DIGITALISERINGSSTYRELSEN

Den Danske Stat
Certification Practice Statement

Contents

Changelog

Date	Version	Change description
30-9-2021	1.0	Support for Signing with qualified certificates issued to natural persons.

References

Term	Reference
[BCP]	Business Continuity Plan
[CEN EN 419 241-2]	Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, CEN.
[CEN EN 419 221-5]	Protection profiles for TSP Cryptographic modules - Part 5, Cryptographic Module for Trust Services, CEN.
[CERTPROF]	Certificate Profiles, Den Danske Stat, Digitaliseringsstyrelsen, Version 1.0.5, september 2021. https://www.ca1.gov.dk/practice/
[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
[eIDAS 1502]	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[ENISA]	Algorithms, key size and parameters report – 2014, ENISA, November 2014. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
[ETSI TS 119 312]	ETSI TS 119 312, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, ETSI ESI, Version 1.3.1, February 2019. https://www.etsi.org/standards
[ETSI EN 319 411-1]	ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, ETSI ESI, Version 1.3.1, May 2021. https://www.etsi.org/standards
[ETSI EN 319 412-2]	ETSI EN 319 412-2, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons, ETSI ESI, Version 2.2.1, July 2020. https://www.etsi.org/standards
[FIPS 140-2]	FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, National Institute of Standards and Technology (NIST), USA, May 2001
[FIPS 186-4]	FIPS PUB 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), USA, July 2013
[OCES Employee]	Certificate Policy for OCES employee certificates (Public Certificates for Electronic Service). Digitaliseringsstyrelsen. Version 7.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[OCES Organization]	Certificate Policy for OCES organizational certificates (Public Certificates for Electronic Services). Digitaliseringsstyrelsen. Version 7.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[PDS]	PKI Disclosure Statement annex A in ETSI EN 319 411-1
[Signing Service]	Den Danske Stat Trust Services, Signing Service. https://www.ca1.gov.dk/practice/

[QSCD-list]	Compiled list of Qualified electronic Signature Creation Devices (QSigCDs) as defined in point 23 of Article 2 of Regulation 910/2014, Qualified electronic Seal Creation Devices (QSealCDs) as defined in point 32 of Article 2 of Regulation 910/2014, and Secure Signature Creation Devices (SSCDs) benefiting from the transitional measure set in Article 51(1) of Regulation 910/2014. https://esignature.ec.europa.eu/efda/home/#/screen/home
[Qualified Employee]	Certificate Policy for qualified employee certificates. Digitaliseringsstyrelsen. Version 1.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[Qualified Organization]	Public Certificate Policy for qualified organizational certificates. Digitaliseringsstyrelsen. Version 1.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[Qualified Person]	Public Certificate for qualified person certificates. Digitaliseringsstyrelsen. Version 1.0, October 2019. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[Revocation Procedures]	Den Danske Stat Trust Services, Revocation Procedures, are described at: https://certifikat.gov.dk/revocation
[RFC3647]	Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, Network Working Group, IETF Network Working Group, Request for Comments: 3647, November 2003, https://tools.ietf.org/html/rfc3647
[RFC5019]	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, Network Working Group, Request for Comments: 5019, September 2007, https://datatracker.ietf.org/doc/html/rfc5019
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF Network Working Group, Request for Comments: 5280, May 2008, https://tools.ietf.org/html/rfc5280
[RFC6960]	X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP, Internet Engineering Task Force (IETF), Request for Comments: 6960, June 2013, https://datatracker.ietf.org/doc/html/rfc6960
[T&C]	Den Danske Stat Trust Services, Terms and Conditions, Digitaliseringsstyrelsen, Version - covered by [PQTERMSDK] and [PQTERMSUK]
[PQTERMSDK]	Vilkår - QC personcertifikat
[PQTERMSUK]	Terms Qualified Person Certificates

1 Introduction

1.1 Overview

The Agency for Digitisation has established a trust service provider Den Danske Stat, which provides certification services which meets the requirements described in the eIDAS regulation [eIDAS] for qualified and non-qualified certificates.
The purpose is to provide end users in Denmark with an infrastructure that can offer certificates for electronic signatures, electronic seals, mail encryption and authentication to secure applications within public and private organisations.

Den Danske Stat provides a series of trust services and acts as Certification Authority, Time Stamp Authority and Validation Authority. With the special status under the regulation [eIDAS], that remote signing is not a recognised as trust service, the remote signing service offered by Den Danske Stat is managed as part of the Certification Authority, where the CA generate, manage and use the subscribers signing key on the sole control of the signer.
This document, being a CPS, describes Participants of the Certification Authority. There is a supplementary document describing the Signing Service and other practice documents describing the other trust services.

The provided infrastructure uses two certificate hierarchies to issue qualified and public certificate for electronic services. Qualified certificates are issued to persons, employees and organizations using the certificate policies referenced in [Qualified Person/Employee/Organizations]. Non-qualified public certificates for electronic services are issued to employees and organizations using the certificate policies in [OCES Employee/Organization].
In all CA certificates, the trust service provider Den Danske Stat is referenced as the legal entity, which acts as certification authority and bears the responsibility and liability for the CAs, and the services used to provide certification services.

1.2 Document name and identification

This version of the CPS can be identified through the OID iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) practice-statements(2) cps(1) major-ver(1) minor-ver(0).

1.3 PKI participants

The PKI Participants of the Den Danske Stat are the entities which consumes services or provides services which allows the Den Danske Stat to provide certification services.

The PKI Participants are identified as the following:

- Certificate Authorities
- Registration Authorities (eID Services)
- Subscribers
- Relying Parties
- Other Participants
    - Qualified Signing Service
    - Certificate Revocation Service
    - Certificate Revocation Status Service
    - Repository Services

1.3.1 Certificate authorities

The Den Danske Stat issues certificates in two key hierarchies for qualified and OCES Certificates. The top level in each key hierarchy is always a self-signed root certificate. Each root certificate issues subordinate CA certificate to issue subject certificates.
Beside issuing subject certificate, the CA system also provides OCSP and time stamp service certificates as illustrated below. Certificates marked with underline are planned for future versions.

- Qualified Root
  - Qualified intermediate
    - Qualified person
    - Qualified employee
    - Qualified Organization
    - Qualified OCSP Responder for subject certificates
  - Time Stamp certificates
  - Qualified OCSP Responder for CA certificates
- OCES Root
  - OCES intermediate
    - OCES employee
    - OCES organization
    - OCES OCSP Responder for subject certificates
  - OCES OCSP Responder for CA certificates

The Den Danske Stat has been assessed for conformity under the regulation [eIDAS] and to meet the requirement in the relevant certificate policies by an accredited conformity assessment body.
The conformity assessment report created by the conformity assessment body has been reviewed by the Danish supervisory body and the status granted to operate its services has been issued.

[REQ 1.3.1-01] The CA organization must be reliable.
Den Danske Stat fulfils all applicable requirements in the relevant CP's.

[REQ 1.3.1-02] The CA must be a natural person or legal entity.
Den Danske Stat, formally The Agency for Digitalisation on behalf of the Danish State.

[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.
Den Danske Stat relies on eID services provided by MitID. In addition, Den Danske Stat has entered contractual agreements with other subcontractors for the operation of the qualified trust services.
Den Danske Stat ensures that relevant policy requirements are identified and met by these services.
Den Danske Stat uses MitID eID service to provide registration information. The registration information received are compliant with eIDAS see 1.3.2.1 eIDAS article 24.1.

[REQ 1.3.1-04] The CA may sub-certify its public root key under other parent CAs. The root key of a CA may also sub-certify the public key of another subordinate CA if it is a qualified trust service. The root CA is responsible for ensuring that any subordinate CA complies with the eIDAS requirements for qualified trust services issuing qualified certificates.
The root CA is not sub-certified by other CAs nor does it sub-certify other CAs.

1.3.2 Registration authorities

Den Danske Stat issues short term qualified person certificates as part of the remote signing service. During the signing session, the signee is redirected to the Login Service for authentication. The Login Service acts as a broker for MitID and redirects the signee to MitID for authentication. Once the signee is authenticated by MitID information is provided back to the Login Service and from there to the signing service.
The signing service uses the signee attributes received form the Login Service to create a certification request which is provided to the CPS.

1.3.2.1 eIDAS article 24.1

Before a qualified certificate can be issued, the CA shall ensure that the requirement in [eIDAS], article 24 are fulfilled. In particular, the CA is responsible for verification of the identity and special attributes associated with the subject.
Since all subject identities eligible to use the signing service and as part of that receive a certificate, will be authenticated using the national infrastructures in MitID as identity providers, the equivalent assurance for these identity providers in terms of reliability to physical presence has been assessed by a conformity assessment body and the result used in the assessment of the qualified trust service for the certificate services.
The assurance level received from the identity providers as part of subject authentication is required to be at least substantial in order to receive a certificate.

[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.

See section 1.3.2 Registration authorities.

1.3.3 Subscribers

The Subscribers of Qualified Person certificates are natural persons, which uses an electronic identification means meeting the requirements in [eIDAS] with an assurance level at least substantial. See also
Subscribers are eligible for receiving Qualified Person Certificates provided they comply with the Terms and Conditions [T&C] and referenced Certificate Policy presented prior certificate issuing and which covers subscriber's obligations.
In this document subject and subscriber are used interchangeably.

1.3.4 Relying parties

The Relying Parties of certificates issued by the Den Danske Stat are natural and legal persons, who relies on the certificate content and services provided by Den Danske Stat.
Before a received certificate from Den Danske Stat is used, the relying party shall ensure:

- The certificate meets the format and algorithm as described in [CERTPROF].
- The validity of the certificate is checked through the certificate revocation services (e.g. CRL and OCSP) mentioned in section 7.
- The certificate policy extension OIDs reflects a certificate policy which targets the context for usage of the certificate.

In addition, Relying Parties shall comply with their Terms and Conditions [T&C] as stated in this CPS.

1.3.5 Other participants

1.3.5.1 Qualified Signing Service

The remote signing service provided by Den Danske Stat offers subscribers to generate qualified electronic signature under this CPS and in conformance with [eIDAS].
The signing service uses MitID as identity provider, see 1.3.2.
The signing service is described in detail in [Signing Service].

1.3.5.2 Certificate Revocation

Subscribers can revoke their certificates using the self-service portal. The Subscriber must log-in using credentials matching the certificates Subject SerialNumber.
Once logged in, the Subscriber can revoke matching certificates, which are not expired.
Subscribers also have the option, to request revocation using these channels:

1) Telephone: 3392 5200
2) Letter:
   Digitaliseringsstyrelsen
   att. CA Forvaltningen

Postboks 2193
1017 København K

1.3.5.3 Certificate revocation status Services Provider

Provision of Certificate revocation status service under this CPS and in compliance with relevant certificate policies is ensured by the infrastructure provided by Den Danske Stat.

1.3.5.4 Repository Services

Den Danske Stat provides a publication service for all versions of this CPS and other documents including Certificate Profiles, Terms and Conditions [T&C] and other related documents and it is available at https://ca1.gov.dk/

1.4 Certificate usage

1.4.1 Appropriate certificate uses

[REQ 1.4.1-01] A qualified person certificate issued under this CP may be used to secure sender and message authenticity, including qualified signature and message integrity. It may also be used to ensure confidentiality (encryption).
The certificates can be used for securing sender authenticity and message authenticity and integrity as set forth in the Terms and Conditions [T&C].

[REQ 1.4.1-02] Certificates issued under this CP may be valid for a period of maximum 4 years.
The validity of subject certificates is described [CERTPROF], which states that certificates are issued with a validity ranging from 10 days to 3 years.

1.4.2 Prohibited certificate uses

[REQ 1.4.2-02] Certificates issued under this CP must not be used to sign other certificates.
Subject certificates shall not be used for signing subordinate certificates as expressed in the certificate extension basicConstraints where CA is set to FALSE. See [CERTPROF] for details.

[REQ 1.4.2-03] The subject's private key must not be used without being authorized in each individual case by the subject through the use of activation data. This means that storing keys in automated systems which use them on behalf of the subject is not allowed.
Subjects must protect the activation data for the certificates to ensure sole control as set forth in the Terms and Conditions [T&C].
Short-term certificates are issued through the signature service, which relies on an identity assertion provided by an identity provider assessed to [eIDAS] Level of Assurance at least substantial.
The Qualified Signature Creation Device manage the subjects private key and short-term certificate under the subject's sole control. Once the private key has been used to sign a document, it is immediately deleted. This ensures that a certificate can only be used once and that the private key cannot be compromised. The private key is either deleted when the signing session is deleted after successful signing or when the session expires. In both cases it is handled by the signing service.

