments such as Cor 1:2014 and Cor 2:2015.

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.

Cryptographic module: Hardware unit which independently of the operating system can generate and store keys and use the digital signature. The unit must be certified according to FIPS 140-2 level 3, CWA 14167-3 or SSCD-PP Type 3.

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
eIDAS	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
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
VOCES	Business 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
RA	Registration Authority
UTC	Universal Time Coordinated
UUID	Universally Unique Identifier

2. Publication and repository responsibilities

2.1 Repositories

[REQ 2.1-01] The CA practice shall at all times comply with the wording of the CPS.

[REQ 2.1-02] The CA shall make the public part of the applicable CPS available on the CA's website on a 24/7 basis.

[REQ 2.1-03] TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties. Terms and conditions shall at least specify:

a) A description of the service,

b) the CPs being applied by the service,

c) any limitations on the use of the service,

d) the obligations of relying parties,

e) the period of time during which event logs are retained,

f) limitations of liability,

g) limitations on the use of service, including the CA's limitation of liability in terms of wrong use of the service,

h) the applicable legal system,

i) dispute procedures,

j) the fact that the CA has been approved by the Danish Agency for Digitisation as issuer of OCES certificates,

k) The CA's contact information, and

l) any undertaking regarding availability.

[REQ 2.1-04] Moreover, the terms of conditions for subscribers shall include:

m) specification of what constitutes certificate acceptance, cf. clause 4.4.1, and that the private key must not be used

- until the certificate has been accepted by the subscriber, except for use that forms part of the certificate application process or
- after the subscriber suspects that the private key has been compromised, except for use for authenticating in connection with a request for revocation of an associated certificate and decryption of data encrypted by the associated public key,

n) indication of the period of time for which the records are retained,

o) the subscribers' obligations, cf. clause 4.5.1.

p) information for relying parties, cf. clause 4.5.2 and

q) information about certificate validity period.

[REQ 2.1-05] The CA shall in particular notify relying parties that the relying parties, prior to trusting a certificate, must ensure:

- that the certificate is valid and has not been revoked - i.e. is not listed on the CA's CRL,
- that the purpose for which the certificate is to be used is suitable in respect of any use limitations in the certificate and
- that the use of the certificate in general is suitable in terms of the level of security as described in this CP.

[REQ 2.1-06] Terms and conditions shall be made available through a durable means of communication.

[REQ 2.1-07] Terms shall be formulated in a readily understandable language and shall be available 24 hours per day, 7 days per week. Upon system failure or other factors which are not under the control of the CA, the CA apply best endeavours

to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the public part of the CPS.

[REQ 2.1-08] Terms and conditions may be transmitted electronically.

2.2 Publication of certification information

[REQ 2.2-01] The CA shall make issued certificates available to subjects, subscribers and relying parties until at least two months after the expiry of the validity period of the specific certificate. However, certificates must only be available to third parties if the subscriber has consented to their publication.

[REQ 2.2-02] After issuance, the complete and accurate certificate shall be made available to the subject for whom the certificate is being issued.

[REQ 2.2-03] The CA shall make the following types of information available to all:

- The CA's root certificate.
- The CA's subordinate CA certificates.
- This CP for as long as valid certificates are issued under this CP and for as long as certificates exists on the CRL for this CP.
- CRL for certificates issued under this CP.

Note: The CA may make the CP available via a link to the Danish Agency for Digitisation's publication of CPs.

[REQ 2.2-04] CRL information shall be provided without any kind of access control.

[REQ 2.2-05] The CA shall ensure that the requirements that the CA imposes on the subscriber and relying party based on this CP are extracted and documented, cf. clauses 6.2 and 6.3.

2.3 Time or frequency of publication

[REQ 2.3-01] The CA's public part of the CPS shall be published immediately after approval.

2.4 Access controls on repositories

[REQ 2.4-01] The CA must not limit access to the public part of the CPS and terms for using the services, and the CPS and terms must be made internationally available.

3. Identification and authentication

3.1 Naming

3.1.1 Types of names

[REQ 3.1.1-01] 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 an identifiable physical or logical entity at the subscriber. In this connection, the subject may be located elsewhere than at the subscriber, e.g. at an operation supplier.

3.1.2 Need for names to be meaningful

[REQ 3.1.2-01] 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 replaced unless this causes obvious misunderstandings, and long names may be abbreviated unless this causes obvious misunderstandings.

[REQ 3.1.2-02] The name of the subject shall be meaningful to all relevant relying parties in terms of the physical or logical entity being identified.

[REQ 3.1.2-03] The subject's name must not be of a nature that may cause obvious misunderstandings and must not be identical or confusingly similar to a trademark. Moreover, the CA may reject the use of pseudonym.

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

3.1.3 Anonymity or pseudonymity of subscribers

N/A

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 serialNumber in subject distinguishedName.

3.1.6 Recognition, authentication, and role of trademarks

N/A

3.2 Initial identity validation

[REQ 3.2-01] The CA shall verify the identity of the subscriber and check that the certificate applications are accurate, authorized and complete according to the collected evidence or attestation of identity.

[REQ 3.2-02] The CA shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.

[REQ 3.2-03] The CA shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.

[REQ 3.2-04] The CA's verification policy may only collect data for evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

[REQ 3.2-05] To avoid any conflicts of interests, the subscriber and the CA entity shall be separate entities. The only exception to this is if an organization entirely or partially undertakes RA tasks in connection with the issuance of certificates for persons associated with the organization and such exceptions are documented in the CA's CPS.

Note: The above requirement does not prevent the CA's organization from obtaining certificates for its own subjects. However, this must be handled by an entity that does not run and/or manage the CA system.

3.2.1 Method to prove possession of private key

[REQ 3.2.1-01] Prior to issuance of a certificate, the CA shall make sure that the subscriber or the subject is in possession of a private key belonging to the subject's public key which must form part of the certificate.

[REQ 3.2.1-02] The CA shall document the method for proof of possession of private key in the CPS.

3.2.2 Authentication of organization identity

[REQ 3.2.2-01] The CA shall establish a procedure for verifying the subscriber's identity to ensure that

a) The subscriber is a legal entity registered in the CVR.
b) Verification of the identity of the subscriber is ensured at NSIS assurance level 'substantial' or 'high'.
c) A management representative with adequate power of procuration from the subscriber must appoint an authorized person/entity, cf. definition in clause 1.6.1.

d) The authorized person/entity may be authenticated at NSIS assurance level 'substantial' or 'high' or eIDAS assurance level 'substantial' or 'high'.
e) All communication based on physical letters forming part of the documentation of the subscriber's identity is based on the current postal address registered in the CVR.

[REQ 3.2.2-02] If the CA has advance knowledge of the identity of the subscriber, the above requirement may be dispensed with in full or in part. The procedure must be submitted to and be approved by the Danish Agency for Digitisation before being implemented.

[REQ 3.2.2-03] The CA shall document the procedure for verifying the identity of the subscriber in CPS.

[REQ 3.2.2-04] The authorized person/entity shall guarantee the identification of the subject on registration by

a) An identification number that uniquely refers to the subject
b) Name of organization
c) All data about the subscriber included in the organizational attributes of the certificate
d) CVR no.

[REQ 3.2.2-05] If the subject is an entity or a system that specifically is to be used by one natural person only, the authorized person/entity shall also register and guarantee

a) A national identification number or other attributes that to the widest possible extent can ensure the uniqueness of the natural person.

3.2.3 Authentication of individual identity

N/A

3.2.4 Non-verified subscriber information

[REQ 3.2.4-01] The subscriber shall provide a physical address or other attributes that describe how the subscriber must be contacted.

3.2.5 Validation of authority

Cf. REQ 3.2.2-01 c) for validation of authority for an authorized person/entity.

3.2.6 Criteria for interoperation

N/A

3.3 Identification and authentication for re-key requests

[REQ 3.3-01] All requests for a certificate for a subject who has previously been registered by the CA shall be complete, accurate and authorized.

[REQ 3.3-02] In case of changes to the CA's terms and conditions, the CA's terms and conditions shall be communicated to and be accepted by the subscriber.

[REQ 3.3-03] Requirement for identity validation, cf. clause 3.2 shall apply.

3.3.1 Identification and authentication for routine re-key

[REQ 3.3.1-01] The CA shall check the existence and validity of the certificate to be re-keyed and that the information used for verifying the identity and attributes of the subjects is still valid.

3.3.2 Identification and authentication for re-key after revocation

[REQ 3.3.2-01] The CA shall verify the existence and validity of the certificate to be re-keyed and that the information used for verifying the identity and attributes of the subjects is still valid.

Note: In terms of validity, it must be verified that the certificate has been revoked in accordance with the above requirement.

3.4 Identification and authentication for revocation request

[REQ 3.4-01] The CA shall reasonably and considering the overall security make sure that revocation requests and reports of events that may give rise to revocation of certificates come from authorized sources.

[REQ 3.4-02] The CA shall document the procedures for revoking end-user and CA certificates in the public part of CPS, including

- Who can request revocation or report events that indicate a need for revocation of a certificate.
- How requests or reports can be submitted.
- Any requirements for subsequent confirmation of revocation requests or reports of events that indicate a need for revocation of a certificate.
- Valid reasons for revoking certificates.
- Mechanisms for distribution of information about revoked certificates (e.g. CRLs and OCSP).
- The maximum time from receipt of a revocation request until the decision to revoke the certificate.
- The maximum time from the decision to revoke the certificate until the actual information that the certificate is publicly available (e.g. via publication of CRL).

4. Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

[REQ 4.1.1-01] The subscriber may apply for a certificate for a subject via the authorized person/entity.

4.1.2 Enrolment process and responsibilities

[REQ 4.1.2-01] Application for certificates shall be made through an RA according to an enrolment process. When the application is made, the authorized person/entity shall be authenticated at a level corresponding to NSIS assurance level 'substantial' or 'high' or eIDAS assurance level 'substantial' or 'high'.

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

[REQ 4.1.2-02] If external RAs are used, registration data shall be exchanged securely and only with recognized RAs, whose identity is authenticated.

[REQ 4.1.2-03] The CA shall ensure that the enrolment process cannot be completed until the subscriber has accepted the terms and conditions for using the CA service.

[REQ 4.1.2-04] If the subject's key pair is not generated by the CA, the certificate request process shall check that the subject has possession or control of the private key associated with the public key that will be inserted in the certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

[REQ 4.2.1-01] Before a certificate is issued to a registered subject, the subject shall be identified and authenticated, for example by use of a reference number and a code securely sent to the authorized party.

4.2.2 Approval or rejection of certificate applications

[REQ 4.2.2-01] The CA shall approve or reject a certificate application and give the subscriber access to information about the status for certificate applications. The CA shall explain the reasons for the rejection of a certificate application to the subscriber.

4.2.3 Time to process certificate applications

[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] The CA shall issue certificates securely to maintain their authenticity.

In particular:

- **[REQ 4.3.1-02]** The CA shall take measures against forgery of certificates.
- **[REQ 4.3.1-03]** In cases where the CA generates the subjects' key pair, the CA shall guarantee confidentiality during the process of generating such data.
- **[REQ 4.3.1-04]** The procedure of issuing the certificate shall be securely linked to the associated registration, certificate renewal or re-key, including the provision of any subject-generated public key.
- **[REQ 4.3.1-05]** The CA must not issue certificates whose lifetime exceeds that of the CA's signing certificate.
- **[REQ 4.3.1-06]** If the CA generates the subject's key pair, the procedure of issuing the certificate shall be securely linked to the generation of the key pair by the CA.
- **[REQ 4.3.1-07]** If the CA generated the subject's key pair, the private key shall be securely passed to the subject or to the TSP managing the subject's private key.
- **[REQ 4.3.1-08]** Over the life time of the CA, a subject distinguished name which has been used in a certificate shall never be re-assigned to another subject.

Note: The name in the above requirement comprises the entire identification in the certificate, including subject serialNumber, cf. clause 7.1.4.

[REQ 4.3.1-10] The CP must be identified in the certificate with NCP (Normalized Certificate Policy) cf. clause 7.1.6.