[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.
The subject's usage of private key is specified in the certificate extension keyUsage, [CERTPROF] as set forth in the Terms and Conditions [T&C].

1.5 Policy administration

1.5.1 Organization administrating the document

Agency for Digitalisation on behalf of the Danish State.

1.5.2 Contact person

Head of Trust Services Administration.

1.5.3 Person determining CPS suitability for the policy

[REQ 1.5.3-01] The CA may issue qualified certificates under this CP if the CA is registered with the Danish Agency for Digitisation, cf. eIDAS Article 21.
Den Danske Stat does not issue any qualified certificates before a qualified service provider status has been granted by the Danish eIDAS Supervisory Authority.

[REQ 1.5.3-02] The CA shall present a conformity assessment report to the Danish Agency for Digitisation at least once a year.
Den Danske Stat provides a conformity assessment report each year to the Danish Supervisory Body within the Danish Agency for Digitisation.

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.
Den Danske Stat has defined and maintain a certificate practices statement (CPS), this document, which address all requirements in the applicable certificate policies.
The CPS is a practise statement and follows the [RFC3647] outline and includes all applicable requirements sections in the relevant CP's for all CA-hierarchies in the PKI System.
When requirements in the [RFC3647] structure are not applicable to the services provided by Den Danske Stat it is either because:

i) the policy requirements are optional and not used; or
ii) ii) the policy requirements in the used policies are not containing any requirement in said [RFC3647].

The CPS is communicated when approved by Den Danske Stat as suitable statements for the implemented CP's. New versions of CPS are edited when new CP's are published, or implementation changed. CPS's are published in English.

[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.
Den Danske Stat uses the included framework with the [RFC3647] structure and the audit guidance to structure the CPS to be able to measure the efficiency, quality, and security.
The CPS describes practises that are common to all CP's. The CPS level of specificity follows [ETSI EN 319 411-1] section 4.2.3 and [RFC3647] section 3.6, thus using references to internal documents when appropriate to allow publication of CPS.

[REQ 1.5.4-03] The CPS shall include the complete CA hierarchy, including root and subordinate CAs.
Section 1.3.1 describes the complete CA hierarchy offered by Den Danske Stat.
A CA hierarchy under this CPS consists of a root CA and one or more intermediate CAs. Root CAs only issue certificates to intermediate CAs and intermediate CAs issues certificates to subjects.

[REQ 1.5.4-04] The CPS must be structured according to the guidelines in RFC 3647.
This CPS is organized according to the guidelines in [RFC3647] section 6 in order to facilitate comparison of this CPS with corresponding requirements in the relevant CPs.
The CPS follows the [RFC3647] outline.

[REQ 1.5.4-05] The CPS must be in Danish or English.
This CPS is in English but internal procedures and documents may be written in either Danish or English as they are out of scope of this document.
CPS's are published in 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.

The certificate profile [CERTPROF] document is published on the same website as CPS and describes the signature parameters for all usages of root, intermediate certificates and OCSP responder certificates when issuing certificates, CRLs and OCSP responses.

[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.
Den Danske Stat management approves the CPS and ensures correct implementation. After approval the CPS is communicated to relevant employees and subcontractors.
The CPS is published to https://ca1.gov.dk.

[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.
This CPS is reviewed at least once every year. Den Danske Stat management is responsible for the review. Any change is documented, and historic versions of the CPS is archived for at least seven years after they are replaced.
The CPS is reviewed at least once a year prior to the regular annual conformity assessment. The process for approval of changes to the CPS is followed.

1.5.5 Definitions and Abbreviations

Term	Description
Advanced Signature Format	Signature format created by the signing service, which includes the signing certificate.
Certificate	Signed assertion binding subject attributes to a public key.
CRL	Certificate Revocation List is a list of certificate serial numbers for revoked certificate.
Signing service	The signing service provided by Den Danske Stat offering subject's to create qualified signatures.
Login service	NemLog-in Login broker acting as Registration Authority for subject's that gets certificates issued through the signing service. It leverages on MitID.
OCSP	Online Certificate Status Protocol providing revocation status for requested certificates.
PKI System	The technical infrastructure used by Den Danske Stat to offer qualified services.
QSCD	Qualified Signature Creation Device meeting the requirements in [eIDAS].
Short-term certificate	Certificate issued as part of a signing session. It has short validity with 10 days.
Signing session	Covers the session starting when a subject initiates a session through the signature client to the backend services and ends with an advanced signature is generated. The session includes subject authentication, key pair generation, certificate issuance, signature generation, formatting of the advanced signature object with certificates, time stamp tokens and OCSP responses and disposal of the signature key.

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.
Practices are periodically and at least once a year audited by internal and external audit to be conformant with this CPS.
Den Danske Stat acts according to the CPS under supervision and conformity assessment.

[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.
The CPS is published on https://ca1.gov.dk 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 subscriber's obligations,**
- **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. that the CA acts as qualified trust service provider, cf. eIDAS,**
- **k. the CA's contact information, and**
- **l. any undertaking regarding availability.**

Den Danske Stat's Terms and Conditions [T&C] includes content mandated by requirements in the applicable certificate policies. The Terms and Conditions [T&C] is approved by Den Danske Stat management and published on https://ca1.gov.dk.
The Terms and Conditions [T&C] is published on https://ca1.gov.dk when a new version is released.

[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**
- **n. until the certificate has been accepted by the subject, except for use that forms part of the certificate application process or**
- **o. after the subject 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,**
- **p. indication of the period of time for which the records are retained,**
- **q. the subscribers' obligations, cf. clause 4.5.1.**
- **r. information for relying parties, cf. clause 4.5.2 and**
- **s. information about the validity period of a qualified person certificate.**

See REQ 2.1-03.

[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 at the time of the private key usage - 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.**

Via the PDS [PDS] Den Danske Stat communicates that any third party shall verify the validity of the certificate either via CRL or OCSP. The PDS is published on https://ca1.gov.dk and links to both CRL and OCSP responders can be found in issued certificates encoded in standard extensions for the purpose as described in [CERTPROF].

[REQ 2.1-06] Terms and conditions shall be made available through a durable means of communication.
Terms and Conditions [T&C] is in Login Service and https://ca1.gov.dk.
For Login Service the Terms and Conditions [T&C] is shown to the subject before a certificate is issued.

[REQ 2.1-07] Terms shall be formulated in a readily understandable language and shall be available on a 24x7 basis. 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.
The Terms and Conditions [T&C] written in Danish in a readily understandable language. See 2.1-06 for availability.

[REQ 2.1-08] Terms and conditions may be transmitted electronically.
See REQ 2.1-06.

2.2 Publication of certification information

[REQ 2.2-01] The CA shall make issued certificates available to 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.
Certificates issued through the signing service can only be used by the signing service for the intended purpose of signing documents and as such they are not published. The certificate is made available through the signed document within the advanced signature object for which the certificate was created and hence available to any relying party validating a signed document based on the subject's certificate.

[REQ 2.2-02] After issuance, the complete and accurate certificate shall be available to the subject to whom the certificate is being issued.
Qualified certificates [Qualified Person] issued during a signing session are made available for the subject as part of the advanced signature format [AdES].

[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.**

The information on the web site, https://ca1.gov.dk/ including Certificate Revocations Lists are provided by the PKI System without access control. On the web site https://ca1.gov.dk/ obligations for certificate owner and certificate subscriber are published.

[REQ 2.2-04] CRL information shall be provided without any kind of access control.
See REQ 2.2-03.

[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.

Terms for subscriber and relying party are described in [PDS].

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.
The CPS including updates of the CPS are published immediately after approval and before it is taken into effect.

2.4 Access control 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.
The CPS and the Terms and Conditions [T&C] is available to anyone internationally without restrictions.

3 Identification and authentication

3.1 Naming

3.1.1 Type of names

[REQ 3.1.1-02] The subject shall be identified by a registered name or a pseudonym. However, deviations are allowed, cf. clause 3.1.2. It must be recorded whether a name or pseudonym has been used.
The Subject DN commonName attribute will contain a name of the subject. If Pseudonym is chosen, the value will be set to 'pseudonym'.

3.1.2 Need for names to be meaningful

[REQ 3.1.2-01] The name of the subject shall be verified via an authoritative source.

Note: An authoritative source may be the Civil Registration system, eIDAS nodes (cf. Article 12 of eIDAS) or a valid passport.
The assessment of the identity verification carried out by MitID as mentioned in 1.3.2 Registration authorities covers that the subject name has been verified via an authoritative source.

[REQ 3.1.2-02] If the subject is registered with a name, such name shall as a minimum consist of a registered first name and last name. Any middle names may be omitted, and the name must not include words not forming part of a subject's name such as pet names.
The Subject DN commonName, surname and givenName attributes will contain the name of the subject as defined by the registered name in CPR. Nicknames, and names with spelling other than registered in CPR is not supported.

[REQ 3.1.2-03] If the subject is registered with a pseudonym, such pseudonym may not be of a nature that may cause obvious misunderstandings and must not be identical or confusingly similar to a trademark. Moreover, the CA may reject the use of pseudonym.
The PKI System supports where applicable according to relevant CP, that the Subject of a certificate may choose a pseudonym when issuing the certificate to avoid the real Subject name to be shown in the certificate. The only allowed pseudonym is "pseudonym".

3.1.3 Anonymity or pseudonymise of subscribers

[REQ 3.1.3-01] The subscriber shall be able to select that the name of the subject does not appear from issued certificates.
See REQ 3.1.2-03.

3.1.4 Rules for interpreting various name forms

N/A. The CP does not pose any policy requirement.

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.
The PKI system ensures uniqueness of names by using serialNumber as part of subject distinguishedName. The subject DN serialNumber will consist of a Unique identifier for the certificate subject in the form UI:DK-XXXXXXX..XX.

3.1.6 Recognition, authentication, and role of trademarks

N/A. The CP does not pose any policy requirement.

3.2 Initial identity validation

[REQ 3.2-01] The CA shall verify the identity of the subject and check that the certificate applications are accurate, authorized and complete according to the collected evidence or attestation of identity.
During a signing session, the Signing Client will redirect to the session to the Login Service. The subscriber submits credentials and upon successful authentication, the Login Service returns a SAML response

containing the authentication information including the subscriber's naming attributes, which will be used to for a certificate signing request.

[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.
See 1.3.2 Registration authorities.

[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.
See 1.3.2 Registration authorities. The CA uses the following information from the identity providers: UUID-CPR and CPR-number are logged.

[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.
The attributes received from the Login Service includes

- LoA
- CertificatePolicyQualifier which is the Class of policy to use for the signing certificate. The value must be either "Person", "Employee", or "Organization". In this case the returned value must be "Person".
- HolderIdentifier in the CPR-UUID format
- Firstname of the End-user
- Lastname of the End-user
- Age of the End-user
- AnonymizedSigner defines whether or not Pseudonym is to be used
- ReferenceText from the Service Provider and verified by the Service Provider. This helps the end-user recognize what's being signed

[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.
N/A. The CA is not a natural person and this CPS is only related to qualified certificates for natural persons.

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 subject is in possession of a private key belonging to the subject's public key which must form part of the certificate.
Short term certificates are issued through the signing service, which relies on an identity assertion provided by an identity provider (see 1.3.2 Registration authorities) assessed to [eIDAS] Level of Assurance at least substantial.
Following a successful authentication and once the signing service has received subject naming attributes from the Login Service, a key pair is generated and assigned on a QSCD. The public key is used in the certificate signing request.

[REQ 3.2.1-02] The CA shall document the method for proof of possession of private key in the CPS. The solution supports certificate signing request provided as PKCS#10 CertificationRequest, where the private key is used to sign the request. Upon receival of the CertificationRequest, the public key is extracted, and the signature is verified as Proof-of-Possession of the private key.

3.2.2 Authentication of organization identity

N/A. The CP does not pose any policy requirement.

3.2.3 Authentication of individual identity

[REQ 3.2.3-01] The subject's physical identity and the attributes of such identity shall be verified in accordance with the provisions of eIDAS either

- **by the personal attendance of the natural person or**
- **by applying methods that provide a similar degree of security as physical attendance and where the CA can prove that the methods offer a similar degree of security.**

In order to issue qualified certificates to be used by the signing service Den Danske Stat applies b) using a remote identification method which meets the requirement of [eIDAS] article 24.1 litra d.
The Login Service uses eID schemes which has been conformity assessed to meet these requirements.

[REQ 3.2.3-03] Documentation for the subject's identity shall include

a. **Full name**
b. **Date and place of birth, reference to a nationally recognized identity document or other attributes that can be used to distinguish the person from others with the same name as far as possible, e.g. the attribute civil registration number (CPR)**

Qualified person certificates are issued on the basis of authentication with a MitID on an [eiDAS] level of assurance at least substantial. The subject naming attributes retrieved from authentication contain full name and CPR/UUID-CPR.