4.3.2 Notification to subscriber by the CA of issuance of certificate

[REQ 4.3.2-01] The CA may notify the subscriber upon certificate issuance.

4.4 Certificate acceptance

4.4.1 Conduct constituting acceptance of modified certificate

[REQ 4.4.1-01] The terms and conditions shall indicate what is deemed to constitute acceptance of the certificate.

In particular

- **[REQ 4.4.1-02]** Before entering into a contractual relationship with a subscriber, the CA shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 2.1.
- **[REQ 4.4.1-04]** The CA shall communicate the terms and conditions through a durable (i.e. with integrity over time) means of communication, and in a human readable form before the agreement.
- **[REQ 4.4.1-05]** The terms and conditions may be transmitted electronically.
- **[REQ 4.4.1-06]** The terms and conditions may use the model specified in ETSI EN 319 411-1 Annex A.
- **[REQ 4.4.1-08]** The agreement in the above requirement shall involve explicit acceptance of the terms and conditions by a wilful act which can be later supported by evidence.

Note: The above evidence may for instance be based on system evidence.

- **[REQ 4.4.1-09]** The subscriber must approve the agreement with the CA, which at a minimum must include:
  a) the subscriber's obligations, including obligations for handling of certificates and the associated private keys.
  b) consent to the CA storing information used in registration, related processing, including whether it is the subscriber or the subject being registered, any subsequent revocation, the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the event the CA shuts down its services.
  c) whether, and under what conditions, the subscriber shall approve the publication of the certificate
  d) confirmation that the information to be held in the certificate is correct
  e) obligations to request the CA revoke certificates issued to subjects when they are no longer associated with the subscriber.
- **[REQ 4.4.1-12]** The agreement may be in electronic form.
- **[REQ 4.4.1-13]** The records identified above shall be retained for the period of time as indicated to the subscriber (as part of the terms and conditions).

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 REQ 4.4.1-09 c).

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 REQ 4.4.1-09 c).

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

[REQ 4.5.1-01] Through an agreement, the CA shall ensure that the subscriber's obligations include items a) to h) below.

a) Information submitted to the CA in accordance with the requirements of this policy must be accurate and complete, particularly with regards to registration.
b) The key pair is only used in accordance with the determined authorized use and not beyond any limitations notified to the subscriber and subject, and the private key must not be used to sign other certificates.
c) Unauthorized use of the subject's private key must be avoided, including
    i) that the choice of password ensures that they cannot be readily guessed through knowledge of the subject,
    ii) that adequate measures are taken to protect the security mechanisms that protect the private key against compromise, change, loss and unauthorized use, and
    iii) that passwords are not disclosed to any other parties.
d) If the subscriber or subject generates the subject's keys:
    i) an obligation or recommendation to generate the subject keys using an algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP, and
    ii) an obligation or recommendation to use key length and algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP during the validity time of the certificate or
    iii) through the use of algorithms and key lengths recommended by the Danish Agency for Digitisation that can replace d).i) and d).ii).
e) If the subscriber or subject generates the subject's keys and the private key pair, and the private key can be used to generate digital seals, the subject shall have sole control of the private key.
f) Notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    i) The subject's access to the private key has been lost or the subject's private key has been stolen or potentially compromised.
    ii) Control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons.
    iii) Inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.
g) Following compromise, the use of the subject's private key is immediately discontinued, subject to a request for revocation, notification of revocation or expiry of certificate, except for any decryption of data.

h) The use of a subject's private key shall be discontinued if the subscriber or subject has been notified that the subject's certificate has been revoked or if the issuing CA has been compromised.

Note: The term 'lost' in REQ 4.5.1-02 f).i) does not include solutions where the private key is not stored but is only used for single operation (signing) and is then destroyed.

4.5.2 Relying party public key and certificate usage

[REQ 4.5.2-01] The CA's information to relying parties shall include the following recommendations:

a) The relying party shall verify the validity or revocation of the certificate using current revocation status information as indicated to the relying party.

b) The relying party shall take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions supplied by the CA.

c) The relying party shall take any other precautions prescribed in agreements or elsewhere.

4.6 Certificate renewal

Renewal of an OCES 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.

4.6.1 Circumstance for certificate renewal

N/A

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

[REQ 4.6.3-01] Requests for certificates issued to a subject who has previously been registered with the CA shall be complete, accurate and authorized.

[REQ 4.6.3-02] In particular, the CA shall check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid.

[REQ 4.6.3-03] If any of the CA's terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with requirements for the first issuance.

[REQ 4.6.3-04] Requirements corresponding to the first issuance for identification and authentication shall apply, cf. clause 3.3.

[REQ 4.6.3-05] The CA shall issue a new certificate using the subject's existing certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised nor that the certificate has been revoked due to any other security breach.

4.6.4 Notification of new certificate issuance to subscriber

[REQ 4.6.4-01] The CA's notification of certificate renewal to the subscriber shall follow the rules for notification of the first certificate, cf. clause 4.3.2.

4.6.5 Conduct constituting acceptance of modified certificate

[REQ 4.6.5-01] Conduct constituting certificate acceptance shall follow the rules for acceptance of the first certificate, cf. clause 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

[REQ 4.6.6-01] Publication of a renewal certificate shall follow the rules for publication of the first certificate, cf. clause 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

[REQ 4.6.7-01] The CA's notification of certificate renewal to other entities shall follow the rules for notification of the first certificate, cf. clause 4.3.3.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Re-key of an OCES 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 4.7.1-01] A certificate issued under this CP may be re-keyed for up to four years at a time.

[REQ 4.7.1-02] The CA or subscriber can specify whether a certificate can be re-keyed.

[REQ 4.7.1-03] The CA shall ensure that a request for and issuance of a re-keyed certificate can be made online, unless the existing certificate is marked as non-renewable, cf. REQ 4.7.1-02.

[REQ 4.7.1-04] For re-keyable certificates, the CA may notify the subject well in advance of the expiry. Moreover, the CA may at the same time notify the authorized person/entity of the expiry.

4.7.2 Who may request certification of a new public key

[REQ 4.7.2-01] A certificate issued under this CP may be re-keyed by the subject if the existing certificate is marked as re-keyable, cf. REQ 4.7.1-02.

4.7.3 Processing certificate re-keying requests

[REQ 4.7.3-01] The CA shall ensure that the re-keying request is signed with the subject's valid private key or that the subject is authenticated at NSIS assurance level 'substantial' or 'high' or eIDAS assurance level 'substantial' or 'high'.

[REQ 4.7.3-02] Certificate application and issuance must follow the requirements in clause 6.1 on generation and installation of the subject's keys.

4.7.4 Notification of new certificate issuance to subscriber

[REQ 4.7.4-01] The CA's notification of certificate re-key to the subscriber shall follow the rules for notification of the first certificate, cf. clause 4.3.2.

4.7.5 Conduct constituting acceptance of modified certificate

[REQ 4.7.5-01] Conduct constituting subject certificate acceptance shall follow the rules for acceptance of the first certificate, cf. clause 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

[REQ 4.7.6-01] Publication of a re-keyed certificate shall follow the rules for publication of first certificates, cf. clause 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

[REQ 4.7.7-01] The CA's notification of a re-keyed certificate to other entities shall follow the rules for notification of the first certificate, cf. clause 4.3.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

[REQ 4.8.1-01] Requests for certificates issued to a subject who has previously been registered with the CA shall be complete, accurate and authorized. This includes certificate update due to changes to the subject's attributes.

4.8.2 Who may request certificate modification

[REQ 4.8.2-01] The subscriber may request a certificate modification.

4.8.3 Processing certificate modification requests

[REQ 4.8.3-01] If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information shall be verified, recorded, agreed to by the subscriber in accordance with clause 3.3.

4.8.4 Notification of new certificate issuance to subscriber

[REQ 4.8.4-01] The CA's notification of certificate modification to subject and/or subscriber shall follow the rules for notification of the first certificate, cf. clause 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

[REQ 4.8.5-01] Conduct constituting certificate acceptance shall follow the rules for acceptance of the first certificate, cf. clause 4.4.1.

4.8.6 Publication of the modified certificate by the CA

[REQ 4.8.6-01] Publication of a modified certificate shall follow the rules for publication of first certificates, cf clause 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

[REQ 4.8.7-01] The CA's notification of modified certificate to other entities shall follow the rules for notification of the first certificate, cf. clause 4.3.3.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

[REQ 4.9.1-01] The CA shall immediately and no later than within 12 hours revoke a certificate issued under this CP if the CA becomes aware of one or more of the following circumstances:

a) The subscriber wants to revoke the certificate or terminate use thereof.
b) The subject has lost access to the private key.
c) Known or suspected compromise of the subject's private key.
d) The private key has been destroyed or lost in any other way.
e) The subject no longer has an association with the subscriber.
f) An inaccuracy has been found in the certificate content or other information associated with the subscriber/subject, however cf. below for matters concerning the subject's change of name.
g) The subscriber's bankruptcy.
h) The subscriber's business activities terminate.

Note: The term 'lost' in REQ 4.9.1-01 b) and the terms 'destroyed' and 'lost' in REQ 4.9.1-01 d) do not include solutions where the private key is not stored but is only used for single operation (signing) and is then destroyed.

[REQ 4.9.1-02] 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.

Note: Please note that the above requirements do not apply if the subscriber maintains the former name as a secondary name, cf. REQ 3.1.2-01.

[REQ 4.9.1-03] Failure by the CA to comply with this CP does not entitle the CA to revoke a certificate.

Note: If inaccuracies are found in a certificate as a result of the CA's non-compliance, the certificate shall, however, still be revoked.

[REQ 4.9.1-04] Once a certificate is definitively revoked it shall not be reinstated.

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] The CA shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests from either of the parties described in clause 4.9.2.

[REQ 4.9.3-02] Revocation requests must as a minimum be sent via one of the following channels:

- Physical mail
- Web
- Over the telephone

[REQ 4.9.3-03] The CA shall notify the subscriber of a revoked certificate via the communication channel agreed between the CA and subscriber.

[REQ 4.9.3-04] If the CA revokes a certificate without being requested to do so, the CA shall send a message stating the reason for the revocation to the subscriber via the communication channel agreed between the CA and subscriber.

[REQ 4.9.3-05] In the event of the bankruptcy of the subscriber, the bankruptcy court or trustee in bankruptcy may request revocation. In such case, the CA shall also send the receipt for revocation to the bankruptcy court or trustee in bankruptcy.

4.9.4 Revocation request grace period

[REQ 4.9.4-01] By agreement, the CA shall ensure that the subscriber must request revocation without undue delay if one or more reasons for revocation, cf. clause 4.9.1, have occurred.

4.9.5 Time within which CA must process the revocation request

[REQ 4.9.5-01] The CA shall start processing revocation requests and reporting of events that may give rise to revocation of certificates immediately after receipt.

[REQ 4.9.5-02] The CA shall ensure that the certificate is revoked immediately after receipt of the request and any confirmation of the requester's identity and authorization.

[REQ 4.9.5-03] If the revocation request requires revocation in advance (e.g. subject's planned termination from his/her duties at a certain date), then the scheduled date may be considered as the confirmation point in time for the CA.

[REQ 4.9.5-04] Through the public part of the CPS, the CA may provide guarantees for faster processing times for certain revocation reasons.

[REQ 4.9.5-05] The time used for the provision of revocation services shall be synchronized with UTC at least once every 24 hours

4.9.6 Revocation checking requirement for relying parties

N/A

4.9.7 CRL issuance frequency (if applicable)

[REQ 4.9.7-01] Certificate Revocation Lists (CRLs) concerning subjects' certificates, including any variants (e.g. Delta CRLs) shall be published at least every 24 hours.

[REQ 4.9.7-02] Any Certificate Revocation Lists (CRL) concerning subjects' certificates, including any variants (e.g. Delta CRLs) shall contain the nextUpdate field defined in IETF RFC 5280, which must state the time of the next scheduled CRL issue, unless it is the last CRL issued for those certificates, in which case the nextUpdate field must be set to "99991231235959Z"

[REQ 4.9.7-03] Certificate Revocation Lists for CA certificates, including any variants (e.g. Delta CRLs) shall be generated and published at least once a year with a nextUpdate of at most 1 year after the issuing date.