[REQ 3.2.3-04] Where place of birth is used, cf. the above requirement, place of birth shall be stated in accordance with national or other applicable conventions for registering births.
N/A. Birthplace is not used.

3.2.4 Non-verified subscriber information

[REQ 3.2.4-01] The subscriber shall provide a physical address, or other attributes, which describe how the subscriber shall be contacted.
The Subscriber is identified as a natural person. All subscribers are contacted using the Danish National Digital Mail system (Digital Post)[1].

3.2.5 Validation of authority

N/A. The CP does not pose any policy requirement.

3.2.6 Criteria for interoperation

N/A. The CP does not pose any policy requirement.

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.
The solution does not support certificates to be re-keyed.

[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 subject.
The solution does not support certificates to be re-keyed.

[REQ 3.3-03] Requirement for identity validation, cf. clause 3.2 shall be complied with.
The solution does not support certificates to be re-keyed.

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.
The solution does not support certificates to be re-keyed.

[1] All residents in Denmark are obliged by law to have a Digital Mailbox

3.3.2 Identification and authentication 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.
The solution does not support certificates to be re-keyed.

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.
Certificates issued through the signing service can be revoked using the schemes described in [Revocation Procedures].

[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).**

See [Revocation Procedures] on revocation procedures.
The PKI System revocation API supports the following revocation reason codes:

- UNSPECIFIED
- KEYCOMPROMISE
- AFFILIATIONCHANGED
- SUPERSEDED
- PRIVILEGEWITHDRAWN

The PKI System immediately without any delay revokes certificates upon receival of revocation requests. The certificate revocation status is reflected through OCSP while it may take up to one minute before all CRL nodes are updated.

4 Certificate life-cycle operational requirements

4.1 Certification Application

4.1.1 Who can submit a certification application

[REQ 4.1.1-01] The subscriber may request a certificate for itself.
During a signing session: Certificates issued through the signing service; it is the authenticated identity who will have a certificate issued.

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.
The Login Service using eID schemes conformant to [eIDAS] and acts as RA.

[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.
The subject naming attributes received by the signing service from the Login Service are protected in confidentiality, integrity and origin 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.
During the signing session, the Subscriber is required to accept Terms and Conditions [T&C] before subject name attributes are delivered to signing 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 presented for certification and that the private key is protected by a QSCD.
Keys issued through the signing service are generated, protected and used by a QSCD. See [Signing Service] for details.

4.2 Certification 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 at NSIS assurance level 'substantial' or 'high' or eIDAS assurance level 'substantial' or 'high'.
The subject's association with the subscriber will be secured at [eIDAS] level of assurance on at least substantial. This is ensured by the mandatory authentication process with the Login Service, which requires an authentication at level of assurance at least Substantial or higher. A user will perform authentication with an eID scheme. If a user provides insufficient credentials, the Login Service will not release naming attributes to signing service.

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 subject access to information about status for certificate applications. The CA shall explain the reasons for the rejection of a certificate application to the subject.
The CA will accept all certificate applications issued through the signing service.

4.2.3 Time to process for certificate applications

The [REQ 4.2.3-01] The CA should process certificate applications without undue delay.
The response time for handling certificate applications is delivered by service targets monitored by the Den Danske Stat and it can be expected that 99% are handled within 2 seconds.

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.

The signing service uses origin authenticated subscriber naming attributes received from the Login Service. Upon receival of these attributes, the signing service request the QSCD to generate a key pair and assign this to the subscriber. The QSCD uses the private key to sign a certification signing request.
The signing service uses the certificate signing request to request the CA Service to issue a certificate for of the type as indicated in the attributes. Once the CA has issued the certificate, it is returned to the signing service and associated with the key pair in the QSCD. At this point the key pair may be used for a signature operation.

[REQ 4.3.1-02] The CA shall take measures against forgery of certificates.
Certificates are protected in integrity using a signature created by the issuing CA in the PKI System. Any modification of the certificate is detectable, and the certificate will appear as modified.

[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.
The signing service uses a Signature Activate Module conformant to [CEN EN 419 241-2], which requires for the physical security and cryptographic operations a cryptographic module conformant to [CEN EN 491 221-5] to generate, protect and use subjects' key pair.

[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.
The signing service uses the information provided by the Login service to assign a key pair including the certificate to the subscriber.

[REQ 4.3.1-05] The CA must not issue certificates whose lifetime exceeds that of the CA's signing certificate.
The PKI System implements the constraint that certificates can't have a validity exceeding the validity of the issuing CA certificate in the PKI System. Thereby there will be no valid certificates when the issuing CA's signing certificate expires.

[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.
See REQ 4.3.1-01.

[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, and the cryptographic device protecting the subject's key shall be securely delivered.
The signing service is operated by the CA.

[REQ 4.3.1-08] Over the lifetime of the CA, a subject distinguished name which has been used in a certificate shall never be re-assigned to another subject.
The name comprises the entire identification of Subject DN in the certificate, including a unique identifier for the certificate subject in the form of the subject serialNumber. The combined information makes the name of the Subject unique and unrepeatable.

[REQ 4.3.1-10] The CP identifier in the certificate shall be as specified in QCP-n-qscd (certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD), cf. clause 7.1.6.
The CP is identified in the certificates with QCP-n-qscd, QCP-l-qscd or NCP according to the applicable CP's.

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.
There is no explicit notification of subjects and/or subscribers when a certificate has been issued.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

[REQ 4.4.1-01] The terms and conditions shall indicate what is deemed to constitute acceptance of the certificate.
Den Danske Stat's Terms and Conditions [T&C] states what is considered to constitute acceptance of the certificate.

[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.
Acceptance of Den Danske Stat's Terms and Conditions [T&C] in the Login Service is an integrated part of the signing session.

[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.
The Terms and Conditions [T&C] is presented to the subject by the Login Service during the signing session. The subject must accept them for the session to continue.
All versions of the Terms and Conditions [T&C] is made available on https://ca1.gov.dk.

[REQ 4.4.1-05] The terms and conditions may be transmitted electronically.
See REQ 4.4.1-04.

[REQ 4.4.1-06] The terms and conditions may use the model specified in ETSI EN 319 411-1 Annex A.
Den Danske Stat does not use the model of terms and conditions described in ETSI EN 319 411-1 Annex A since the Terms and Conditions [T&C] is an integrated part of a larger agreement complex.

[REQ 4.4.1-07] The CA shall record the agreement with the subscriber. If the subscriber and subject are two separate natural persons or legal entities, the agreement with the subject shall also be recorded.
The Login Service records which version of the Terms and Conditions [T&C], the subject has accepted.

[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.
The acceptance of the Terms and Conditions [T&C], within the Login Service require the subject the tick a check box.

[REQ 4.4.1-09] If the subscriber and subject are two separate natural persons or legal entities, the agreement shall be in two parts and the first part of the agreement shall be ratified by the subscriber and include:

a. **the subscriber's obligations**
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 at-tributes 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 terminates its services.**
c. **whether, and under what conditions, the subscriber may require and the subject shall approve the publication of the certificate**
d. **confirmation that the information to be held in the certificate is correct**
e. **obligations applicable to subjects**
f. **obligations to request the CA revoke certificates issued to subjects when they are no longer associated with the subscriber.**

Den Danske Stat have included the contractual requirements in relevant certificate policies in the Terms and Conditions [T&C]. Terms and conditions must be accepted by subscriber prior to the insurance of certificates. For qualified person [Qualified Person] certificate Subscriber and Subject is always one and the same.

[REQ 4.4.1-12] The agreement may be in electronic form. If the agreement is in electronic form, it should be signed using an advanced electronic signature or an advanced electronic seal, cf. eIDAS.

For certificates issued through the signing service, the Terms and Conditions [T&C] is in electronic form and presented online to the subject by the Login Service prior to issuance and can be downloaded from https://ca1.gov.dk as PDF. All connections are secured TLS connection.

[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).
The Login Service retains in the log the registration of End-user acceptances to the Terms and Conditions [T&C] according to the time period specified in the agreement.

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).
Certificates issued through the signing service are not published.

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).
N/A. There is no notification to other participants of certificates issued through the Signing Service.

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 j) 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 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 a subject generates the subject's keys and the private key pair, and the private key can be used to generate digital signatures, the subject shall have sole control of the private key.**
- **f. The subject's private key(s) may only be used for cryptographic functions within the secure cryptographic devices (QSCD).**
- **g. The subject's private key(s) shall be generated in the subject's cryptographic device (QSCD) if the subject's key(s) is/are generated under the control of the subscriber or subject.**
- **h. 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.**

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

The [T&C] complies with this requirement.

[REQ 4.5.1-03] If the subject's keys are managed in a QSCD by a TSP or by the CA, the private key must not be used for signing except within a QSCD.
See REQ 4.3.1-03.

[REQ 4.5.1-04] If the subject's keys are managed in a QSCD by a TSP or by the CA, the subject's private key shall be used under the subject's sole control.
See REQ 4.3.1-01 for key and certificate generation. The information received by the Login Service following a successful authentication, is used to create and certify a key pair assigned to subject. Once the certificate has been created and associated with the private key in the QSCD, Signature Activation Data is generated, which may be used for to activate the private key to generate a signature on the document as presented for the user during the signing session. The Signature Activation Data can-not be used for other keys or to sign other documents.

[REQ 4.5.1-05] If the subject's keys are managed in a QSCD by a TSP or by the CA, the subject's keys shall be used only to generate qualified electronic signatures.
The signing service can only be used to generate qualified electronic signatures.

[REQ 4.5.1-06] If the subject's keys are managed by a TSP which is not the CA, the CA shall ensure by agreement that the TSP complies with the requirements REQ 4.5.1-03 – REQ 4.5.1-06.
N/A. Den Danske Stat is both CA and manage the subject's keys.

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.**

Den Danske Stat have published recommendations for relying parties in the PDS [PDS].

4.6 Certificate renewal

4.6.1 Circumstances for certification renewal

N/A. The CP does not pose any policy requirements.

4.6.2 Who may request renewal

[REQ 4.6.2-01] The subscriber may apply for a certificate renewal for itself.
N/A. The signing service does not support certificate renewal.

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.
See REQ 4.6.2-01.

[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.
See REQ 4.6.2-01.

[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.
See REQ 4.6.2-01.

[REQ 4.6.3-04] Requirements corresponding to the first issuance for identification and authentication shall apply, cf. clause 3.3.
See REQ 4.6.2-01.

[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.
See REQ 4.6.2-01.

4.6.4 Notification of new certificate issuance to subscriber

[REQ 4.6.4-01] The CA's notification of certificate renewal to the subject shall follow the rules for notification of the first certificate, cf. clause 4.3.2.
See REQ 4.6.2-01.

4.6.5 Conduct constituting acceptance of a renewal 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.
See REQ 4.6.2-01.

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.
See REQ 4.6.2-01.

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.
See REQ 4.6.2-01.

4.7 Certificate re-key

4.7.1 Circumstance certificate re-key

[REQ 4.7.1-01] A certificate issued under this CP may be re-keyed for up to four years at a time.
N/A. The signing service does not support re-key of certificates.

[REQ 4.7.1-02] The CA or subscriber can specify whether a certificate can be rekeyed.
See REQ 4.7.1-01.

[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.
See REQ 4.7.1-01.

[REQ 4.7.1-04] For re-keyable certificates, the CA may notify the subject well in advance of the expiry.
See REQ 4.7.1-01.

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.
See REQ 4.7.1-01.

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'.
See REQ 4.7.1-01.

[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.
See REQ 4.7.1-01.

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 subject shall follow the rules for notification of the first certificate, cf. clause 4.3.2.
See REQ 4.7.1-01.

4.7.5 Conduct constituting acceptance of a re-keyed 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.
See REQ 4.7.1-01.

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.
See REQ 4.7.1-01.

4.7.7 Notification of certificate issuance by the CA to other entities

[REQ 4.7.7-01] The CA's notification of re-keyed certificate to other entities shall follow the rules for notification of the first certificate, cf. clause 4.3.3.
See REQ 4.7.1-01.

4.8 Certificate modification

4.8.1 Circumstances 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.
N/A. The signing service does not support certificate modification.

4.8.2 Who may request certificate modification

[REQ 4.8.2-01] The subscriber may request a certificate modification.
See REQ 4.8.1-01.

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.
See REQ 4.8.1-01.

4.8.4 Notification of new certificate issuance to subscriber

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

See REQ 4.8.1-01.

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.
See REQ 4.8.1-01.

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.
See REQ 4.8.1-01.

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.
See REQ 4.8.1-01.

4.9 Certificate revocation and suspension

4.9.1 Circumstances 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. **An inaccuracy has been found in the certificate content or other information associated with the subject, however cf. below for matters concerning the subject's change of name.**
f. **Subject has died.**

Den Danske Stat has implemented procedures, [Revocation Procedures], for timely handling of revocation requests from authenticated sources. This includes revocation request addressed to the support.

[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 30 days. If the certificate is not renewed, the CA shall revoke the certificate.
N/A. Certificates issued through the signing service has a validity of 10 days.

[REQ 4.9.1-03] Failure by the CA to comply with this CP does not entitle the CA to revoke a certificate.
Den Danske Stat does not revoke subject's certificates in case of non-compliance issued with applicable CPs.

[REQ 4.9.1-04] Once a certificate is definitively revoked it shall not be reinstated.
A certificate can't be reactivated after it has been revoked. Note that the PKI System does not support suspended certificates.

4.9.2 Who can request revocation

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

- **Subject,**
- **the CA if the rules of this CP have not been complied with or if other circumstances so warrant,**
- **an estate trustee appointed by the Probate Court or an heir to the subject, if the subject has died and**
- **a guardian with proper documentation.**

Den Danske Stat uses the procedures described in [Revocation Procedures] for certificate revocation.

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.
Den Danske Stat uses the procedures described in [Revocation Procedures] for certificate revocation.

[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**

Den Danske Stat uses the procedures described in [Revocation Procedures] for certificate revocation.

[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.
Den Danske Stat uses the procedures described in [Revocation Procedures] for certificate revocation.

[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 via the communication channel agreed between the CA and subscriber.
N/A. Den Danske Stat does not revoke certificates issued through the Signing Service. While certificates have a validity of 10 days, the private key is destroyed immediately after the signing session. Note that keys generated during a signing session, can only be used to sign the document for which the session was created.

[REQ 4.9.3-05] If revocation occurs based on the request from the Probate Court of estate trustee, the CA must send a receipt for the revocation to the Probate Court and estate administrator, respectively.
Den Danske Stat uses the procedures described in [Revocation Procedures] for certificate revocation.

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.
Den Danske Stat's Terms and Conditions [T&C] requires subscribers to request revocation of valid certificates in case of an event described in section 4.9.1 occurs.

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.
Den Danske Stat uses the procedures described in [Revocation Procedures] for certificate revocation. These procedures require staff to manage revocation inquiries without hesitation after they are received.

[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 requesters identity and authorization.
See REQ 4.9.5-01. Certificates issued through the signing service can only be revoked by the end-entity through GUI which requires authenticated log-in. Revocation is processed immediately after the users consent to do so. A confirmation of revocation will be presented to the End-user.

[REQ 4.9.5-03] If the revocation request requires revocation at a planned future point in time, then the scheduled date may be considered as the confirmation point in time for the CA.
Den Danske Stat does not support Subscriber planned revocation.

[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.
Den Danske Stat does not support faster revocation 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
The local clock of the servers is synchronized with a reliable time source using an NTP service provided by the operating system. NTP manages all time information based on UTC.

4.9.6 Revocation checking requirement for relying parties

N/A. The CP does not pose any policy requirement.

4.9.7 CRL issuing 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.
The CRL profile as specified in [CERTPROF], section 14, indicates that CRL's are issued within the frequency limits required in the applicable CP's i.e. 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"
The CRL profile as specified in [CERTPROF], section 14, is compliant with [RFC5280]. Den Danske Stat has implemented procures to ensure that CRL are automatically generated at least every 24th hour.

[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.
The CRL profile as specified in [CERTPROF], section 14, indicates that 'nextUpdate' for CRLs providing revocation status for intermediate CAs, that the CRL is created at least every 3 months. There is no CRL for root CA certificates. The overlap between CRLs is 15 to 20 days.
For CRLs issued by the intermediate CAs providing status for subject certificates, a new CRL is available at least every 24 hours. The overlap between CRLs is 12 hours.
Delta CRL is not part of the implementation.

[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.
By revoking a Root CA or intermediate CA the PKI System will revoke all certificates issued by the CA and create a new CRL.

[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.
See REQ 4.9.7-03.

[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.
N/A. Den Danske Stat does not issue any cross-certificates.

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 for root CA must be published no later than 10 minutes after revocation.
Revocation and maximum latency for CRLS's are supported as defined in the CP's. Revoking a certificate will result in the issuing a new CRL containing the revoked certificate for the affected CA. For efficiency reasons, all revocations, pertaining to a specific issuing CA, are batched together for a 10 second interval, whereupon a new CRL is issued for that CA.

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.
Certificate revocation status information is available through OCSP. The url can be found in the non-critical certificate extension, authorityInformationAccess, as specified in [CERTPROF].

4.9.10 On-line revocation checking requirements

N/A. The CPs does not pose any policy requirements.

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.
Certificate revocation lists containing certificate status information are provided at https://ca1.gov.dk. In addition, they can be found as stated in the non-critical certificate extension, cRLDistributionPoints.

4.9.12 Special requirements re-key compromise

N/A. The CP does not pose any policy requirement.

4.9.13 Circumstances for suspension

[REQ 4.9.13-01] A certificate issued under this CP must not be suspended.
Den Danske Stat does not support suspension of certificates.

4.9.14 Who can request suspension

N/A. The CPs does not pose any policy requirements.

4.9.15 Procedures for suspension request

N/A. The CPs does not pose any policy requirements.

4.9.16 Limits on suspension period

N/A. The CPs does not pose any policy requirements.

4.10 Certificate status services

[REQ 4.10-01] The CA shall provide services for checking the status of the certificates.
Den Danske Stat provides access to certificate status information through CRL and OCSP as described in REQ 4.9.9-01 and REQ 4.9.11-01.

[REQ 4.10-02] The CA shall document precisely in its practice's statements and in its terms and conditions how requirements REQ 4.10.1-01 and REQ 4.10.1-05 are met, including

- **a. the period over which the revocation status information is made available;**
- **b. how the revocation status information is provided in the case of CA's key compromise; and**
- **c. how the revocation status information is provided in the case of the CA's termination.**

The CPS and Terms and Conditions [T&C] includes a description of how requirements REQ 4.10.1-01 and REQ 4.10.1-05 are met.

4.10.1 Operational characteristics

[REQ 4.10.1-01] Status information for certificates issued under this CP shall be available beyond the validity period of the certificate.
The CRL profile as specified in [CERTPROF], section 14, specifies that CRLs contains the extension ExpiredCertificatesOnCRL indicating that revoked certificates are kept on the CRL after the certificate has expired.
The PKI System ensures certificate information is maintained in the OCSP responder database after certificate validity and thereby ensures the OCSP responder can process expired certificates.

[REQ 4.10.1-02] The integrity and authenticity of the status information shall be protected.
The PKI System signs CRLs using the issuer CA of the certificates contained in the CRL thereby ensuring the integrity and authenticity of the CRL.
The OCSP responder certificate profiles as specified in [CERTPROF], section 6 and 12, describes the profiles of the OCSP issuer ensuring the integrity and authenticity of the OCSP responses.

[REQ 4.10.1-03] As a minimum, the CRL and OCSP shall be supported as certificate status checking methods.
See REQ 4.10-01.

[REQ 4.10.1-04] Revocation status information shall include information on the status of certificates at least until the certificate expires and the CA should not remove revoked certificates from CRLs after they have expired.

See REQ 4.10.1-01.

[REQ 4.10.1-05] The CA shall preserve the integrity and the availability of the last CRL at least for the period specified in the CPS.
The last CRL is preserved and available at least until the last issued certificate expires. The duration of various types of issued certificates are listed in the public available certificate profile document.

[REQ 4.10.1-06] The CA should not issue a last CRL until all certificates potentially in the scope of the CRL are either expired or revoked.
Den Danske Stat maintains termination plans which ensures that all certificates for a CA are revoked before the last CRL is issued.

[REQ 4.10.1-07] The CRL shall be signed digitally by the CA that has issued a revoked certificate.
See REQ 4.10.1-02.

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

- **LDAP**
- **HTTP**

CRLs are made available for download via both LDAP and 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.
See REQ 4.9.8-01 and REQ 4.9.9-01.

[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.
The OCSP responders configured in the PKI System does not make use of pre-generated OCSP responses.

[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.**

OCSP responder certificates issued by the PKI System are issued for the specific purpose of service OCSP responders.
The OCSP responder certificate profiles are specified in [CERTPROF]. In section 6 and 12 the profiles are specified with the following extensions:

- keyUsage: digital Signature
- extKeyUsage: OCSPSigning
- CRLDistributionPoint: Not included
- AIA: not included
- OCSPNoCheck: Contains OID 1.3.6.1.5.5.7.48.1.5

[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.
The lifetime of OCSP responder certificates for CAs that issue certificates to subjects are set to maximum of 72 hours.

[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.

The lifetime of OCSP responder certificates for the root CA are set to maximum of 3 months. See clause 6.2 for details on cryptographic devices.

[REQ 4.10.1-14] When a CA certificate is about to expire, the CA may compute a last OCSP answer which is used for all OCSP requests with the nextUpdate field set to "99991231235959Z".
Before a CA certificate expires, the OCSP responder providing status for certificates for the CA certificate is configured with a nextUpdate set to “99991231235959Z”.

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.
The PKI System provides certificate status on a 24/7/365 basis under a contractual Service Level Agreement ensuring availability with maximum 2 hours unavailability.

[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.
The PKI System provides certificate status on a 24/7/365 basis under a contractual Service Level Agreement ensuring response time conformant to the requirement.

[REQ 4.10.2-03] The certificate status information shall be publicly and internationally available. The certificate status service OCSP is internationally available. Validation Authority OCSP endpoint is publicly available at the URL: http://ca1.gov.dk/ocsp.

4.10.3 Optional features

N/A. The CPs does not pose any policy requirements.

4.11 End of subscription

N/A. The CPs does not pose any policy requirements.

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.
The CA services provided by the Den Danske Stat does not use key escrow or perform backup of keys in any way. Subject’s signing keys are deleted immediately as part of termination of the signing session.

4.12.2 Session key encapsulation and recovery policy and practices

N/A. The CPs does not pose any policy requirements.

5 Facility, management, and operational controls

[REQ 5-01] The CA shall ensure that it operates in a legal and trustworthy manner.
The Trust Service Provider, Den Danske Stat is operated by Agency for Digitalisation on behalf of the Danish State. The agency is under control by The Ministry of Finance Supervisory Authority, parliamentary control via The Auditor General. The sub supplier contracts are reviewed by the attorney general. The subcontractors are selected based on an evaluation of the skills within trust services.

[REQ 5-02] The CA shall carry out a risk assessment to identify, analyse and evaluate business and technical risks.
Den Danske Stat administration conducts a yearly risk assessment as part of the Agency for Digitisation ISO/IEC 27001 compliance program. Specific risk assessments are conducted on the trust services on a quarterly basis.
Risk identification, analysis and evaluation is established to include all common technical environments and business processes related hereto relevant to providing trust services and qualified trust services. All such procedures are compliant with ISO/IEC 27001.

[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.
See REQ 5-02.
Risk mitigations are evaluated as part of risk identification, analysis and evaluation that includes all common technical environments and business processes related hereto relevant to providing trust services and qualified trust services.

[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.
The CPS identifies all practises specific for the Den Danske Stat and required for implementing the CP requirements. The lower-level documentation used in the daily operation and reviewed by those doing a process review, are due to its internal nature considered private and proprietary and therefore beyond the scope of the present document.

[REQ 5-05] The risk assessment shall be reviewed and revised at least once a year.
See REQ 5-02.
Risk assessment is performed on regular basis and minimum every 6th month.

[REQ 5-06] The CA's management shall approve the risk assessment and accept the residual risk identified.
The trust service Management of Den Danske Stat approves and accepts residual risk from the assessment of the overall risk picture applicable to the services provided, including risks from other government agencies and subcontractors.
Management approves the risk assessment following the risk management process.

[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.
All information assets are maintained in a central CMDB including risk levels and classification. This includes all internal PKI System certificates and Configuration Items of the components.

[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.
The applicable and appropriate physical and logical access procedures to protect the common systems and facilities under the CP's and this CPS have been established. There are not any decentralized RA systems implemented.

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.
The applicable and appropriate physical access procedures to protect the common elements of the PKI System components have been established and are available in internal documents. This includes using high security zones with dual access control inside the protected zones of the data centres.

[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.**

Physical security is continuously managed to ensure that physical controls are defined, appropriate, applied and controlled to effectively protect equipment and services.