[REQ 4.9.7-04] If a CA certificate is revoked the signing CA shall issue and publish a new Certificate Revocation List immediately thereafter.

[REQ 4.9.7-05] For any current CRL, including any variants (e.g. Delta CRLs), a new CRL must be published no later than one hour before the time stated in the nextUpdate field.

[REQ 4.9.7-06] In the case of any cross-certificates issued by the CA to other TSPs, the CA should be issued at least every 31 days.

4.9.8 Maximum latency for CRLs (if applicable)

[REQ 4.9.8-01] After completed revocation, the CA shall publish an updated CRL. This must be done no later than 1 minute after revocation. However, an updated CRL must be published no later than 10 minutes after revocation.

4.9.9 On-line revocation/status checking availability

[REQ 4.9.9-01] The CA shall 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

[REQ 4.9.11-01] The CA shall make information about certificate status available via manual online posts.

4.9.12 Special requirements re 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

[REQ 4.10-01] The CA shall provide services for checking the status of the certificates.

4.10.1 Operational characteristics

[REQ 4.10.1-02] The integrity and authenticity of the status information shall be protected.

[REQ 4.10.1-03] As a minimum, the CRL and OCSP shall be supported as certificate status checking methods.

[REQ 4.10.1-04] Status information must contain information on revocation status for a certificate at a minimum until the certificate's point of expiry.

[REQ 4.10.1-07] The CRL shall be signed digitally by the CA that has issued a revoked certificate.

[REQ 4.10.1-08] The CA shall make CRLs available for download via the following channels:

- LDAP
- HTTP

[REQ 4.10.1-09] Updated revocation information shall be available via all methods offered for checking certificate status, and all services shall be consistent over time taking into account small delays.

[REQ 4.10.1-10] OCSP responses can be pre-generated, but if a certificate is revoked, it is a requirement that the related OCSP response is re-generated, and no later than 1 minute after registration of the revocation, the OCEP response shall indicate that the certificate has been revoked.

[REQ 4.10.1-11] OCSP responders shall have dedicated business certificates which are exclusively used for OCSP. In addition to the formal requirements for a business certificate, the following requirements exist for the content:

- Key Usage: Digital Signature
- Extended Key Usage: OCSP Signing
- CRL Distribution Point: Not included
- AIA: Not included
- OCSP No Check: Included but blank.

[REQ 4.10.1-12] The lifetime of OCSP responder certificates for CAs that issue certificates to subjects shall be a maximum of 72 hours, and the related keys shall be protected by cryptographic devices as specified in clause 6.2.

[REQ 4.10.1-13] The lifetime of OCSP responder certificates for the root CA shall be a maximum of 3 months, and the related keys shall be protected by cryptographic devices as specified in clause 6.2.

4.10.2 Service availability

[REQ 4.10.2-01] Certificate status information shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that

this information service is not unavailable for longer than a maximum period of time as denoted in the public part of the CPS.

[REQ 4.10.2-02] All services to check certificate status shall have a response time where 99% of responses measured over a period of 60 minutes must be under 1 second measured at server entry – i.e. from the server has registered the request and until it starts to return the response.

[REQ 4.10.2-03] The certificate status information shall be publicly and internationally available.

4.10.3 Optional features

N/A

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] The CA must not use key escrow for the 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] The CA shall ensure that it operates in a legal and trustworthy manner.

[REQ 5-02] The CA shall carry out a risk assessment to identify, analyse and evaluate business and technical risks.

[REQ 5-03] The CA shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

[REQ 5-04] The CA shall determine and document all security requirements and operational procedures that are necessary to comply with this CP. The documentation must be part of the CPS.

[REQ 5-05] The risk assessment shall be reviewed and revised at least once a year.

[REQ 5-06] The CA's management shall approve the risk assessment and accept the residual risk identified.

[REQ 5-07] The CA must maintain an overview of its assets, including information assets. All information assets shall be classified according to the CA's risk assessment, and the CA shall ensure adequate protection of all assets.

[REQ 5-08] The CA shall implement efficient access control that protects against unauthorized physical or logical access to the CA's systems, and the CA shall provide RA systems which ensure that only authorized employees at the RA have access to operate them.

5.1 Physical controls

[REQ 5.1-01] The CA shall control physical access to components of the CA's system based on the classification policy. This includes minimizing risks related to physical security.

[REQ 5.1-02] The CA shall implement effective protection against

- loss, damage or compromise of assets and interruption to business activities; and
- compromise or theft of information and information processing facilities.

[REQ 5.1-03] The CA shall implement physical and environmental security controls to protect the facility housing, system resources, and the facilities used to support their operation.

[REQ 5.1-04] The CA shall implement physical and environmental security controls for systems concerned with certificate generation and revocation. The controls shall include physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, vibrations, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

[REQ 5.1-05] The CA shall implement controls to protect against equipment, information, media and software relating to the CA's services being taken off-site without authorization.

5.1.1 Site location and construction

[REQ 5.1.1-01] The CA shall clearly describe on which sites employees and data centres in connection with the activities of the CA are located. The sites on which equipment for the operation of CA is located, including but not limited to servers for key management and servers for status information, are referred to as the CA operating facility housing.

[REQ 5.1.1-02] The CA shall ensure that access to the CA facilities is limited to authorized individuals.

[REQ 5.1.1-03] The CA shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationships between critical systems and services.

[REQ 5.1.1-04] The requirements of this CP applies 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] The CA shall establish physical perimeter protection based on a specific risk assessment.

[REQ 5.1.2-02] Components that are critical for the secure operation of the CA shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

[REQ 5.1.2-03] Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation and revocation management services.

[REQ 5.1.2-04] The CA shall ensure that CA facilities concerned with certificate generation and revocation management are be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

[REQ 5.1.2-05] The CA shall ensure that access to all zones in all of the CA facilities is restricted to that necessary based on the principle of least privilege.

[REQ 5.1.2-06] As part of the access procedures, the CA shall ensure that subcontractors' personnel are covered by the CA's rules for trusted personnel and that they cannot work unsupervised at the CA.

[REQ 5.1.2-07] Other functions relating to CA's operations may be supported within the same secured area provided that the access is limited to authorized personnel.

[REQ 5.1.2-08] Any parts of the CA facilities shared with other organizations shall be outside the perimeter of the certificate generation and revocation management services.

[REQ 5.1.2-09] The CA shall ensure that efficient guard duty 24 hours a day is established.

[REQ 5.1.2-10] The CA shall ensure that video surveillance is used to control access to and activities in the central CA facilities.

[REQ 5.1.2-11] Every entry to the physically secure area shall be subject to independent oversight and a non-authorized person shall be accompanied by an authorized person whilst in the secure area.

[REQ 5.1.2-12] Root CA private keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates, CRL and OCSP responses.

[REQ 5.1.2-13] Every entry and exit shall be logged.

5.1.3 Power and air conditioning

See REQ 5.1-04.

5.1.4 Water exposures

See REQ 5.1-04.

5.1.5 Fire prevention and protection

See REQ 5.1-04.

5.1.6 Media storage

[REQ 5.1.6-01] All media in the CA's operating system shall be handled securely in accordance with its classification, and

- media shall be protected from damage, theft, unauthorized access and obsolescence;
- sensitive data shall be protected against unauthorized access through reused storage objects. In this connection, registration data are also considered sensitive data.

[REQ 5.1.6-02] The CA shall media management procedures in place to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

5.1.7 Waste disposal

[REQ 5.1.7-01] Storage media containing sensitive data shall be securely disposed of according to its classification.

5.1.8 Off-site backup

[REQ 5.1.8-01] If data are 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

5.2.1 Trusted roles

[REQ 5.2.1-01] Trusted roles, on which the security of the CA's operation is dependent, shall be clearly identified and approved by the management.

[REQ 5.2.1-02] The CA shall establish and implement procedures for all trusted and administrative roles that may impact on the CA's security and operations.

[REQ 5.2.1-03] All the CA's personnel in trusted roles shall be free from conflicts of interest that might prejudice the impartiality of the CA's operations.

[REQ 5.2.1-04] Trusted roles shall include roles that involve the following responsibilities:

a) Security Officers: Overall responsibility for administering the implementation of the security practices.

b) System Administrators: Authorized to install, configure and maintain the CA's critical systems for service management including system re-establishment.

c) System Operators: Responsible for operating the CA's critical systems on a day-to-day basis. Authorized to perform system backup.

d) System Auditors: Authorized to view archives and audit logs of the CA's critical systems.

e) Registration Officers: As defined in CEN TS 419 261.

f) Revocation Officers: As defined in CEN TS 419 261.

[REQ 5.2.1-05] Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the CA's assets.

5.2.2 Number of persons required per task

[REQ 5.2.2-01] Certificate issuance by the root CA shall be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

5.2.3 Identification and authentication for each role

[REQ 5.2.3-01] Personnel that are to access or configure privileges for trusted roles shall be formally approved by a security manager at the senior management level according to the "least privilege" principle.

[REQ 5.2.3-02] Trusted roles shall be approved by the management and accepted by the person to fulfil the role.

[REQ 5.2.3-03] The CA's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of

duties and least privilege, the sensitivity of data that can be accessed, background screening and employee training and awareness.

[REQ 5.2.3-04] Where appropriate, job descriptions shall differentiate between general functions and CA's specific functions. These should include skills and experience requirements.

[REQ 5.2.3-05] Personnel shall not have access to the trusted functions until the necessary checks are completed.

5.2.4 Roles requiring separation of duties

[REQ 5.2.4-01] The CA shall ensure that persons with oversight functions at the CA do not report to the same management as the system operators and administrators report to.

5.3 Personnel controls

[REQ 5.3-01] The CA shall ensure that employees and contractors support the trustworthiness of the CA's operations.

5.3.1 Qualifications, experience, and clearance requirements

[REQ 5.3.1-01] The CA shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding information security and personal data protection rules as appropriate for the offered services and the job function.

[REQ 5.3.1-02] Managerial personnel shall have experience or training in relation to operation of the CA, knowledge of compliance controls for personnel with security responsibility and experience with information security and risk assessment that is sufficient to be able to perform management functions for the CA.

[REQ 5.3.1-03] Security roles and responsibilities as specified in the CA's information security policy shall be documented in job descriptions or in documents that are accessible to all the employees concerned.

5.3.2 Background check procedures

[REQ 5.3.2-01] The CA shall carry out sufficient identification of personnel in connection with hiring them.

[REQ 5.3.2-02] The CA must check that managers and employees performing trusted tasks at or for the CA have not been convicted of a crime that makes them unsuitable for performing their job. This also applies to RA employees.

5.3.3 Training requirements

[REQ 5.3.3-01] The CA's personnel, including personnel of any possible subcontractors, must be in a condition to fulfil the requirement concerning "expert

knowledge, experience and qualifications" through formal educations and accreditations or through actual experience or a combination of the two.

[REQ 5.3.3-02] RA employees must receive training that will enable them to perform their work correctly and securely.

5.3.4 Retraining frequency and requirements

[REQ 5.3.4-01] The above training requirements should encompass regular (at least every 12 months) updates concerning new threats and current security practices.

5.3.5 Job rotation frequency and sequence

N/A

5.3.6 Sanctions for unauthorized actions

[REQ 5.3.6-01] Personnel shall use administrative procedures and processes that are in accordance with the CA's governing information security procedures.

[REQ 5.3.6-02] Appropriate disciplinary sanctions shall be used for personnel who violate the CA's policies or procedures.

5.3.7 Independent contractor requirements

[REQ 5.3.7-01] The CA shall ensure that the personnel of subcontractors fulfil the same requirements for training, experience and security classification as the CA's own employees in those functions that the subcontractor's personnel address for the CA.

5.3.8 Documentation supplied to personnel

N/A

5.4 Audit logging procedures

5.4.1 Types of events recorded

[REQ 5.4.1-01] All security-critical activities must be logged, including changes related to the security policy, system start-up and shut-down, system crashes and hardware failures, firewall and router activities and PKI system access attempts.