[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.
All data centres have suitable power supply and air-conditioning for the requirements of the equipment installed in them. The infrastructure is protected against power failures or any other electricity supply anomaly. Appropriate measures have been taken to prevent exposure of the equipment and cables to water. The data centres have the suitable means (detectors and automatic fire suppression systems) to protect their content against fire. Cabling is installed under a false floor or under the ceiling in cable baskets and the appropriate means (detectors in the floor and ceilings) have been installed to protect them against fire.

[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.
See REQ 5.1-03.
The data centres are furthermore protected with physical access control, and the high security zones are protected with dual access control.

[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.
Physical security of the PKI System is used to mitigate risk of environmental or human physical threats to an acceptable level supporting the overall security and contingency requirements, including preventing PKI System equipment, information, media and software relating to the 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.
The data centres are located in Denmark.

[REQ 5.1.1-02] The CA shall ensure that access to the CA facilities is limited to authorized individuals.
The data centres have access control security measures that permit only authorised personnel to access the buildings. Authorised personnel access rights are attested on a regular basis to ensure access is granted on a business need.

[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.

All critical operations are carried out in physically secure facilities, with specific levels of security for the most critical elements. The internal networks are separated in Production and non-Production environments for the PKI System. Network environments are sanitized and segmented to secure and protect communication.

[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.
CP requirements are applied to all locations of the PKI System environments.

5.1.2 Physical access

[REQ 5.1.2-01] The CA shall establish physical perimeter protection based on a tangible risk assessment.
The complete system to control physical access comprises various levels of security in a risk-based approach. All sensitive operations are carried out within a physically secure facility with high levels of security required for physical access to critical secrets in the PKI systems.

[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.
All sensitive components and physical operations are located within a physically secure facility with different levels of security required to access critical machinery and applications.

[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.
Physical barriers are established by using data centres secure facilities and high security rooms for housing the certificate issuing and certificate revocation 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.
All sensitive operations are carried out within physical barriers established by using data centres secure facilities and high security rooms for housing the certificate issuing and certificate revocation services.

[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.
Physical access is provided with “least privileges” principles and with additional restrictions on physical access to critical systems used for the provisioning of the trust services. Access to high security zones is managed by IDM system and logged by the access control systems.

[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.
Access to restricted areas is logged and audited and escorted access for non-authorized personnel is mandatory.

[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.
See REQ 5.1.2-06.

[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.
The services for certificate generation and revocation are placed in same dedicated security zone.

[REQ 5.1.2-09] The CA shall ensure that efficient guard duty 24 hours a day is established.
Physical access to Production locations, data centres and high security zones are monitored under continuous surveillance and video recording.

[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.
See REQ 5.1.2-09.

[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.
See REQ 5.1.2-06.

[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.
The PKI Systems Root CA private keys are held and used physically in dedicated security zone and only designated trusted personnel have access.

[REQ 5.1.2-13] Every entry and exit shall be logged.
Access to restricted areas is logged and audited and escorted access for non-authorized personnel is mandatory.

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 re-used storage objects. In this connection, registration data are also considered sensitive data.**

Media storage is classified and protected accordingly. This includes secure life-cycling when replaced or no longer in use.

[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.
See REQ 5.1.6-01. All Medias used by Den Danske Stat are all registered in either central CMDB or for MBK/Smart Cards and Security Tokens are registered as part of media management process - this includes time of usage and expected lifetime duration - for life recycling control.

5.1.7 Waste disposal

[REQ 5.1.7-01] Storage media containing sensitive data shall be securely disposed of according to its classification.
Information assets are securely disposed by use of a standardised and centralised procedure.

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.
The PKI Systems holding data in cold standby locations are subject to same security and protection level requirements as on-site information assets.

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.
Trusted roles included trusted at subcontractors are identified and approved by management. The following trusted roles are currently identified and approved:

- Organization Enrolment Staff
- Revocation Staff
- Security Officer
- Administrator
- System Operator
- Auditor

[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.
Trusted roles performing critical activities follows pre-defined and approved procedures such as, unboxing, key signing ceremonies etc.

[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.
All employees are covered by the Danish Public Administration Act §§ 3-6 regarding the impartiality of public employees. Employees and subcontractors are made aware of their obligations regarding impartiality via Code of conduct in the public sector. Persons in trusted roles must sign an impartiality clause stating that they are aware of the rules of impartiality and that they are not current in a situation that can question their impartiality.
Information about the impartiality rules and the impartiality clause are given to employees in trusted roles upon recruitment. Signed impartiality clauses are filed for documentation.
Trusted roles are approved by management and acknowledged by identified assigned personnel.

[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 trustworthy 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.**

Trusted roles include revocation officers performing critical activities follows pre-defined and approved procedures for revocation of certificates.
Trusted roles include officers, admins, operators and auditors performing critical activities following pre-defined and approved procedures such as, unboxing, key signing ceremonies etc.

[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.
Trusted roles segregate duties and are approved by management and acknowledged by identified assigned personnel.

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.
Dual control is implemented in the high security zone to ensure confidentiality and integrity of the PKI System that one person alone cannot sign subordinate certificates on his own during management of cryptographic modules.

5.2.3 Identification and authentication of 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.
Personnel appointed to trusted roles are approved by management and the Security Officer. The principle of "least privilege" applies.

[REQ 5.2.3-02] Trusted roles shall be approved by the management and accepted by the person to fulfil the role.
Assigned Trusted roles are approved by management and acknowledged by identified assigned personnel.

[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.
Job descriptions exists for all trusted roles and is taking segregation of duties and least privileges into account.

[REQ 5.2.3-04] Where appropriate, job descriptions shall differentiate between general functions and the CA's specific functions. These should include skills and experience requirements.
PKI System-specific functions are handled by Trusted Roles. Job descriptions exists for all trusted roles and includes requirements for skills and/or experience.

[REQ 5.2.3-05] Personnel shall not have access to the trusted functions until the necessary checks are completed.
Trusted roles are approved by management and acknowledged by identified assigned personnel.

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.
The personal conducting internal ISO 27001 audit is referring to the management of department in the Ministry of Finance whereas the personal administrating Den Danske Stat is referring to management within the Agency for Digitisation.
Internal audit or external audit are independent functions.

5.3 Personnel controls

[REQ 5.3-01] The CA shall ensure that employees and contractors support the trustworthiness of the CA's operations.
Procedures to ensure trustworthy operations of common system and functions relevant to the CP's are established and available in internal documents. This includes personnel security controls applied during engagement and when on-boarding and off-boarding.
This also applies to subcontractors.
Procedures to ensure trustworthy operations of common system and functions relevant to the CP's are established and available in internal documents. This includes personnel security controls applied during engagement and when on-boarding and off-boarding.

5.3.1 Qualification, 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.
The identity and trustworthiness of all personnel are verified, whether as an employee, agent, or an independent contractor, prior to the engagement of such person(s).
Personnel occupying a Trusted Role, as defined in 5.2.1, must possess suitable experience and be deemed qualified. Personnel in Trusted Roles shall undergo training prior to performing any duties as part of that role.

[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.
Den Danske Stat management and administration are all individuals with a basic knowledge of security procedures. The Agency has for more than 10 years been involved in the OCES CA (NemID) which has been operated under contract with the Agency. Furthermore, the Den Danske Stat staff is trained in specific topics related to the operation of a trust service provider.
The management team has been formed to consist of staff with different skills so they can complement each other.
Managerial personnel shall possess experience or receive training with respect to the trust service that is provided for which they have a managerial role. Familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment is required to carry out management functions.

[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.
Ministry of Finance has a common information security policy for the entire department and associated agencies. In connection with the information security policy a document setting out a policy for the security responsibilities of management of each agency is defined. Roles related to Den Danske Stat management is therefore not directly described in the in common information security policy.
Security roles and responsibilities are documented are available to all concerned personnel in internal documents.

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.
Newly employed personnel must exhibit a valid passport or similar recognised photo-id at the first day of work to ensure visual identification. The employee's closest superior validates the identity of new personnel.
Den Danske Stat and subcontractors verify the identity of all personnel prior to engagement.

[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.
Employees in trusted roles are security approved by the Danish intelligence service (PET) in accordance with the administrative regulation regarding public security approvals: CIR1H nr 10338 of 17/12/2014. Employees in trusted roles must be able to exhibit a clean criminal record upon recruitment and they must be able to maintain their security approval during their employment.
HR is notified by PET if an employee commits a crime during their employment. In this case HR will evaluate whether the security approval can be maintained.
Den Danske Stat and subcontractors ensures that personnel in Trusted Roles don't have a criminal record making them unfit to carry out their jobs. There are not RA personnel at the Den Danske Stat.

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.
Den Danske Stat administrative- and management staff has necessary internal training in topics covered by the services and regulation under which the services are operated including: eIDAS, PKI, timestamping and electronic signatures and seals.
Subcontractors must demonstrate that employees with sufficient expert knowledge have been hired.
Qualifications of Trusted Roles, as defined in 5.2.1, are evaluated as part of hiring procedure.

[REQ 5.3.3-02] RA employees must receive training that will enable them to perform their work correctly and securely.
Den Danske Stat issues certificates based on eID schemes without physical RA staff being involved.

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.
Employees are subjected to on-going security awareness based on the current threat landscape and security best-practices.

5.3.5 Job rotation frequency and sequence

N/A. The CP does not pose any policy requirement.

5.3.6 Sanctions for unauthorised 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.
Personnel are required to use and adhere to administrative and management procedure that are in line with the CAs information security management procedure.
Personnel are required to use and adhere to administrative and management procedures and processes.

[REQ 5.3.6-02] Appropriate disciplinary sanctions shall be used for personnel who violate the CA's policies or procedures.
Disciplinary sanctions are applied to employees that violates the Den Danske Stat's policies or procedures, as it may be appropriate under the circumstances. HR evaluates the violation and the disciplinary sanction in accordance with the Danish employment rules, including case law and The Salaried Employees Act. The disciplinary sanctions may include among others revocation of privileges, written warnings, dismissal, summary dismissal and/or criminal pursuit.
Sanctions are provided to personnel staff for policies or procedures violations, unauthorised actions, unauthorised use of authority and unauthorised use of systems for the purpose of imposing accountability on the personnel, as it may be appropriate under the circumstances. This may include among others revocation of privileges, administrative discipline and/or criminal pursuit.

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.
Den Danske Stat has ensured that staff at subcontractors performing tasks for Den Danske Stat possess the necessary expertise, reliability, experience, and qualifications via contract.

5.3.8 Documentation supplied to personnel

N/A. The CP does not pose any policy requirement.

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.
Audit logging of critical events is automated by systems and infrastructure. Audit log includes security logging, error and operational performance logging and user and access logging. Changes are documented and logged by use of change management procedures and supporting documentation and approval system.

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

Audit logging of critical events is automated by systems and infrastructure. Further, audit logging is manually supplemented where needed to ensure completeness of audit log. Audit log includes security logging, error and operational performance logging and user and access logging.

[REQ 5.4.1-03] All lifecycle events related to CA's private keys must be logged by the CA.
In addition to logging by systems all manual life cycle events of the PKI System are documented and logged, and when relevant under supervision of system auditors.

[REQ 5.4.1-04] All lifecycle events at the CA related to certificates must be logged by the CA, including that all relevant information on transmitted and received data must be stored and all events relate to registering, generating, conveying and possibly revocation of certificates must be logged. Finally, events in connection with the handling of a subject's cryptographic devices must be logged.
See REQ 5.4.1-03.

[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.
See REQ 5.4.1-03.

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

[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.
Access event logging is implemented for the purpose of maintaining a secure environment. This includes logging physical access of personnel and other persons to sensitive parts of any secure site or area.

[REQ 5.4.1-08] All lifecycle events at the CA related to QSCDs must be logged, including initiation and any possible personalisation.
See REQ 5.4.1-03.

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.
Audit logs are reviewed on a regular basis, annually as minimum.

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.
The retention policy for logs common to CP under this CPS is ten years, as the longest lifetime for issued certificates applicable to the CP's is three years.

[REQ 5.4.3-02] The CA must store all other audit logs for at least seven years.
The retention policy for audit logs common to CP under this CPS is minimum seven years as defined by the applicable CP's.

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).
Audit log is protected by standard security measures in the systems logging infrastructure to ensure the confidentiality and integrity of log data in transmission over network and in systems at rest.

[REQ 5.4.4-02] The CA must ensure protection of the privacy of subjects.
Audit log is protected by standard security measures in the systems logging infrastructure to ensure the security and privacy of log data in transmission over network and in systems at rest.

[REQ 5.4.4-03] The CA must store and manage log data with respect to applicable statutes also after termination of the CA service.
The log files are properly protected by an access control mechanism. Only authorised personnel can have access to audit logs.

[REQ 5.4.4-04] The CA must document in the CPS how log data can be accessed both before and after the termination of the CA service and the CA must document in the CPS the storage time, cf. clause 5.4.3 and precisely which log data is being transferred in connection with termination of the CA service.
Appropriate protection against modification and deletion of the audit logs is implemented such that no one can modify or delete audit records except for transfer to long term media for archiving purposes. Retention policy applies and log archives are available for transfer upon termination of PKI System CA unit.

5.4.5 Audit log back up procedures

[REQ 5.4.5-01] The CA must implement a procedure for regular security copying of audit logs.
Audit logs are included in the overall backup and recovery strategy.

5.4.6 Audit collection system (internal vs. external)

N/A. The CP does not pose any policy requirement.

5.4.7 Notification to event-causing subject

N/A. The CP does not pose any policy requirement.

5.4.8 Vulnerability assessment

N/A. The CP does not pose any policy requirement.

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.
For the established periods, all the information related to the operations carried out with certificates are stored and a change log securing the archival timestamp is kept. Changes to the PKI System software and hardware are recorded in internal ITSM, following best practice.

[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.
Via contracts with subcontractors Den Danske Stat ensures that logs and data is stored according to best practice which includes timestamps.
Subcontractor follows contractual requirements.

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.
Electronical records archived for issued certificates (tokens) are kept accessible for an appropriate period.

[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.**

The signing service receives a signed assertion from the Login Service providing attributes for the subject. The assertion is stored by the signing service and kept in the PKI System.
The Login Service uses [eIDAS] conformant identification schemes, which are used with a level of assurance of at least substantial.

[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).**

Certificate applications, i.e. signed certification requests, are logged. Renewal is not possible.
Signed agreements are stored in Den Danske Stat's contract management system.
All CPS approved versions are stored in Den Danske Stat's EDRMS.
Records include all relevant information concerning data issued and received by the Den Danske Stat for providing evidence in legal proceedings and for ensuring continuity of the service.

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

Video surveillance data are kept within the timeframe needed for the purpose and within the statutory limitations.

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.

The retention time for archived records from the PKI System are minimum seven years as defined by the applicable CPs.

[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.

See REQ 5.5.1-01.

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.

Stored data include log data and other relevant registered data including, but not limited to, OIOSAML Assertion is stored and kept in the PKI Systems data centres. Log data solution provides a data integrity control feature to guarantee and verify the integrity of data that is indexed.

[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.

Data are stored according to the practice stated in REQ 5.5.3-01 and in compliance with other related requirements in the CP.

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.

Backup copies, frequency and recovery tests are made in accordance with the standard measures established by Den Danske Stat for PKI System to protect against loss of data. Backup and recovery of the HSM environment is performed and tested under dual control by use of trusted roles according to this CPS. Recovery of backup is tested on a regular basis.

[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.

Via contracts with subcontractors Den Danske Stat ensures that logs and data is stored according to best practice which includes timestamps.
Backup and frequent recovery tests are made to ensure recovery of all significant information and software of the PKI System is possible.

[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.
Backup and recovery of the HSM environment is performed and tested under dual control by use of trusted roles. Backup copies are protected and kept in manner that ensures recovery within the defined recovery targets.

[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.
Recovery of backup is tested by the trusted roles on a regular basis, minimum 6 times annually.

[REQ 5.5.4-05] Functions for backing up and recovery must be performed by the relevant trusted roles, which are specified in clause 5.2.1.
See REQ 5.5.4-04.

[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.
A risk analysis has been conducted to identify critical operations where dual control must be ensured.

5.5.5 Requirements for time-stamping of records

N/A. The CP does not pose any policy requirement.

5.5.6 Archive collection system (internal or external)

N/A. The CP does not pose any policy requirement.

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.
Den Danske Stat will provide any data including relevant parts of audit logs if a legal basis exists e.g. warrant from a Danish court.

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.
The validity of PKI System root certificates is longer than the expected lifetime of the solution. Hence root certificates are not to be renewed. Intermediate CA will not be renewed but new intermediate CA will be established instead prior to an expiry of an intermediate CA certificate.

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.**

Security incidents are prioritized and classified based on their urgency and potential impact using the categories below:

- Low

- Medium
- High
- Critical

The applicable and appropriate incident and/or compromise reporting and handling procedures have been established.

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.
All relevant system events are monitored to generate forensic evidence and ensure timely response to and resolution of security incidents.

[REQ 5.7.1-02] The monitoring must take into account the sensitivity of the data that is being collected or analysed.
Log data are protected according to their classification.

[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.
All systems activity is logged into centralised log system, monitoring of these logs are done and upon abnormality alerting is triggered into incident mgmt. System - including security and Intrusion detection.

[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.**

Monitoring implemented to detect log functions being disabled - Monitoring / Auditing of usage of PKI System components.

[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.
The applicable and appropriate incident and/or compromise reporting and handling procedures have been established. This includes events where Den Danske Stat and/or data owner are required to act according to EU requirements.

[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.
Trusted roles resources are notified when potential security incident arises and are reported.

[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.
The procedures are described in internal security breach procedures. These procedures include notification of relevant parties including the Danish data protection authority and the Danish eIDAS supervisory body. See REQ 5.7.1-05.

[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.
Den Danske Stat ensures that a physical or legal person are informed according to internal security breach procedures in the likelihood that a security incident or loss of integrity could adversely affect the subject without undue delay via Den Danske Stat's general compliance with GDPR.

[REQ 5.7.1-09] 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.
System log is monitored in real-time to ensure that potential malicious events are identified and handled as incidents, including escalation of potential security incidents to the security function.

[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.
The applicable and appropriate incident and/or compromise reporting and handling procedures have been established. This includes events where Den Danske Stat is required to act according to CP requirements.

[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.**

See REQ 5.7.1-10.

[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.
See REQ 5.7.1-10.

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.
The subscriber is notified via a relevant channel according to internal security breach procedures.

[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.
CRL procedure will be prioritised in re-establishment after a Disaster Recovery is successfully completed.

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.
The Business Continuity Plan [BCP] includes a scenario with compromise of the Den Danske Stat's private key.

[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.
The Business Continuity Plan [BCP] includes a scenario with compromise of the Den Danske Stat private key.

[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.**

Den Danske Stat has established procedures for PKI System's private key compromise which includes the listed actions.

[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.
Den Danske Stat has established procedures for events where cryptographic algorithms or associated parameters have inadequate security which includes the listed actions.

[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.
If computing resources, software, and/or data are corrupted or suspected to be corrupted operations will be halted until the environment's security has been re-established, with the incorporation of new components, the suitability of which can be accredited.

[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.
Den Danske Stat has internal plans in the event that the private keys of many subjects are compromised.

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.
Den Danske Stat management has approved the Business Continuity Plan [BCP] which is activated in case of an operational disaster.
Contingency and recovery plans are planned and tested for the provided PKI System services and updated in advance of major changes affecting provided CA services.

[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.
Contingency plans are activated in case of disaster, including compromising of one of the PKI Systems' private signature keys.

[REQ 5.7.4-03] After a disaster, the CA must, where it is possible, implement mitigating precautions in order to avoid repetitions.
After a disaster the root cause will be analysed and evaluated to mitigate 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.
Den Danske Stat maintains an internal plan for termination of trust service activities.

[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.
In case the Den Danske Stat terminates trust service activities; subscribers will be notified via electronic mail at least 3 months prior to Den Danske Stat stops issuing (incl. renewal and rekeying) and 6 months prior to Den Danske Stat stops activities which affects already issued certificates e.g. certificate status services and revocation of existing certificates for the purpose of termination.
Other parties with a contractual relation with Den Danske Stat will be notified at least 6 months prior to a termination.
Den Danske Stat do not have or plan to have agreements or contracts with other parties to continue trust service activities in case of a termination.

[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.
Den Danske Stat's termination plans include:

- At least 6 months prior to termination of PKI System's activities the Supervisory Authority is informed.
- Subscribers and other parties with a contractual relation to Den Danske Stat will be informed as described above.
- At least 6 months prior termination of trust service activities relying parties are informed via https://ca1.gov.dk and a press release will be published.

[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.
Den Danske Stat's termination plans include procedures for disabling any issuance, rekey or renewals of certificates to subjects.
All issuances of certificates will be stopped if the PKI System ceases to function according to procedure.

[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.
In case of termination availability of CRL and revocation of certificates are ensured in compliance with contract.

[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.
Den Danske Stat's termination plans include appropriate data retention of data and logs.

[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.
Den Danske Stat's termination plans include requirements of planned termination of subcontractors acting on behalf of the Den Danske Stat.

[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.
Termination process will be engaged when PKI System is terminated to ensure that 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.
Due to the nature of the Den Danske Stat currently no other TSP is identified which can take over the delivery of Den Danske Stat's trust services.

[REQ 5.8-10] When another cross-certified CA stops all operations, including handling revocation, all cross-certificates to that CA shall be revoked.
N/A. The implemented PKI does not certify any certificate from other PKI.

[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.
N/A. Den Danske Stat is not a private organisation or a physical person.

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.
The PKI Systems [CERTPROF] root CA key pair are valid for 25 years, and the issuing CA key pair are valid for 10 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.
Certificate and key pairs for PKI System root CA component and issuing CA component are generated with a long lifetime using Key Signing Ceremony procedures and cryptographic hardware modules installed in their respective systems.

[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 if the recommendations are up to date.
Internal certificate and key pairs for PKI Systems root CA and intermediate CA certificates are generated with a long lifetime. These key pairs for internal certificates are generated in cryptographic hardware modules and follow the recommendations from ENISA, if these recommendations are updated.
The following key sizes, algorithms and validity have been chosen for the profiles [CERTPROF]:

- Root CA: RSA 4096 bits and 25 Years and self-signed using RSA PSS with SHA-512.
- Intermediate CA: RSA 3072 bits and 10 Years and signed using RSA PSS with SHA-512.

[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.
Internal certificate and key pairs for PKI System root CA component and issuing CA component are generated with a long lifetime. These key pairs for internal certificates are generated in cryptographic hardware modules installed in their respective systems.

[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.**

The hardware and software devices, as well as Trusted Roles and the physical security environment, follows official best practices and international ETSI standards as determined by the CP's. This includes, but is not limited to, the use of dual controls, high-security zones, logging, monitoring, security surveillance and managing changes such as transferring a private key in its encrypted module environment from one cryptographic module to another. Keys created by the TSP Signing component are created in conformance with ETSI TS 119 312.

[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.
Before an issuing CA is about to expire it will be renewed (key rollover) and a new issuing CA will be generated. This can all be done without interrupting the operations.

[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.
Any new PKI System CA certificates will be generated and distributed in accordance with this practise statement.

[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, 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.
N/A. The CA service is planned to cease operation before the expiry of the CA certificate, and last issued certificates are not allowed to exceed the expiry date 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).
The 'Key Signing Ceremony' KSC document describes the procedure for preparing:

- Root CAs and CRLs
- Intermediate CAs and CRLs
- OCSP Responders
- Time Stamp Authority
- Signing Service

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

- **roles that participate (both internal and external).**
- **Functions to be performed by every role and during which phases.**
- **Responsibilities during and after the ceremony.**
- **Requirements for documentation to be collected as evidence of the ceremony.**

The KSC meets the requirement in the CP.

[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.
See REQ 6.1.1-10.

[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.**

Key management report is signed by Security Officer and for Root CA also by independent trustworthy witness.

[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.

Managing subject's keys is carried out by the Signing Service, which uses a QSCD to manage the subject's key pair and certificate and use it for signing. The QSCD ensures that private keys are generated using recognised and approved algorithms and remains at all time protected in confidentiality.

[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.
Subject keys generated by the QSCD operated by Den Danske Stat are created in compliance with [FIPS 186-4], chapter 6.

[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.
Subject keys generated by the QSCD follows the recommendation in [ETSI TS 119 312], section 6.2.2.3. and uses Elliptic Curve Cryptography on the curve P-256.

[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.
The Signing Service generates subject's keys using a remote QSCD, which handles public/private keys and certificates used for signing. Once a key pair has been used by the QSCD for signing it is automatically deleted.

[REQ 6.1.1-17] Whether the CA controls of the cryptographic device for handling the subject's keys is initiated by CA or others, the CA shall verify that the device is certified as a QSCD, cf. eIDAS.
All qualified certificates issued by Den Danske Stat must resides and are protected by a QSCD. See [Signing Service] for details.
All QSCD's meets the requirement in [eIDAS] and their status as QSCD is published at [QSCD list].

[REQ 6.1.1-18] If the cryptographic device for handling the subject's keys is handled on behalf of the subject by a trusted service other than the CA, the CA shall verify that such other trusted service meets the appropriate requirements, cf. eIDAS, including in terms of qualification.
N/A. Den Danske Stat is the only trusted service which manage subject's keys on behalf of the subject.