[REQ 5.4.1-02] All events related to registration, including requests for re-key or renewal of certificates must be logged.

[REQ 5.4.1-03] All lifecycle events related to CA's private keys must be logged by the CA.

[REQ 5.4.1-04] All lifecycle events at the CA related to certificates must be logged by the CA.

[REQ 5.4.1-05] All lifecycle events related to keys managed by the CA, including any possible handling of the keys of subjects must be logged by the CA.

[REQ 5.4.1-06] All reports and requests concerning revocation and the resultant action must be logged by the CA.

[REQ 5.4.1-07] All accesses and attempted accesses to areas that must be protected by access control must be logged by the CA.

5.4.2 Frequency of processing log

[REQ 5.4.2-01] The CA must document and follow written policies for regular reviewing of all audit logs. The frequency for the reviews must be established in the CPS.

5.4.3 Retention period for audit log

[REQ 5.4.3-01] The CA must store logs of all lifecycle events related to the CA's management of keys, including any possible handling of the keys of subjects for at least seven years after the expiry of the validity of every certificate related to the log.

[REQ 5.4.3-02] The CA must store all other audit logs for at least seven years.

5.4.4 Protection of audit log

[REQ 5.4.4-01] The CA must ensure the confidentiality and integrity of log data, including that events must be logged in a manner such that the log cannot easily be deleted or destroyed during the period in which the log must be stored (unless it is transferred securely to media for long-term storage).

[REQ 5.4.4-02] The CA must ensure protection of the privacy of subjects.

5.4.5 Audit log backup procedures

[REQ 5.4.5-01] The CA must implement a procedure for regular security copying of audit logs.

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] The CA is responsible for the establishment of a records archival system, which must contain all data that is necessary for secure operation of the CA in accordance with this CP.

[REQ 5.5-02] The CA and RA must ensure that all electronic archive material will be stored with a specification of the point in time of its archiving.

Note: There is no requirement that time-stamping must be based on electronic time stamps or qualified electronic time stamps, cf. [eIDAS]

5.5.1 Types of records archived

[REQ 5.5.1-01] The CA must register and be able to access all relevant information concerning data generated and received by the CA during an appropriate space of time, including after termination of the activities at the CA, namely for purposes of being able to submit evidence material in legal cases and to be able to ensure the continued operation of the service.

[REQ 5.5.1-02] All registration information must be recorded, including:

a) Type(s) of documentation that were submitted in connection with the registration.

b) Registration of unique identification data, numbers or a combination thereof of identification documents, if it is relevant and with respect for the protection of the privacy of the subject.

c) Storage location of copies of applications and identification documents, including agreements entered into.

d) Any specific choices in agreements, for example consent to publication of certificates.

e) The identity of the person who accepts agreements.

f) The method used for validation of documentation of identity, if any.

g) Specification of name of receiving CA and RA, if applicable.

[REQ 5.5.1-03] The CA must ensure that the following data is stored:

a) Certificate applications and relevant associated communications, including applications related to renewals.
b) Signed orders and written agreements,
c) CPS (all approved versions).

[REQ 5.5.1-04] All video monitoring of CA operating premises must be stored.

5.5.2 Retention period for archive

[REQ 5.5.2-01] Data must be stored for at least seven years to be able to be used as evidence and with regard for protection of privacy. The policy for storage time must be documented and stated in the terms and conditions. This also applies to

any possible data from the RA's IT systems that is relevant for documentation of the CA's work.

[REQ 5.5.2-02] In particular, the CA must store documentation described in clause 4.4 for at least seven years after the expiry of validity of every certificate related to the log.

5.5.3 Protection of archive

[REQ 5.5.3-01] The CA must ensure the confidentiality and integrity of stored data related to the operation of the CA's services.

[REQ 5.5.3-02] The CA must ensure the completeness, confidentiality and integrity of stored data related to the operation of the CA's services with respect to documented business practices published in the CPS.

5.5.4 Archive backup procedures

[REQ 5.5.4-01] Regular back-up copies must be made of critical data and software in accordance with ISO 27002, clause 12.3.

[REQ 5.5.4-02] Adequate back-up copying facilities should be ensured in order to ensure that all significant information and software can be recovered after a critical event or fault in storage media.

[REQ 5.5.4-03] The CA's system data that is necessary to recover the CA operation after a critical event/catastrophe must be backed up and stored securely, preferably at an off-site location, such that it is possible for the CA to recover operation within a reasonable period of time.

[REQ 5.5.4-04] Back-up solutions must be tested regularly in order to ensure that they fulfil the requirements in established recovery plans.

[REQ 5.5.4-05] Functions for backing up and re-establishment must be performed by the relevant trusted roles, which are specified in clause 5.2.1.

[REQ 5.5.4-06] Data, which through risk analysis has been identified to require handling with the use of dual control, for example keys, must use dual control in connection with recovery.

5.5.5 Requirements for time-stamping of records

N/A

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] Data, including audit logs, must be able to be restored and made available as evidence in a legal case.

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 utilised for issuance of certificates.

5.7 Compromise and disaster recovery

[REQ 5.7-01] The following security events must be regarded as critical:

- Compromising of the CA's private key.
- Suspicions of compromising of the CA's private key.
- Breakdowns and critical faults in CA operating components (CRLs, etc.).
- Halting of the CA operating environment sur to fire, loss of electrical power, etc.
- Significant irregularities in the logging procedure.
- Physical penetration.

5.7.1 Incident and compromise handling procedures

[REQ 5.7.1-01] System activities such as access to IT systems, use of IT systems and calls to services must be monitored.

[REQ 5.7.1-02] The monitoring must take into account the sensitivity of the data that is being collected or analysed.

[REQ 5.7.1-03] Abnormal system activities that constitute a potential security breach, including intrusion into the CA's network, must be detected and reported as alarms.

[REQ 5.7.1-04] The CA must monitor the following events:

a) start-up and shut-down of the log functions and

b) availability and utilization of needed services with the CA's network.

[REQ 5.7.1-05] The CA must act in a timely and co-ordinated manner in order to respond quickly to security incidents and limit the consequences of security breaches.

[REQ 5.7.1-06] The CA must have personnel with a trusted role for following up on alerts of potential critical security events and ensure that relevant incidents are reported in line with the CA's procedures.

[REQ 5.7.1-07] The CA must have procedures and emergency preparedness that ensure notification of a security event or loss of integrity to relevant parties, cf. applicable regulations, for example the data protection authorities, at the latest 72 hours after and/or the eIDAS supervisory body at the latest 24 hours after the event has been identified.

[REQ 5.7.1-08] If there is a likelihood that a security incident or loss of integrity can affect a physical person or a legal entity negatively, then the CA must also notify them without undue delay.

[REQ 7.11-09] The CA's systems must be monitored, which must encompass monitoring or regular review of audit logs in order to identify malicious activity for purposes of sending alarms for potential critical security events to security personnel.

[REQ 5.7.1-10] The CA must handle every critical vulnerability that has not previously been handled by the CA, within 48 hours after its discovery.

[REQ 5.7.1-11] For any identified vulnerability, the CA must in relation to the potential impact either

- create and implement a plan for mitigation of the vulnerability or
- document the basis for the CA's decision that the vulnerability does not require remediation.

[REQ 5.7.1-12] Incident reporting and response procedures must be established in a manner such that damages from security incidents and malfunctions are minimised.

5.7.2 Computing resources, software, and/or data are corrupted

[REQ 5.7.2-01] The CA must in the event of critical events for data processing equipment, software and/or data orient the subscriber of such to the extent that it is relevant for their use of the CA services. With consideration to the situation that has arisen, relying parties must be informed via public media and by advertisement in the daily press.

[REQ 5.7.2-02] The CA must ensure that all procedures with a relation to CRLs, including requests concerning revocation, have the highest priority in connection with the re-establishment of business procedures after a breakdown.

5.7.3 Entity private key compromise procedures

[REQ 5.7.3-01] The CA's Business Continuity Plan (or Disaster Recovery Plan) must handle the compromising, loss and suspected compromising of one of the CA's private keys as a critical event or a disaster.

[REQ 5.7.3-02] Planned processes must be established for handling of the compromising, loss or suspected compromising of one of the CA's private keys. The plan must contain processes for management of the certificates of subjects issued under the keys involved.

[REQ 5.7.3-03] In the event of the compromising of the CA's private keys, the CA must

- inform subscribers and other parties who have a contractual relationship with the CA or another relevant relationship to the CA, for example other trusted service providers and relying parties,
- inform the Danish Agency for Digitisation with an in-depth description of the situation that has arisen,

- make information on the compromising accessible to third parties,
- state that certificates and revocation status information issued with the use of this CA key are no longer valid and
- revoke every CA certificate that was issued with a public key corresponding to the compromised CA key.

[REQ 5.7.3-04] In the event that some of the algorithms or associated parameters that are used by the CA or subscribers have inadequate security within the period for their remaining intended use, then the CA must inform all subscribers and relying parties that the CA has an agreement or other form of established connections with. In addition, the CA must make this information available to other relying parties.

[REQ 5.7.3-05] In the event that some of the algorithms or associated parameters that are used by the CA or subscribers have inadequate security within the period for their remaining intended use, then the CA must revoke all valid certificates affected.

[REQ 5.7.3-06] The CA must have a documented plan for an event with a general compromising of the private keys of many subjects.

5.7.4 Business continuity capabilities after a disaster

[REQ 5.7.4-01] The CA must establish, test and maintain a Business Continuity Plan (BCP), which shall be enacted in in case of an operating-related disaster.

[REQ 5.7.4-02] In the event of an operating-related disaster, including compromising of one of the CA's private signature keys, then operation must be re-established within the delay that is established in the BCP once the cause of the disaster has been handled with appropriate remediation measures.

[REQ 5.7.4-03] After a disaster, the CA must, where it is possible, implement mitigating precautions in order to avoid repetitions.

5.8 CA or RA termination

[REQ 5.8-01] The CA must on an on-going basis maintain a plan for termination of the CA services.

[REQ 5.8-02] The CA must, in the CPS, specify provisions upon termination of the service. These must at a minimum include information on who will be notified upon termination and who will take over customers and users, if these types of agreements exist, as well as who will take over responsibility for the revocation status service.

[REQ 5.8-03] Prior to termination, the CA must inform relevant authorities, including the Danish Agency for Digitisation, subscribers and all other parties that have a contractual relationship with the CA. In addition, the CA must make information on termination available to relying parties before the termination.

[REQ 5.8-04] The CA must ensure that all issuance and renewal of certificates is immediately stopped when a CA function ceases to function.

[REQ 5.8-05] Potential disruptions for subscribers and other parties must be minimised in consequence of termination of the CA's services. The CA must ensure the continued operational operation of CRLs and requests for revocations, until all certificates issued by this CA have expired or possibly been transferred to another CA that fulfils the requirements in this CP. Moreover, the CA shall ensure that the CA's root certificates and intermediate certificates are made available to the public for a reasonable period of time.

[REQ 5.8-06] The CA shall ensure that archives can be accessed for at least seven years after the expiry of the last certificate issued by the CA, including registration information, revocation status information and event log archives.

[REQ 5.8-07] In connection with the CA terminating its services, the CA shall terminate authorization for all subcontractors to act on behalf of the CA in carrying out any functions relating to the process of issuing and handling of certificates.

[REQ 5.8-08] In connection with the CA terminating its services, the CA's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

[REQ 5.8-09] Where possible, the CA shall make arrangements to transfer provision of trust services for its existing customers and users to another CA.

[REQ 5.8-10] When another cross-certified CA stops all operations, including handling revocation, all cross-certificates to that CA shall be revoked.

[REQ 5.8-11] Where the CA is a private business or a natural person, the CA shall provide an irrevocable demand guarantee or the like with an approved institute to secure payment of its financial obligations in accordance with REQ 5.8-1 to REQ 5.8-10.

6. Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

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

[REQ 6.1.1-02] The CA shall implement secure handling of cryptographic keys and cryptographic devices. The handling shall cover the full lifecycle of keys and devices.

[REQ 6.1.1-03] For critical parts of the CA's infrastructure, the CA shall follow relevant and official recommendations from ENISA regarding the use of up-to-date algorithms and key lengths.