[REQ 6.1.1-19] The certificate request process shall ensure that the subject's public key to be certified is from a key pair generated by a QSCD.
Qualified certificates for natural persons and the private/public keys pertaining to a certificate are created as part of the signature session by the Signing Service. The Certification Authority only accepts certificate requests which originates from the Signing Service.

[REQ 6.1.1-20] If the subject's key pair is generated by a qualified trusted trust service provider and imported into a QSCD used for signature, the environmental assumptions and security objectives for the given QSCD shall be met by the trust service provider.
N/A. The implemented solution does not allow for subject's key pair to be imported into the QSCD.

[REQ 6.1.1-21] If the subject's private key is moved between cryptographic devices, potential vulnerabilities to key compromise shall be determined and adequate mechanisms implemented to mitigate any vulnerabilities.
When a subject's private key is moved between QSCDs, it is protected in integrity and confidentiality using AES-GCM as scheme by a 256 bits AES key, that is only available by the QSCDs.

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.
N/A. The subject's key pair remains at all time at the TSP.

[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.
N/A. The subject's key pair remains at all time at the TSP.

[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.
N/A. The subject's key pair remains at all time at the TSP.

[REQ 6.1.2-04] If the CA generates the subject's keys, the CA shall secure the issuance of a cryptographic device to the subject.

In particular: (see REQ 6.1.2-05 and 6.1.2-06)
N/A. Den Danske Stat does not issue qualified certificates for natural persons with a cryptographic device physically distributed to the subject. The certificates remain protected by the QSCD operated by the CA.

[REQ 6.1.2-05] If the CA generates the subject's keys, cryptographic device preparation shall be done securely.
See 6.1.2-04.

[REQ 6.1.2-06] If the CA generates the subject's keys, the secure cryptographic device shall be securely stored and distributed.
See 6.1.2-04.

6.1.3 Public key delivery to certificate issuer

[REQ 6.1.3-01] If the subject delivers the subject's public key to the CA, they shall apply a mechanism to assure the integrity of the key
N/A. The solution does not support that the subject delivers the subject's public key to the CA.

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.
Den Danske Stat's public keys are published via EU Commission's trusted service list (TSL).

[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.
Verification of the Den Danske Stat's public keys can be conducted through via the TSL.

6.1.5 Key sizes

See clause 6.1.1

6.1.6 Public key parameters generation and quality checking

N/A. The CP does not pose any policy requirement.

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

[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].
[CERTPROF] specifies that subject certificates include the extension keyUsage and has profile A as described 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.
Den Danske Stat's root keys are generated, protected, and used by cryptographic modules which are certified following Common Criteria (ISO 15408) for assurance level EAL 4+ using the protection profile [CEN EN 419 221-5]. The modules are managed using operational procedures.

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 within a secure cryptographic device which is a trustworthy system which:

a) is assured to EAL 4 or higher in accordance with ISO 15408 or equivalent national or internationally recognized evaluation criteria for IT security provided this is a security target or protection profile which 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.

Den Danske Stat uses the following cryptographic modules which meets the requirement in the following standards:
For Root CA keys see REQ 6.2-01.
The Signing Service uses cryptographic modules which are certified after the same protection profile as the cryptographic modules used by the Root CAs. In addition, these cryptographic modules are loaded with a Signature Activation Module, which are certified following Common Criteria (ISO 15408) for assurance level EAL 4+ using the protection profile [CEN EN 419 241-2].
For all other services, the cryptographic modules are certified to meet the requirements in [FIPS 140-2] level 3.

[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.
Cryptographic modules certified according to [CEN EN 419 221-5] are operated according to the vendor guidance.
Cryptographic modules certified according to [FIPS 140-2] are operated in the same environment and under the same procedures as cryptographic modules certified according to [CEN EN 419 221-5]. They are deployed with an equivalent vendor supplied and recommended configuration, which uses internal software modules that are updated following the initial module certification.

[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.
Cryptographic modules are delivered as sealed devices not to be broken at any time.

[REQ 6.2.1-04] The CA shall ensure that cryptographic devices for certificate and status information signing have not been compromised during use.
Cryptographic modules are delivered as sealed devices not to be broken at any time, why all access to physical handling of the cryptographic modules is secured under dual control by minimum two Trusted Roles according to strict procedures, including unpacking and transportation after unpacking. When unpacked cryptographic modules are to be transported outside high-security zones the modules are additionally sealed off and transported under dual control.
Monitoring is set-up to monitor all activity on cryptographic modules for all cryptographic modules.

[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 each holding trusted roles in the CA.
Physical handling of the cryptographic modules is secured under dual control by minimum two Trusted Roles.

[REQ 6.2.1-06] The CA shall ensure that cryptographic devices for certificate and status information signing function correctly at all times.
Cryptographic modules are monitored for correct performance when online.

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

The root and intermediate CA private signing keys are held and used within cryptographic devices as specified above.

6.2.2 Private keys (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).
Backup of CA private keys are encrypted and kept under same high-security level as the keys in operation. The number of authorised persons having Trusted Roles with access to backup and recovery of CA private keys are limited to a minimum within the requirement of continuous 24/7 operations. At least two Trusted Roles are required for initial onset of Private key backup, routinely validation of backups or recovery from backup.

[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.
See REQ 6.2.4-01.

[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.
See REQ 6.2.4-01.

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.
As per design of the cryptographic modules the private key used for signing are, if moved from one cryptographic module to another, or when backed up, contained within an encrypted container controlled by the cryptographic modules in a secured setting provided by the module manufacturer. This is to ensure the same level of protection when outside the physical modules.

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.
See 6.2.5-01.

[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.
All manual operations of the Den Danske Stat's private keys are performed under dual control by Trusted Roles, including transport and backup/recovery.

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.
See 6.2.1 Cryptographic module standards and controls for implementation.

[REQ 6.2.7-02] The secure cryptographic device shall not be tampered with during shipment.
Visual inspection as part of the unboxing procedure ensures that cryptographic modules are not manipulated during delivery or storage.

[REQ 6.2.7-03] The secure cryptographic device shall not be tampered with while stored.
Visual inspection is part of internal compliance reviews and relevant operational procedures to ensure that the seal is not broken.

[REQ 6.2.7-04] The secure cryptographic device shall be functioning correctly.
See 6.2.1 Cryptographic module standards and controls for implementation.

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

Private keys associated with qualified certificates for natural persons, are generated, protected, and used by QSCDs operated as part of the Signing Service offered by Den Danske Stat. After the private key has been used for a signature operation, it is automatically destroyed. Similar, the Signing Service ensures the private key is deleted in case the signing session expires. By design the private key can only be activated for a signature operation after the subject has performed a successful authorisation by logging into the Login Service.

6.2.9 Method of deactivating private key

N/A. The CP does not pose any policy requirements.

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.
Procedures for secure disposal of Den Danske Stat's systems is established and performed under dual control if needed.

6.2.11 Cryptographic Module Rating

[REQ 6.2.11-01] The CA shall monitor the certification status of used QSCDs (including the subject's QSCDs) until the expiry of certificates on the QSCDs. The CA shall undertake suitable measures upon changing this status for a QSCD. Such measures shall be documented in CPS.
Den Danske Stat keeps a list of QSCD which holds private keys. The list includes the QSCD managed by Den Danske Stat.
In case Den Danske Stat becomes aware of a change of status of a QSCD, relevant parties are notified in writing via agreed communication channels.
Certification status of implemented cryptographic modules (QSCD) as stated in 6.2.1. using common criteria by the protection profiles [CEN EN 419 221-5] and [CEN EN 419 241-2] certification will be monitored.
If status is changed an analysis of consequence will be initiated and a plan for handling this will be prepared.

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 qualified certificates and/or issuing revocation status information shall not be used for any other purpose.**
- **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.**

Note: CA can issue internal operation-related certificates.

Other aspects of PKI Systems internal CA key pair management in HSM within the secure rooms are implemented in the following way:

- CA private keys are not usable for signing after end of life;
- Root CA and intermediate CA private keys are only used for issuing certificates and CRL's;
- Private keys are only used and operated in the physical high-security zones established according the CP requirements hereto;
- Private keys hash algorithm, signing algorithm and length are the same for each use;
- Private keys are destroyed (access removed) after end of life following a procedure; and
- Root-CA is self-signed with attributes following Recommendation ITU-T X.509.

[REQ 6.3-02] If the CA is managing the subject's private key, the CPS shall state whether the CA assures that the certificate is valid at the time of use of the private key.
Certificates and private keys used by the Signing Service are generated, used, and deleted by the QSCD during a signing session. The signature operation using the private key is carried out before the Signing Service retrieves OCSP status information for the subject certificate to form the Advanced signature format. Since the PKI System supports that it is possible to revoke all the subject's certificates using other interfaces, Den Danske Stat does not assure the certificate is valid at the time of use of the private key.
However in the unlikely event, if the Signing Service receives an OCSP response indicating the subject certificate is revoked, the Signing Service terminates the session and returns an error and a document signed with the subjects key will not be returned.

6.3.1 Public key archival

N/A. The CP does not pose any policy requirements.

6.3.2 Certificate operational periods and key pair usage periods

N/A. The CP does not pose any policy requirements.

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.
N/A. The CA does not issue cryptographic devices.

[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.
The Terms and Conditions [T&C] require subjects to protect credential data for the identity provider used by the Login Service against unauthorized use.
The subject's private key and certificate are generated, managed, and used in a QSCD. Activation of a private key for signature generation is under the subject's sole control and requires during the signing session, the subject to present credentials for the identity provider. It is only after a successful authentication, that the private key is generated and used. The subject's private key is therefore effectively protected against unauthorized use.

[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.

The Signing Service provides activation data based on the authentication with MitID which at level substantial or higher uses two factors.

[REQ 6.4.1-04] If the subject's private key is installed on devices to which only the subject has access but without effective protection against exhaustive search, 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. If password is used in environments that effectively prevents exhaustive searches, it may however be picked from a range of at least 9,800 possible codes.
N/A. Qualified certificates are only issued to the Signing Service, which manage private key on behalf of the subject.

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.
Den Danske Stat does not issue personalized cryptographic modules.

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.
The Key Signing Ceremony is performed under dual control using Den Danske Stat's cryptographic devices.

[REQ 6.4.3-02] The CA shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.
The cryptographic modules used by the Den Danske Stat are operated under dual control, and multifactor authentication is required for all Trusted Roles accessing the modules.

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.
Den Danske Stat's operating systems are hosted in an IT environment protected by best practise computer security controls ensuring that a proper use of system utility programs is in place and a proper separation of trusted roles, including the separation of security administration and operation functions, and practised.

[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.
Effective change control procedures are applied for releases, modifications, patches and emergency software fixes of any operational software and changes to the configuration (including firmware updates). All changes and change types have a documented audit trail with formal description of change, reason for change, risk assessment/impact assessment and fall-back plan.

[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.**

Den Danske Stat has covered this by relevant IT operation procedures.

[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.
All systems are protected by access control ensuring that only authorised actions are performed.

[REQ 6.5.1-05] The CA's systems shall enforce access control on attempts to modify revocation status information.
See REQ 6.5.1-04.

[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.
Den Danske Stat has monitoring capabilities, which monitors all logical access to all devices.

6.5.2 Computer security rating

N/A. The CP does not pose any policy requirements.

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.
See REQ 6.2.1-01 for the detailed specification of the cryptographic modules used by Den Danske Stat.

[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.
Den Danske Stat systems are external developed and certified under Common Criteria's in combination with in-house developed supporting systems approved by using S-SDLC methods ensuring security analysis as part of the process.

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.
Den Danske Stat and relevant subcontractors are managing information security according to ISO 27001.
Den Danske Stat and subcontractors are managed under applicable and appropriate procedures compliant with ISO 27001:2013 and externally audited annually.

[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.
This includes an information security policy covering the Ministry of Finance and all associated agencies under the ministry. The policy is approved by the management in the department.
Den Danske Stat and subcontractors has a management approved ISMS policy.

[REQ 6.6.2-03] Changes to the information security policy shall be communicated to third parties, where applicable. This may include subscribers, conformity assessment body, supervisory body and other authorities.
The information security policy accessible to all employees in Den Danske Stat.
When relevant, subcontractors and other third parties are informed of changes in the information security policy.

[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.
The information security policy including updates are documented and published internally.
The applicable and appropriate information security policies and procedures have been established.

[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.
The information security policy accessible to all employees in Den Danske Stat.
When relevant, subcontractors and other third parties are informed of content in the information security policy.

[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.
The Agency for Digitalisation reviews the information security policy on a yearly basis.
All inventory including relevant policies in the Ministry of Finance and subordinate agencies are maintained by The Agency for Governmental IT Services.
The Agency for Governmental IT Services reviews the information security policy on a yearly basis.
All ISMS documents are reviewed minimum once a year, and if changes occur that requires a revision.