[REQ 6.1.1-04] The CA shall generate CA keys, including keys used by revocation and registration services, securely, and the private key shall be secret.

[REQ 6.1.1-05] In particular the following must be observed:

- The CA key generation and the subsequent certification of the public key shall be undertaken in a physically secured environment (cf. clause 5.1) by personnel in trusted roles (cf. clause 5.2).
- CA keys used for signing certificates shall be created under dual control monitored by two persons, each with their trusted function in the CA.
- The number of personnel authorized to carry out CA key generation shall be kept to a minimum and be consistent with the CA's CPS.
- CA key generation shall be performed using an algorithm as specified in ETSI TS 119 312 for the CA's signing purposes.
- The selected key length and algorithm for the CA signing key shall be one which is specified in ETSI TS 119 312 for the CA's signing purposes. However, the recommendation for choice of cryptographic algorithms and parameters defined in ETSI TS 119 312 may be superseded by national recommendations.

[REQ 6.1.1-06] Before expiration of the CA certificate which is used for signing subject certificates, the CA shall, if it continues the service, generate a new certificate for signing subject certificates, and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate.

[REQ 6.1.1-07] Before expiration of its CA certificate which is used for signing subject certificates, the new CA certificate shall, if the CA continues the service, also be generated and distributed in accordance with the present document.

[REQ 6.1.1-08] The operations described in REQ-6.1.1-06 and REQ-6.1.1-07 shall be performed with a suitable interval between CA certificate expiry date and the last certificate issued to a subject to allow all parties that have relationships with the CA (subjects, subscribers, relying parties and other relevant CAs) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply if the CA ceases its operations before the expiry of the CA certificate.

[REQ 6.1.1-09] The CA shall have a documented procedure called 'Key Signing Ceremony (KSC)' for conducting CA key generation for a certificate to issue the certificate. This applies to all CAs (root CA and subordinate CAs, including CAs that issue certificates to subjects).

[REQ 6.1.1-10] The KSC shall indicate at a minimum:

a) roles that participate (both internal and external).

b) Functions to be performed by every role and during which phases.

c) Responsibilities during and after the ceremony.

d) Requirements for documentation to be collected as evidence of the ceremony.

[REQ 6.1.1-11] The CA shall produce a report proving that the key generation was carried out in accordance with the stated KSC procedure and that the integrity and confidentiality of the key pair was ensured.

[REQ 6.1.1-12] This report shall as a minimum be signed by

- For root CA: by the trusted role responsible for the security of the CA's key management (e.g. security officer) and a trusted person independent of the CA's management (e.g. the conformity assessment body) as witness that the report correctly records the KSC as carried out.
- For subordinate CAs: by the trusted role responsible for the security of the CA's key management (e.g. security officer) as witness that the report correctly records that the KSC was carried out.

[REQ 6.1.1-13] The CA shall ensure that the subject's keys, as generated by the CA, are generated securely and that the confidentiality of the subject's private keys is ensured.

[REQ 6.1.1-14] If the CA generates the subject's keys, CA-generated subject keys shall be generated using an algorithm recognized as being fit for the uses identified in the CP during the entire period of validity of the certificate.

[REQ 6.1.1-15] If the CA generates the subject's keys, CA-generated subject keys shall be of key lengths and algorithms as specified in ETSI TS 119 312. However, the recommendation for choice of cryptographic algorithms and parameters defined in ETSI TS 119 312 may be superseded by national recommendations.

[REQ 6.1.1-16] If the CA generates the subject's keys, CA-generated subject keys shall be generated and stored securely whilst held by the CA in a manner such that the subject alone can use the private key.

6.1.2 Private key delivery to subscriber

[REQ 6.1.2-01] If the CA generates the subject's keys, the subject's private key shall be delivered to the subject's key protection device or to the TSP managing the subject's private key, in a manner such that the secrecy and integrity of the key is not compromised. For example, a cryptographic device and associated activation code must not be delivered in the same letter.

[REQ 6.1.2-02] If the CA generates the subject's keys and if the CA or any of its designated RAs become aware that a subject's private key has been communicated to an unauthorized person or an organization not affiliated with the subject, then the CA shall revoke all certificates that include the public key corresponding to the communicated private key.

[REQ 6.1.2-03] If the CA generates the subject's keys, the CA shall delete all copies of a subject's private key after delivery of the private key to the subject.

6.1.3 Public key delivery to certificate issuer

[REQ 6.1.3-01] If the subject or subscriber delivers the subject's public key to the CA, they shall apply a mechanism to assure the integrity of the key

6.1.4 CA public key delivery to relying parties

[REQ 6.1.4-01] The CA's (public) keys shall be available to relying parties in a manner that assures the integrity of the CA key and authenticates its origin.

[REQ 6.1.4-02] In particular, the CA shall allow verification of the root certificate via another channel. Verification may take place by using a fingerprint for the certificate.

6.1.5 Key sizes

See clause 6.1.1.

6.1.6 Public key parameters generation and quality checking

N/A

6.1.7 Key usage purposes (as per X.509v3 keyUsage)

[REQ 6.1.7-01] The CA shall include extension keyUsage in issued certificates to the subject and keyUsage shall comply with the requirements in clause 4.3.2 Key usage in [ETSI EN 319 412-2].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

[REQ 6.2-01] The CA shall ensure that the CA's root keys are not compromised and that they retain their integrity at all times.

6.2.1 Cryptographic module standards and controls

[REQ 6.2.1-01] The CA's key pair generation, including keys used by revocation and registration services, shall be carried out in a secure cryptographic module that is a trustworthy system which

a) has been evaluated as EAL 4 or higher in accordance with ISO 15408 or the equivalent national or internationally recognized evaluation criteria for IT security provided this is a security level or protection profile that meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures, or

b) meets the requirements identified in ISO/IEC 19790 or FIPS PUB 140-2 level 3.

Note: With the general availability of products that meet REQ 6.2.1-01 a), it is expected that REQ 6.2.1-01 b) will be omitted in future versions of this CP

[REQ 6.2.1-02] The cryptographic device shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

[REQ 6.2.1-03] The CA shall ensure that cryptographic devices for certificate and status information signing have not been compromised prior to installation.

[REQ 6.2.1-04] The CA shall ensure that cryptographic devices for certificate and status information signing have not been compromised during use.

[REQ 6.2.1-05] The CA shall ensure that all handling of cryptographic devices for certificate and status information signing takes place with the assistance of at least two persons that each hold trusted roles in the CA.

[REQ 6.2.1-06] The CA shall ensure that cryptographic devices for certificate and status information signing function correctly at all times.

[REQ 6.2.1-07] The CA private signing key shall be held and used within a secure cryptographic device meeting the requirements above.

6.2.2 Private key (n out of m) multi-person control

See REQ 6.2.4-01.

6.2.3 Private key escrow

See REQ 4.12.1-01.

6.2.4 Private key backup

[REQ 6.2.4-01] The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 5.1).

[REQ 6.2.4-02] The number of personnel authorized to carry out CA private signing key back up, storage and recovery shall be kept to a minimum and be consistent with the CA's CPS.

[REQ 6.2.4-03] Copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

6.2.5 Private key archival

[REQ 6.2.5-01] When outside the secure cryptographic device, the CA private key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.

6.2.6 Private key transfer into or from a cryptographic module

[REQ 6.2.6-01] If the CA's root keys or other private keys are to be transmitted from a cryptographic module, this shall take place in encrypted form and with the assistance of at least two persons holding different trusted functions in the CA.

[REQ 6.2.6-02] Transport of the CA's root keys and other critical private keys shall be supervised by two persons each holding a trusted function in the CA.

Note: In this respect, the subject's private keys are generally not considered as critical private keys unless they are used e.g. in connection with the administration of the CA's systems.

6.2.7 Private key storage on cryptographic module

[REQ 6.2.7-01] Where the CA private signing keys and any copies are stored in a dedicated secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device.

[REQ 6.2.7-02] The secure cryptographic device shall not be tampered with during shipment.

[REQ 6.2.7-03] The secure cryptographic device shall not be tampered with while stored.

[REQ 6.2.7-04] The secure cryptographic device shall be functioning correctly.

6.2.8 Method of activating private key

[REQ 6.2.8-01] The CA shall ensure that the subject's private key cannot be used without the subject authorising such use in each case, meaning that the subject retains sole control over its private key.

This can be done

- Via an agreement that obligates the subscriber if the private key is generated and used solely while under the subscriber's control.
- By means of a combination of technical controls and agreements that obligates the subscriber and other relevant parties if the private key is generated and used in full or in part by a trusted service.

6.2.9 Method of deactivating private key

N/A

6.2.10 Method of destroying private key

[REQ 6.2.10-01] The CA's private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.

6.2.11 Cryptographic Module Rating

N/A

6.3 Other aspects of key pair management

[REQ 6.3-01] The CA shall solely use the CA's private keys for signing in an appropriate manner. In particular:

- The CA shall not use private keys for signing beyond the end of their life cycle.
- The CA's private keys used for generating OCES certificates and/or issuing revocation status information shall not be used for other purposes.
- The CA's private keys used for generating certificates shall only be used within physically secure premises
- The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with current practice as in requirement clause 6.1.
- All copies of the CA's private signing keys shall be destroyed at the end of their life cycle.
- If a self-signed certificate is issued by the CA, the attributes of the certificate shall be compliant with the defined key usage as defined in Recommendation ITU-T X.509 and requirements in clause 6.1.

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

6.4.1 Activation data generation and installation

[REQ 6.4.1-01] If the CA issues a secure cryptographic device (e.g. smartcard) deactivation and reactivation shall be done securely.

[REQ 6.4.1-02] Through agreement and/or technical controls, the CA shall ensure that the subject's private key is effectively protected against unauthorized use by means of activation data or other corresponding mechanisms that give an equivalent or higher level of protection.

[REQ 6.4.1-03] If the subject's private key is installed on devices to which others have access, the activation data shall consist of at least two varying, independent factors (among 'something the subscriber knows', 'something the subscriber has'

and 'something the subscriber is') and efficient protection shall be provided against exhaustive search for valid activation data.

Note: Biometry ("something the subscriber is") is primarily relevant if the subscriber is identical with a natural person.

[REQ 6.4.1-04] If the subject's private key is installed on devices to which only the subject has access, the security of activation data shall at least constitute a password consisting of at least 8 characters containing at least one small and one capital letter as well as a number, and the password must be difficult to guess. Alternatively, other mechanisms can be used that give an equivalent or higher level of protection. If a password is used in environments that effectively prevent exhaustive searches, the password may however be picked from a range of at least 9,800 possible codes.

6.4.2 Activation data protection

[REQ 6.4.2-01] If the CA issues a secure cryptographic device, and where the personalized secure cryptographic device (e.g. smartcard) has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure cryptographic device.

6.4.3 Other aspects of activation data

[REQ 6.4.3-01] The installation and recovery of the CA's key pairs in a secure cryptographic device shall require simultaneous control by at least two trusted employees.

[REQ 6.4.3-02] The CA shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

[REQ 6.5.1-01] The CA's operating systems shall provide sufficient computer security controls for the separation of trusted roles identified in the CA's CSP, including the separation of security administration and operational roles. Particularly, use of system utility programs shall be restricted and controlled to what is necessary.

[REQ 6.5.1-02] The CA shall implement documented processes for release and change management of software, hardware and configuration changes. The CA shall have documented processes for security update of proprietary and standard software and firmware. The processes shall include documentation of the changes.

[REQ 6.5.1-03] The integrity of the CA's systems and information shall be protected against viruses, malicious and unauthorized software, and the CA shall implement processes that ensure:

- security patches are applied within a reasonable time after they come available;
- security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
- the reasons for not applying any security patches are documented.

[REQ 6.5.1-04] The CA's systems shall enforce access control on attempts to add or delete certificates and modify other associated information.

[REQ 6.5.1-05] The CA's systems shall enforce access control on attempts to modify revocation status information.

[REQ 6.5.1-06] Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

6.5.2 Computer security rating

N/A

6.6 Life cycle technical controls

6.6.1 System development controls

[REQ 6.6.1-01] The CA shall use trustworthy systems and products that are protected against modification. The products shall provide an adequate protection profile in accordance with ISO 15408 or similar.

[REQ 6.6.1-02] The CA shall ensure that, prior to any system development (e.g. undertaken by the CA or on behalf of the CA), a plan approved by management is provided to ensure that security is built into the systems. The plan shall include an analysis of security requirements being met in order to maintain an adequate level of security.

6.6.2 Security management controls

[REQ 6.6.2-01] The CA shall live up to the requirements in the information security standard ISO 27001 and be able to document compliance through e.g. certification.

[REQ 6.6.2-02] The CA shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.

[REQ 6.6.2-03] The CA shall communicate changes to the information security policy to relevant parties.

[REQ 6.6.2-04] A CA's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for the CA's facilities, systems and information assets providing the services.

[REQ 6.6.2-05] The CA shall publish and communicate the information security policy to all employees who are impacted by it, including employees at subcontractors performing work for the CA.

Note: Employees working for the CA's organization but who do not carry out work related to its roles as CA are not covered by the above requirement.

[REQ 6.6.2-06] The CA's information security policy and inventory of assets for information security shall be reviewed at annually and if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

[REQ 6.6.2-07] Any changes that may impact on the level of security provided shall be approved by the CA's management.

[REQ 6.6.2-08] The configuration of the CA's systems shall be checked at fixed intervals and at least once a year for changes which violate the CA's information security policy.

[REQ 6.6.2-09] The CA shall check the configuration of the CA's systems for changes that violate the CA's information security policy in connection with significant organizational or operational changes.

[REQ 6.6.2-10] The maximum interval between two of the above checks shall be documented in CPS.

6.6.3 Life cycle security controls

[REQ 6.6.3-01] The CA shall implement an efficient user administration, including administer user access of operators, administrators and system auditors.

[REQ 6.6.3-02] User accounts shall be checked regularly to ensure that the users only have the necessary rights cf. access control policy.

[REQ 6.6.3-03] Access to information and application system functions shall be restricted in accordance with the access control policy.

[REQ 6.6.3-04] The CA's personnel shall be identified and authenticated before using critical systems and applications.

[REQ 6.6.3-05] The CA's personnel shall be accountable for their activities, e.g. through efficient event logging.

[REQ 6.6.3-06] The CA shall monitor and plan capacity requirements to ensure the adequate processing power and storage are available to be able to maintain a suitable service.

6.7 Network security controls

[REQ 6.7-01] The CA shall protect its network and systems protected from attacks and unauthorized access, including access by subjects, subscribers and relying parties.

[REQ 6.7-02] The CA shall segment its networks into zones based on risk assessment considering the criticality of the individual sub-systems and their physical location.

[REQ 6.7-03] The CA shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high-security zones.

[REQ 6.7-04] The CA shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

[REQ 6.7-05] Local network components (e.g. routers) shall be kept in a physically and logically secure environment.

[REQ 6.7-06] Local network components (e.g. routers) configurations shall be periodically checked for compliance with the requirements specified by the CP in the CSP.

[REQ 6.7-07] The CA shall apply the same security controls to all systems co-located in the same zone.

[REQ 6.7-08] The CA shall place particularly critical systems, including root-CA in high-security zones.

[REQ 6.7-09] The CA shall grant access to secure zones and high security zones to only trusted roles.

[REQ 6.7-10] The CA shall separate dedicated network for administration of IT systems and the CA's operational network.

[REQ 6.7-11] The CA shall not use systems used for administration of the security policy implementation for other purposes.

[REQ 6.7-12] The CA shall separate the production systems from systems used in development and testing.

[REQ 6.7-13] Firewalls shall be configured to only allow relevant protocols and communication parties and communication between zones shall be restricted to those necessary for the operation. The CA shall explicitly forbid or deactivate unneeded connections and services.

[REQ 6.7-14] The CA shall establish communication between critical systems only through trusted channels that are physically or logically distinct from other communication channels and provide confidentiality, integrity and authenticity between the systems.

[REQ 6.7-15] The CA shall review the established network and firewall rules set on a regular basis.

[REQ 6.7-16] If a high level of availability of external access to the trust service is required, the external network connection shall be redundant.

[REQ 6.7-17] The CA shall perform regular vulnerability scans on external and internal IP addresses. The vulnerability scans shall be performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report. Scans shall be documented.

[REQ 6.7-18] The CA shall perform a penetration test after set up and in case of significant infrastructure or application upgrades or modifications. The penetration test shall be performed by a person or entity with the skills, tools, code of ethics and independence necessary to provide a reliable report. The penetration test shall be documented.

6.8 Time-stamping

[REQ 6.8-01] The CA shall use a reliable time source that must be synchronized with UTC at least once a day. The synchronization source shall be documented in the public part of the CA's CPS.

[REQ 6.8-02] The precise time of significant environmental, key management and clock synchronization events shall be recorded.

7. Certificate, CRL, and OCSP profiles

7.1 Certificate profile

[REQ 7.1-01] The certificates shall meet the requirements specified in Recommendation ITU-T X.509 or IETF RFC 5280.

[REQ 7.1-02] The certificates shall be issued according to ETSI EN 319 412-2.

7.1.1 Version number(s)

[REQ 7.1.1-01] Certificate version number(s) shall be stated and provided as 'V3' (0x2).

7.1.2 Certificate extensions

[REQ 7.1.2-02] All certificates issued under this CP shall contain a non-critical extension qcStatements using the predefined qcStatement-2 in RFC 3739, where all values in sematicsInformation shall be

- semanticsIdentifier: id-etsi-qcs-semanticsId-Legal
- nameRegistrationAuthorities: https://uid.gov.dk (of the type URI generalName)

[REQ 7.1.2-03] All certificates issued under this CP shall contain a non-critical extension authorityKeyIdentifier and shall contain identifier for the issuing CA's public key.

[REQ 7.1.2-04] All certificates issued under this CP shall contain one (and only one) critical or non-critical extension keyUsage with one of the profiles specified in ETSI EN 319 412-2 clause 4.3.2.

[REQ 7.1.2-05] If a certificate issued under this CP contains extension subjectAlternativeName, this extension shall be marked non-critical.

[REQ 7.1.2-06] If a certificate issued after this CP contains extension issuerAlternativeName, this extension shall be marked as non-critical.

[REQ 7.1.2-07] All certificates issued under this CP shall contain a non-critical extension cRLDistributionPoints, that contains at least one reference to a publicly available CRL and least one of the present references shall use the http protocol (http://) IETF RFC 7230-7235.

[REQ 7.1.2-08] All certificates issued under this CP and CA certificates that are not root certificates shall contain a non-critical extension authorityInformationAccess (AIA). AIA shall include at least one accessMethod, id-ad-caIssuers, with accessLocation, that refers to the issuing CA's valid certificate based on either the http or https protocol. Moreover, AIA shall include at least one accessMethod, id-ad-ocsp with accessLocation that refers to a publicly available OCSP-responder that is able to provide valid responses to the certificate status based on either the http or https protocol and that accepts non-signed and non-authenticated status requests.

[REQ 7.1.2-09] No certificates issued under this CP may include the following extensions:

- policyMapping
- subjectDirectoryAttributes
- nameConstraints
- policyConstraints
- inhibitAnyPolicy

Note: See below for further extension requirements.

7.1.3 Algorithm object identifiers

N/A

7.1.4 Name forms

[REQ 7.1.4-01] The designation 'OCES' shall form part of the CA certificates' commonName.

[REQ 7.1.4-02] All certificates issued under this CP shall include a subject field that, as a minimum, must contain:

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

This content shall ensure the uniqueness of the subject.

[REQ 7.1.4-03] countryName shall have the value 'DK'.

[REQ 7.1.4-04] commonName shall include a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA or some other format. Names with spelling other than defined by the registered name may be used.

[REQ 7.1.4-05] The semantics of serialNumber shall be as follows:

UI:DK-xxxxxxxxxxxxxxxx,

where "xxxxxxxxxxxxxxxx" is the subject's UUID as registered in the Danish Agency for Digitisation's UUID numbering service.

[REQ 7.1.4-06] organizationIdentifier must have the following semantics:

VATDK-xxxxxxxx

where "xxxxxxxx" is the CVR number of the subscriber.

[REQ 7.1.4-07] organizationName must contain the subscriber's registered name. It is permitted to omit any company types like 'ApS' and 'Fonden', and it is permitted to use registered secondary names. Finally, it is permitted to abbreviate the registered name if this does not cause any misunderstandings.

7.1.5 Name constraints

[REQ 7.1.5-01] The subject field shall not contain more than one instance of commonName, organizationIdentifier, organizationName and countryName.

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 OIDs may only be referenced in a certificate or written agreement with the Danish Agency for Digitisation, cf. clause 1.1.

[REQ 7.1.6-03] All 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.

[REQ 7.1.6-04] certificatePolicies extension should not be marked as critical.

7.1.7 Usage of Policy Constraints extension

See REQ 7.1.2-08.

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] CRLs shall meet the requirements specified in ISO 9594-8, Recommendation ITU-T X.509 or IETF RFC 5280.

[REQ 7.2-02] **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

There is no requirement to use CRL extensions.

7.3 OCSP profile

[REQ 7.3-01] The OCSP shall be as defined in IETF RFC 6960.

[REQ 7.3-02] The OCSP shall use a profile that complies with IETF RFC 5019.

[REQ 7.3-03] If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder shall not respond with a 'good' status as per clause 2.2 of IETF RFC 6960.

[REQ 7.3-04] The CA should monitor OSCP requests concerning non-issued certificates on the OSCP responder as part of its security response procedures to check if this is an indication of an attack.

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 REQ 7.3-02.

8. Compliance audit and other assessments

8.1 Frequency or 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] 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] 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 Digitisation that it possesses the requisite resources to perform an adequate system audit of the CA. The Danish Agency for Digitisation 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 Digitisation.

[REQ 8.2-02] The CA must make the selected conformity assessment body aware that it in accordance with good auditing practices must perform system audits with respect to the auditing instructions published by the Danish Agency for Digitisation for public certificate policies, 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 the computer-based as well as the manual, are reliable as regards security and checking considerations and in accordance with the CA's CPS.

[REQ 8.2-03] 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 Digitisation 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 Digitisation 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] The Danish Agency for Digitisation 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] Upon changing the conformity assessment body, the CA and the or those withdrawing conformity assessment bodies must each give an explanation to the Danish Agency for Digitisation.

8.3 Assessor's relationship to assessed entity

[REQ 8.3-01] 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] A system audit shall be carried out at the CA. What is to be understood by audit is an audit with respect to the auditing instructions for public certificate policies published by the Danish Agency for Digitisation.

[REQ 8.4-02] 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 8.4-03] 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 8.4-04] 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 8.4-05] 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] 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 Communication of results

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

[REQ 8.6-02] At the end of CA's financial year, the selected conformity assessment body will prepare a report for the CA's management.

[REQ 8.6-03] 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;
- the overall data, system and operational security should be considered as adequate.

9. Other business and legal matters

[REQ 9-01] The CA organization shall be reliable and non-discriminatory.

[REQ 9-02] The CA should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the CA's terms and conditions.

[REQ 9-03] Services and end user products provided by the CA shall be made accessible for persons with disabilities, where feasible and applicable standards on accessibility such as ETSI EN 301 549 should be taken into account.

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 Digitisation.

9.1.5 Refund policy

N/A

9.2 Financial responsibility

9.2.1 Insurance coverage

[REQ 9.2.1-01] The CA shall maintain sufficient financial resources and/or obtain appropriate liability insurance in accordance with applicable law, including eIDAS, to cover liabilities arising from its operations and/or activities.

[REQ 9.2.1-02] If the CA is a private enterprise or a natural person, the CA shall subscribe to and maintain liability insurance, cf. REQ 9.2.1-01. Such insurance shall as a minimum provide a coverage of DKK 25 million per year.

9.2.2 Other assets

[REQ 9.2.2-01] The CA shall have the financial stability and resources required to operate in conformity with this policy.

Note: The above requirements must be assessed in respect of the context in which the CA operates, including but not limited to the number of subscribers and the financial risk undertaken by the CA in respect of the issued certificates.

9.2.3 Insurance or warranty coverage for end-entities

See REQ 9.2.1-01.

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] Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

[REQ 9.4.1-02] Moreover, the confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed CA system components.

[REQ 9.4.1-03] Some data may need to be processed and retained to meet statutory requirements, as well as to support essential business activities. Such data shall be processed and retained in a secure manner.

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

[REQ 9.4.4-01] The CA and RA shall ensure that confidential information is protected from being compromised and must not use confidential information for any purpose other than what is required for operating the CA.

[REQ 9.4.4-02] The CA and RA shall ensure that statistical information about the use of certificates cannot be related to the individual certificate.

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 Digitisation holds all rights to this certificate policy, the OCES name and OCES-OID. Use of OCES-OID 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 Digitisation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

[REQ 9.6.1-01] The CA shall retain overall responsibility for conformance with the certificate policy and information security policy regardless of the use of any subcontractors, including RA. The CA shall set out and ensure efficient implementation of relevant controls at the subcontractors.

[REQ 9.6.1-02] The CA shall provide all its certificate services consistent with its CPS.

[REQ 9.6.1-03] The CA shall in respect of any party reasonably relying on the certificate accept liability according to the general rules of Danish law.

[REQ 9.6.1-04] 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 wilfully.

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

N/A

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] The CA shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about

the provisioning of the services or any other related matters and such policies and procedures shall comply with the CA's terms and conditions, cf. clause 2.1.

9.14 Governing law

[REQ 9.14-01] 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] The CA and RA shall ensure compliance with legislation, including in particular relevant acts regarding the processing of personal information and the eIDAS Regulation.

[REQ 9.15-02] In particular, the CA shall provide evidence of how it meets applicable data protection legislation within its registration process.

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 (attorneys' fees and waiver of rights)

N/A

9.16.5 Force Majeure

N/A

9.17 Other provisions

[REQ 9.17-01] The CA shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

[REQ 9.17-02] The parts of the CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies.

[REQ 9.17-03] In particular, the senior executive, senior staff and staff in trusted roles of the CA concerned with certificate generation and revocation management shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

[REQ 9.17-04] The parts of the CA's organization concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

[REQ 9.17-05] The CA shall provide the capability to allow third parties to check and test all the certificate types that the CA issues.

[REQ 9.17-06] Any test certificates should clearly indicate that they are for testing purposes.

Note: E.g. the used CA that issues certificates for testing purposes may include the word 'test' in commonName.

[REQ 9.17-07] Certificates for testing purposes may not be issued under the same root CA as certificates for subjects.

Annex A

Fulfilment of this CP is a requirement for NCP established in ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-1, ETSI EN 319 412-2 and ETSI EN 319 412-3.

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

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

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

REQ 3.2.2-02					
REQ 3.2.2-03					
REQ 3.2.2-04		REG-6.2.2-13 REG-6.2.2-15			
REQ 3.2.2-05		REG-6.2.2-16 REG-6.2.2-17			
REQ 3.2.4-01		REG-6.2.2-21			
REQ 3.3-01		REG-6.2.3-01			
REQ 3.3-02		REG-6.2.3-08			
REQ 3.3-03		REG-6.2.3-09			
REQ 3.3.1-01		REG-6.2.3-02			
REQ 3.3.2-01		REG-6.2.3-02			
REQ 3.4-01		REV-6.2.4-09			
REQ 3.4-02		REV-6.2.4-01			
REQ 4.1.1-01					
REQ 4.1.2-01		REG-6.3.2-01			
REQ 4.1.2-02		REG-6.3.2-02			
REQ 4.1.2-03	REQ-6.2-01 REQ-6.2-03				
REQ 4.1.2-04		REG-6.3.1-01			
REQ 4.2.1-01					
REQ 4.2.2-01					
REQ 4.2.3-01					
REQ 4.3.1-01		GEN-6.3.3-01			

REQ 4.3.1-02		GEN-6.3.3-02			
REQ 4.3.1-03		GEN-6.3.3-03			
REQ 4.3.1-04		GEN-6.3.3-04			
REQ 4.3.1-05		GEN-6.3.3-05 GEN-6.3.3-06			
REQ 4.3.1-06		GEN-6.3.3-07			
REQ 4.3.1-07		SDP-6.3.3-08			
REQ 4.3.1-08		GEN-6.3.3-10			
REQ 4.3.1-10		GEN-6.3.3-12			
REQ 4.3.2-01					
REQ 4.4.1-01		OVR-6.3.4-01			
REQ 4.4.1-02		REG-6.3.4-02			
REQ 4.4.1-04		OVR-6.3.4-04			
REQ 4.4.1-05		OVR-6.3.4-05			
REQ 4.4.1-06		OVR-6.3.4-06			
REQ 4.4.1-08		REG-6.3.4-08			
REQ 4.4.1-09		REG-6.3.4-12 REG-6.3.4-13			
REQ 4.4.1-12		REG-6.3.4-16			
REQ 4.4.1-13		REG-6.3.4-17			
REQ 4.4.2-01					
REQ 4.4.3-01					
REQ 4.5.1-01		OVR-6.3.5-01			
REQ 4.5.2-01		OVR-6.3.5-03			

REQ 4.6.2-01					
REQ 4.6.3-01		REG-6.3.6-01			
REQ 4.6.3-02		REG-6.3.6-02			
REQ 4.6.3-03		REG-6.3.6-08			
REQ 4.6.3-04		REG-6.3.6-09			
REQ 4.6.3-05		GEN-6.3.6-10			
REQ 4.6.4-01					
REQ 4.6.5-01					
REQ 4.6.6-01					
REQ 4.6.7-01					
REQ 4.7.1-01					
REQ 4.7.1-02					
REQ 4.7.1-03					
REQ 4.7.1-04					
REQ 4.7.2-01					
REQ 4.7.3-01					
REQ 4.7.3-02					
REQ 4.7.4-01					
REQ 4.7.5-01					
REQ 4.7.6-01					
REQ 4.7.7-01					
REQ 4.8.1-01		REG-6.3.8-01			
REQ 4.8.2-01					
REQ 4.8.3-01		REG-6.3.8-02			

REQ 4.8.4-01					
REQ 4.8.5-01					
REQ 4.8.6-01					
REQ 4.8.7-01					
REQ 4.9.1-01		REV-6.2.4-03			
REQ 4.9.1-02					
REQ 4.9.1-03					
REQ 4.9.1-04		REV-6.3.9-03			
REQ 4.9.2-01					
REQ 4.9.3-01		REV-6.3.9-01			
REQ 4.9.3-02					
REQ 4.9.3-03		REV-6.3.9-02			
REQ 4.9.3-04					
REQ 4.9.3-05					
REQ 4.9.4-01					
REQ 4.9.5-01		REV-6.2.4-08			
REQ 4.9.5-02					
REQ 4.9.5-03		REV-6.2.4-05			
REQ 4.9.5-04		REV-6.2.4-06			
REQ 4.9.5-05		REV-6.2.4-07			
REQ 4.9.7-01		CSS-6.3.9-04			
REQ 4.9.7-02		CSS-6.3.9-05			
REQ 4.9.7-03		CSS-6.3.9-11			
REQ 4.9.7-04		CSS-6.3.9-12			

REQ 4.9.7-05		CSS-6.3.9-06			
REQ 4.9.7-06		CSS-6.3.9-13			
REQ 4.9.8-01					
REQ 4.9.9-01					
REQ 4.9.11-01					
REQ 4.9.13-01					
REQ 4.10-01		CSS-6.3.10-01			
REQ 4.10.1-02		CSS-6.3.10-03			
REQ 4.10.1-03		CSS-6.3.10-05			
REQ 4.10.1-04		CSS-6.3.10-04			
REQ 4.10.1-07		CSS-6.3.10-07			
REQ 4.10.1-08					
REQ 4.10.1-09		CSS-6.3.10-08 CSS-6.3.10-09			
REQ 4.10.1-10					
REQ 4.10.1-11					
REQ 4.10.1-12					
REQ 4.10.1-13					
REQ 4.10.2-01		CSS-6.3.10-02			
REQ 4.10.2-02					
REQ 4.10.2-03		CSS-6.3.10-10			
REQ 4.12.1-01					
REQ 5-01	REQ-7.13-01				
REQ 5-02	REQ-5-01				

REQ 5-03	REQ-5-02				
REQ 5-04	REQ-5-03				
REQ 5-05	REQ-5-04				
REQ 5-06	REQ-5-05				
REQ 5-07	REQ-7.3.1-01 REQ-7.3.1-02				
REQ 5-08	REQ-7.4-01				
REQ 5.1-01	REQ-7.6-01				
REQ 5.1-02	REQ-7.6-03 REQ-7.6-04				
REQ 5.1-03		OVR-6.4.2-07			
REQ 5.1-04		OVR-6.4.2-08			
REQ 5.1-05		OVR-6.4.2-09			
REQ 5.1.1-01					
REQ 5.1.1-02	REQ-7.6-02				
REQ 5.1.1-03	REQ-7.8-02				
REQ 5.1.1-04					
REQ 5.1.2-01					
REQ 5.1.2-02	REQ-7.6-05				
REQ 5.1.2-03		OVR-6.4.2-05			
REQ 5.1.2-04		OVR-6.4.2-02			
REQ 5.1.2-05	REQ-7.8-04				
REQ 5.1.2-06					
REQ 5.1.2-07		OVR-6.4.2-10			

REQ 5.1.2-08		OVR-6.4.2-06			
REQ 5.1.2-09					
REQ 5.1.2-10					
REQ 5.1.2-11		OVR-6.4.2-03			
REQ 5.1.2-12		OVR-6.4.2-11			
REQ 5.1.2-13		OVR-6.4.2-04			
REQ 5.1.6-01	REQ-7.3.2-01 REQ-7.4-10 REQ-7.7-06	OVR-6.4.3-01			
REQ 5.1.6-02	REQ-7.7-07				
REQ 5.1.7-01	REQ-7.3.2-01				
REQ 5.1.8-01					
REQ 5.2.1-01	REQ-7.2-07 REQ-7.2-08				
REQ 5.2.1-02	REQ-7.7-08				
REQ 5.2.1-03	REQ-7.2-14				
REQ 5.2.1-04	REQ-7.2-15	OVR-6.4.4-02			
REQ 5.2.1-05	REQ-7.1.2-01				
REQ 5.2.2-01		GEN-6.4.3-02			
REQ 5.2.3-01	REQ-7.2-16				
REQ 5.2.3-02	REQ-7.2-09				
REQ 5.2.3-03	REQ-7.2-10				
REQ 5.2.3-04	REQ-7.2-11				
REQ 5.2.3-05	REQ-7.2-17				

REQ 5.2.4-01					
REQ 5.3-01	REQ-7.2-01				
REQ 5.3.1-01	REQ-7.2-02				
REQ 5.3.1-02	REQ-7.2-13				
REQ 5.3.1-03	REQ-7.2-06				
REQ 5.3.2-01	REQ-7.4-08				
REQ 5.3.2-02					
REQ 5.3.3.-01	REQ-7.2-03				
REQ 5.3.3.-02					
REQ 5.3.4-01	REQ-7.2-04				
REQ 5.3.6-01	REQ-7.2-12				
REQ 5.3.6-02	REQ-7.2-05				
REQ 5.3.7-01					
REQ 5.4.1-01		OVR-6.4.5-02			
REQ 5.4.1-02		REG-6.4.5-03			
REQ 5.4.1-03		GEN-6.4.5-06			
REQ 5.4.1-04		GEN-6.4.5-07			
REQ 5.4.1-05		GEN-6.4.5-08			
REQ 5.4.1-06		REV-6.4.5-09			
REQ 5.4.1-07					
REQ 5.4.2-01					
REQ 5.4.3-01		OVR-6.4.6-01			
REQ 5.4.3-02					

REQ 5.4.4-01	REQ-7.10-02 REQ-7.10-08				
REQ 5.4.4-02		REG-6.4.5-05			
REQ 5.4.5-01					
REQ 5.5-01					
REQ 5.5-02					
REQ 5.5.1-01	REQ-7.10-01				
REQ 5.5.1-02		REG-6.4.5-04			
REQ 5.5.1-03					
REQ 5.5.1-04					
REQ 5.5.2-01	REQ-7.10-07				
REQ 5.5.2-02		OVR-6.4.6-01			
REQ 5.5.3-01	REQ-7.10-02				
REQ 5.5.3-02	REQ-7.10-03				
REQ 5.5.4-01		OVR-6.4.8-03			
REQ 5.5.4-02		OVR-6.4.8-04			
REQ 5.5.4-03		OVR-6.4.8-02			
REQ 5.5.4-04		OVR-6.4.8-05			
REQ 5.5.4-05		OVR-6.4.8-06			
REQ 5.5.4-06		OVR-6.4.8-07			
REQ 5.5.7-01	REQ-7.10-04				
REQ 5.6-01					

REQ 5.7-01					
REQ 5.7.1-01	REQ-7.9-01				
REQ 5.7.1-02	REQ-7.9-02				
REQ 5.7.1-03	REQ-7.9-03				
REQ 5.7.1-04	REQ-7.9-04				
REQ 5.7.1-05	REQ-7.9-05				
REQ 5.7.1-06	REQ-7.9-06				
REQ 5.7.1-07	REQ-7.9-07				
REQ 5.7.1-08	REQ-7.9-08				
REQ 5.7.1-09	REQ-7.9-09				
REQ 5.7.1-10	REQ-7.9-10				
REQ 5.7.1-11	REQ-7.9-11				
REQ 5.7.1-12	REQ-7.9-12				
REQ 5.7.2-01					
REQ 5.7.2-02					
REQ 5.7.3-01		OVR-6.4.8-08			
REQ 5.7.3-02		OVR-6.4.8-09			
REQ 5.7.3-03		OVR-6.4.8-11 OVR-6.4.8-12 OVR-6.4.8-13 OVR-6.4.8-14			
REQ 5.7.3-04		OVR-6.4.8-15			
REQ 5.7.3-05		OVR-6.4.8-16			
REQ 5.7.3-06					

REQ 5.7.4-01	REQ-7.11-01				
REQ 5.7.4-02	REQ-7.11-02				
REQ 5.7.4-03		OVR-6.4.8-10			
REQ 5.8-01	REQ-7.12-02				
REQ 5.8-02	REQ-6.1-11 REQ-7.12-10	OVR-6.4.9-03			
REQ 5.8-03	REQ-7.12-03 REQ-7.12-04				
REQ 5.8-04					
REQ 5.8-05	REQ-7.12-01 REQ-7.12-11				
REQ 5.8-06	REQ-7.12-06	OVR-6.4.9-02			
REQ 5.8-07	REQ-7.12-05				
REQ 5.8-08	REQ-7.12-07				
REQ 5.8-09	REQ-7.12-08				
REQ 5.8-10		OVR-6.4.9-04			
REQ 5.8-11	REQ-7.12-09				
REQ 6.1.1-01					
REQ 6.1.1-02	REQ-7.5-01				
REQ 6.1.1-03					
REQ 6.1.1-04		GEN-6.5.1-02			
REQ 6.1.1-05		GEN-6.5.1-03 GEN-6.5.1-04 GEN-6.5.1-05			

		GEN-6.5.1-06 GEN-6.5.1-07			
REQ 6.1.1-06		GEN-6.5.1-08			
REQ 6.1.1-07		GEN-6.5.1-09			
REQ 6.1.1-08		GEN-6.5.1-10			
REQ 6.1.1-09		GEN-6.5.1-11			
REQ 6.1.1-10		GEN-6.5.1-12			
REQ 6.1.1-11		GEN-6.5.1-13			
REQ 6.1.1-12		GEN-6.5.1-14			
REQ 6.1.1-13					
REQ 6.1.1-14		SDP-6.5.1-17			
REQ 6.1.1-15		SDP-6.5.1-18			
REQ 6.1.1-16		SDP-6.5.1-19			
REQ 6.1.2-01		SDP-6.5.1-20			
REQ 6.1.2-02		SDP-6.5.1-21			
REQ 6.1.2-03		SDP-6.5.1-22			
REQ 6.1.3-01					
REQ 6.1.4-01		DIS-6.5.1-16			
REQ 6.1.4-02					
REQ 6.1.7-01					
REQ 6.2-01					
REQ 6.2.1-01		OVR-6.5.2-01 OVR-6.5.2-03			
REQ 6.2.1-02		OVR-6.5.2-02			

REQ 6.2.1-03					
REQ 6.2.1-04					
REQ 6.2.1-05					
REQ 6.2.1-06					
REQ 6.2.1-07		GEN-6.5.2-04			
REQ 6.2.4-01		GEN-6.5.2-06			
REQ 6.2.4-02		GEN-6.5.2-07			
REQ 6.2.4-03		GEN-6.5.2-08			
REQ 6.2.5-01		GEN-6.5.2-05			
REQ 6.2.6-01					
REQ 6.2.6-02					
REQ 6.2.7-01		GEN-6.5.2-09			
REQ 6.2.7-02		OVR-6.5.2-10			
REQ 6.2.7-03		OVR-6.5.2-11			
REQ 6.2.7-04		OVR-6.5.2-12			
REQ 6.2.8-01					
REQ 6.2.10-01		GEN-6.5.2-13			
REQ 6.3-01		OVR-6.5.3-01 OVR-6.5.3-02 GEN-6.5.3-03 GEN-6.5.3-04 GEN-6.5.3-05 GEN-6.5.3-06 GEN-6.5.3-07			

REQ 6.4.1-01		SDP-6.5.4-02			
REQ 6.4.1-02					
REQ 6.4.1-03					
REQ 6.4.1-04					
REQ 6.4.2-01		SDP-6.5.4-03			
REQ 6.4.3-01		GEN-6.5.4-01			
REQ 6.4.3-02		GEN-6.5.5-04			
REQ 6.5.1-01	REQ-7.4-07				
REQ 6.5.1-02	REQ-7.7-03 REQ-7.7-04				
REQ 6.5.1-03	REQ-7.7-05 REQ-7.7-09				
REQ 6.5.1-04		DIS-6.5.5-05			
REQ 6.5.1-05		CSS-6.5.5-06			
REQ 6.5.1-06		OVR-6.5.5-07			
REQ 6.6.1-01	REQ-7.7-01				
REQ 6.6.1-02	REQ-7.7-02				
REQ 6.6.2-01					
REQ 6.6.2-02	REQ-6.3-01				
REQ 6.6.2-03	REQ-6.3-02				
REQ 6.6.2-04	REQ-6.3-03				
REQ 6.6.2-05	REQ-6.3-04				
REQ 6.6.2-06	REQ-6.3-07				
REQ 6.6.2-07	REQ-6.3-08				

REQ 6.6.2-08	REQ-6.3-09				
REQ 6.6.2-09					
REQ 6.6.2-10	REQ-6.3-10				
REQ 6.6.3-01	REQ-7.4-04				
REQ 6.6.3-02	REQ-7.4-05				
REQ 6.6.3-03	REQ-7.4-06				
REQ 6.6.3-04	REQ-7.4-08				
REQ 6.6.3-05	REQ-7.4-09				
REQ 6.6.3-06		OVR-6.5.6-02			
REQ 6.7-01	REQ-7.4-02 REQ-7.8-01				
REQ 6.7-02	REQ-7.8-02				
REQ 6.7-03		OVR-6.5.7-02			
REQ 6.7-04		OVR-6.5.7-03			
REQ 6.7-05		GEN-6.5.5-02			
REQ 6.7-06		GEN-6.5.5-03			
REQ 6.7-07	REQ-7.8-03				
REQ 6.7-08	REQ-7.8-07	OVR-6.5.7-05			
REQ 6.7-09		OVR-6.5.7-04			
REQ 6.7-10	REQ-7.8-08				
REQ 6.7-11	REQ-7.8-09				
REQ 6.7-12	REQ-7.8-10				
REQ 6.7-13	REQ-7.4-03				

	REQ-7.8-04 REQ-7.8-05				
REQ 6.7-14	REQ-7.8-11				
REQ 6.7-15	REQ-7.8-06				
REQ 6.7-16	REQ-7.8-12				
REQ 6.7-17	REQ-7.8-13				
REQ 6.7-18	REQ-7.8-14 REQ-7.8-15				
REQ 6.8-01	REQ-7.10-06				
REQ 6.8-02	REQ-7.10-05				
REQ 7.1-01		GEN-6.6.1-01			
REQ 7.1-02		GEN-6.6.1-02			
REQ 7.1.1-01					
REQ 7.1.2-02			Clause 5.1.4		
REQ 7.1.2-03				Clause 4.3.1	
REQ 7.1.2-04				Clause 4.3.2	
REQ 7.1.2-05				Clause 4.3.5	
REQ 7.1.2-06				Clause 4.3.6	
REQ 7.1.2-07				Clause 4.3.11	
REQ 7.1.2-08				Clause 4.4.1	
REQ 7.1.2-09				Clause 4.3.4 + 4.3.7 + 4.3.8 + 4.3.9 + 4.3.12	
REQ 7.1.4-01					
REQ 7.1.4-02					Clause 4.2.1

REQ 7.1.4-03					Clause 4.2.1
REQ 7.1.4-04					Clause 4.2.1
REQ 7.1.4-05			Clause 5.1.3		
REQ 7.1.4-06			Clause 5.1.4	Clause 4.2.4	Clause 4.2.1
REQ 7.1.4-07					Clause 4.2.1
REQ 7.1.5-01					Clause 4.2.1
REQ 7.1.6-01					
REQ 7.1.6-02					
REQ 7.1.6-03					
REQ 7.1.6-04				Clause 4.3.3	
REQ 7.2-01		OVR-6.6.2-01			
REQ 7.2-02					
REQ 7.2.1-01					
REQ 7.3-01		OVR-6.6.3-01			
REQ 7.3-02					
REQ 7.3-03		OVR-6.6.3-02			
REQ 7.3-04		OVR-6.6.3-03			
REQ 7.3.1-01					
REQ 8.1-01					
REQ 8.1-02					
REQ 8.2-01					
REQ 8.2-02					
REQ 8.2-03					
REQ 8.2-04					

REQ 8.2-05					
REQ 8.3-01					
REQ 8.4-01					
REQ 8.4-02					
REQ 8.4-03					
REQ 8.4-04					
REQ 8.4-05	REQ-7.13-02				
REQ 8.5-01					
REQ 8.6-01					
REQ 8.6-02					
REQ 8.6-03					
REQ 9-01	REQ-7.1.1-01 REQ-7.1.1-02				
REQ 9-02	REQ-7.1.1-03				
REQ 9-03	REQ-7.13-03 REQ-7.13-04				
REQ 9.1.4-01					
REQ 9.2.1-01	REQ-7.1.1-04				
REQ 9.2.1-02					
REQ 9.2.2-01	REQ-7.1.1-05				
REQ 9.4.1-01	REQ-7.13-05				
REQ 9.4.1-02		OVR-6.8.4-02			
REQ 9.4.1-03		OVR-6.8.4-03			
REQ 9.4.4-01					

REQ 9.4.4-02					
REQ 9.4.5-01					
REQ 9.5-01					
REQ 9.6.1-01	REQ-6.3-05 REQ-6.3-06				
REQ 9.6.1-02		OVR-6.8.6-02			
REQ 9.6.1-03					
REQ 9.6.1-04					
REQ 9.8-01					
REQ 9.8-02					
REQ 9.11-01					
REQ 9.13-01	REQ-7.1.1-06	OVR-6.8.13-01			
REQ 9.14-01					
REQ 9.15-01					
REQ 9.15-02		REG-6.2.2-22			
REQ 9.17-01	REQ-7.1.1-07				
REQ 9.17-02		OVR-6.9.1-02			
REQ 9.17-03		OVR-6.9.1-03			
REQ 9.17-04		OVR-6.9.1-04			
REQ 9.17-05		OVR-6.9.2-01			
REQ 9.17-06		OVR-6.9.2-02			
REQ 9.17-07					