[REQ 6.6.2-07] Any changes that may impact on the level of security provided shall be approved by the CA's management.
Den Danske Stat management approval of changes which may impact the security level is ensured via documented change management procedures.
Changes that can impact the security level are part of the risk assessment, which approved by 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.
The state and configuration of systems are regularly assessed for changes which could violate the security policies. The maximum interval between checks/assessments is one year.

[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.
See REQ 6.6.2-08.

[REQ 6.6.2-10] The maximum interval between two of the above checks shall be documented in CPS.
See REQ 6.62.-08.

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.
Access control is applied and managed for trusted roles access – with defined access management procedures for handling PKI System specific roles.

[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.
Access control is applied and managed according to best practises and requirements in the CP's.

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

[REQ 6.6.3-04] The CA's personnel shall be identified and authenticated before using critical systems and applications.
Access control is applied and managed according to best practises and requirements in the CP's.
Individual accounts are created for each PKI System component. All resources go through onboarding process with specific identity validation.

[REQ 6.6.3-05] The CA's personnel shall be accountable for their activities., e.g. through efficient event logging.
Access control is applied and managed according to best practises and requirements in the CP's. All access is logged and monitored for all trusted role operations.

[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.
Capacity reports are created, and capacity meetings are held every month. The reports are based on:

- monitoring of current usage,
- upcoming changes, and
- three months forecasts.

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.
Internal network and systems are protected from unauthorized access.

[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.
Networks are segmented and protected following a risk-based approach considering functional, logical, and physical (including location) relationship between trustworthy systems and services.

[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.
All systems are maintained and protected within secure zones and this includes protection of communications between systems across 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.
The PKI Systems used by Den Danske Stat are configured to ensure that unnecessary accounts, applications, services, protocols, ports, etc. are either removed or disabled.

[REQ 6.7-05] Local network components (e.g. routers) shall be kept in a physically and logically secure environment.
All secure room internal network components are stored inside High Security Zones with same security requirements as for all devices inside secure zone.

[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.
The secure room internal network component (e.g. routers, firewalls and switches) configurations are periodically checked for compliance with the specified requirements, minimum once a year.

[REQ 6.7-07] The CA shall apply the same security controls to all systems co-located in the same zone.
All systems are maintained within a zone are protected in same manner.

[REQ 6.7-08] The CA shall place particularly critical systems, including root-CA in high-security zones.
Critical systems including the root CA are placed in special secure rooms on a separate high-security network and a separate physical security zone.

[REQ 6.7-09] The CA shall grant access to secure zones and high security zones to only trusted roles.
Physical access policy is established to ensure security zones are limited to authorised personnel and the security practises here for.

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

[REQ 6.7-11] The CA shall not use systems used for administration of the security policy implementation for other purposes.
The internal administration network is separated from the application network, and systems administrating the security are not used for other purposes.

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

The production environments and systems are separated from development, testing and staging environments.

[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.
Firewalls are configured to prevent all protocols and accesses not required for the operation. This includes enforced encrypted traffic and protocols, zone restrictions, restrictions on network-to-network access, authentication and authorisation requirements and restriction of remote accesses.

[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.
Communication between distinct trustworthy systems is established only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

[REQ 6.7-15] The CA shall review the established network and firewall rules set on a regular basis.
Ruleset on network devices such as firewalls are reviewed 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.
Where a high level of availability of external access to the trust service is required, the external network connection is redundant to ensure availability of the services in case of a single failure.

[REQ 6.7-17] At least once every quarter the CA shall perform a vulnerability scan from 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.
Vulnerability scans are conducted and documented at least once every quarter by and external independent and competent external party.

[REQ 6.7-18] At least once a year, after set up and in case of significant infrastructure or application upgrades or modifications the CA shall perform a penetration test. 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.
Penetration tests are conducted and documented at least once a year, after setup and in case of significant infrastructure or application upgrades or modifications. The penetration test is conducted by and external independent and competent external party.

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.
PKI System is connected to a NTP device that receives the time from external time source via satellite.

[REQ 6.8-02] The precise time of significant environmental, key management and clock synchronization events shall be recorded.
All CA devices and Network devices are connected to NTP servers - that all gets it time from same Time source.

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.
The [CERTPROF] specifies certificate profiles issued by Den Danske Stat for Root CAs, Issuing CA, OCSP Responder, Time Stamp Units and subject certificates. The profiles are specified to meet requirements in [RFC5280] and [ETSI EN 319 412-2].

[REQ 7.1-02] The certificates shall be issued according to ETSI EN 319 412-2.
See REQ 7.1-01.

7.1.1 Version number(s)

[REQ 7.1.1-01] Certificate version number(s) shall be stated and provided as 'V3' (0x2).
[CERTPROF] throughout the document specifies the certificates to be 'V3'.

7.1.2 Certificate extensions

[REQ 7.1.2-01] All certificates issued under this CP shall contain all appropriate qcStatements as defined in ETSI EN 319 412-5 clause 5, including esi4-qcStatement-4.
[CERTPROF], section 9.5, specifies the content the non-critical extension qcStatements. It contains:

- The certificate is qualified: esi4-qcStatement-1
- The certificate is qualified according to [eIDAS]: esi4-qcStatement-6
- The certificate is issued to a natural person: QCType is set to: id-etsi-qct-esign
- The private key is managed by a QSCD: esi4-qcStatement-4
- From QPerson REQ 7.1.2-02
- From REQ 7.1.2-02 semanticsIdentifier: id-etsi-qcs-semanticsId-Natural and nameRegistrationAuthorities: https://uid.gov.dk

[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-Natural**
- **nameRegistrationAuthorities: https://uid.gov.dk (of the type URI generalName)**

See REQ 7.1.2-01.

[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.
[CERTPROF], section 9.5, specifies the content the non-critical extension authorityKeyIdentifier.

[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.
[CERTPROF], section 9.5, specifies the content the critical extension keyUsage to have the value as specified in Profile A of [ETSI EN 319 412-2] clause 4.3.2 to contentCommitment.

[REQ 7.1.2-05] If a certificate issued under this CP contains extension subjectAlternativeName, this extension shall be marked non-critical.
N/A. [CERTPROF], section 9.5, specifies the extensions for qualified certificates issued to natural persons. The extension subjectAlternativeName is not supported by the PKI System and excluded in the description.

[REQ 7.1.2-06] If a certificate issued after this CP contains extension issuerAlternativeName, this extension shall be marked as non-critical.
N/A. [CERTPROF], section 9.5, specifies the extensions for qualified certificates issued to natural persons. The extension issuerAlternativeName is not supported by the PKI System and excluded in the description.

[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.

[CERTPROF], section 9.5, specifies the content the non-critical extension cRLDistributionPoint containing the url http://ca1.gov.dk/qualified/issuing/N/crl/issuing.crl, where N is index for current active intermediate CA, staring from 1.

[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.
[CERTPROF], section 9.5, specifies the content the non-critical extension authorityInformationAccess containing id-adcaIssuers and id-ad-ocsp in subsection.

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

- **policyMapping**
- **subjectDirectoryAttributes**
- **nameConstraints**
- **policyConstraints**
- **inhibitAnyPolicy**

[CERTPROF] specifies all extensions, and list above is not included. This is emphasized in the specification section 1.1.

7.1.3 Algorithm object identifiers

N/A. The CP does not pose any policy requirements.

7.1.4 Name forms

[REQ 7.1.4-01] The designation 'Kvalificeret' or 'Qualified' shall form part of the CA certificates' commonName.
[CERTPROF], section 7.3 and 8.3 specifies the naming of qualified root and intermediate certificates. For both certificates the term 'kvalificeret' is includes in the certificate subject common name as:

- Root CA: 'Den Danske Stat kvalificeret rod-CA'
- Intermediate CA: 'Den Danske Stat kvalificeret udstedende-CA N'

Where N is index of the current active intermediate CA starting from 1...

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

- **countryName,**
- **either (givenName and surname) or pseudonym,**
- **commonName and**
- **serialNumber.**

[CERTPROF], section 9.3 specifies the subject name attributes and includes exactly those mentioned above.

[REQ 7.1.4-03] countryName shall have the value 'DK'.
[CERTPROF], section 9.3 specifies the subject name attribute countryName to 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. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used.
Certificate subject name is determined by information received from the Login Service as described in REQ 3.2-02, 3.2-03 and 3.2-04.
The service provider using the Signing Server, may instruct the Signer Service to use the pseudonym 'Pseudonym' in commonName and leave givenName and surname unused.

[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.

The subject serialNumber is specified in [CERTPROF] section 1.5 and has the information: UI:DK-<identity type acronym>:<persistence level acronym>:<uuid>, where identity type acronym can be P, E or O indicating if the certificate is issued according to respectively [Qualified Person], [Qualified Employee] or [Qualified Organisation]. Persistence level acronym can be either G, C or S to indicate Global, Certificate or Session.

7.1.5 Name constraints

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

[CERTPROF] specifies supported subject names and they can only occur once. any attribute of subject name

[REQ 7.1.5-02] The pseudonym attribute shall not be present if the givenName and surname attribute are present.

See REQ 7.1.4-04.

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.

[CERTPROF] specifies that OIDs from clause 1.2.2 of relevant CPs.

[REQ 7.1.6-02] OIDs for qualified CPs prepared by the Danish Agency for Digitisation may only be referred to in a certificate or written agreement with the Agency.

Includes OID's mentioned in 7.1.6-01 as per agreement with the Agency for Digitisation.

[REQ 7.1.6-03] All certificates issued under this CP shall refer to QCP-n-qscd by stating OID:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

in certificatePolicies extension.

[CERTPROF] specifies for all certificate which policies that are used for issuing.

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

[CERTPROF] specifies for all certificates that the certificatePolicies extension is not 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. The CP does not pose any policy requirements.

7.1.9 Processing semantics for the critical Certificate Policies extension

N/A. The CP does not pose any policy requirements.

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.

[CERTPROF] section 14 specifies CRL issued by the PKI System is compliant with IETF RFC 5280 [RFC5280].

[REQ 7.2-02] thisUpdate and nextUpdate shall be stated in UTCTime format YYMMDDHHMMSSz.

[CERTPROF] specifies that CRLs thisUpdate and nextUpdate are encoded in UTCTime format.

[REQ 7.2-03] If the CA decides to terminate the issuance of CRLs, the CA shall issue and publish at the corresponding CRL distribution point a last CRL with a nextUpdate field containing the value '99991231235959Z'

As part of the termination of the issuance of CRL's, Den Danske State will issue a final CRL with the nextUpdate value '99991231235959Z'.

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).
[CERTPROF] specifies that CRLs issued by the PKI System has version number 2.

7.2.2 CRL and CRL entry extensions

[REQ 7.2.2-01] If CA does not remove revoked certificates from CRLs, the CRLs shall include the 'expiredCertsOnCRL' extension as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509.
Den Danske Stat keeps revoked certificates on CRL after certificate expiry. This is indicted in [CERTPROF] section 14.2 where it is specified that the CRL extension expiredCertificatesOnCRL is marked as non-critical.

[REQ 7.2.2-02] If CA removes revoked certificates from CRLs, the CRLs must not include the 'expiredCertsOnCRL' extension as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509.
See REQ 7.2.2-01. Revoked certificates are kept on the CRL after certificate expiry.

7.3 OCSP profile

[REQ 7.3-01] The OCSP shall be as defined in IETF RFC 6960.
[CERTPROF] section 15 specifies the OCSP responses generated by the PKI System is compliant with [RFC6960].

[REQ 7.3-02] The OCSP shall use a profile that complies with IETF RFC 5019. However, SHA1 can be replaced by more secure algorithms such as SHA256.
See REQ 7.3-01.
Note that for security reasons the hash algorithm is SHA256 and not as required by [RFC5019] SHA-1.

[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.
[CERTPROF] section 15 specifies that the OCSP responder will return the status unknown in case a request for a certificate that has not been issued.

[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.
The VA/OCSP appliance logs to a SIEM, including events for requests for non-issued certificates. As part of the security response procedures a trigger is implemented to alert the monitoring team in case of repeated requests.

7.3.1 Version number(s)

[REQ 7.3.1-01] The OCSP responder shall support version number 'v1' (0x0).
[CERTPROF] section 15 specifies that OCSP responses issued by the PKI System has version number 1.

7.3.2 OCSP extensions

[REQ 7.3.2-01] The OCSP responder should use the archiveCutOff extension as specified in IETF RFC 6960, with the date set to the CA certificate's 'notBefore' value.
[CERTPROF] section 15 specifies that archiveCutOff is used.

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.
All common systems under trust service policies and practise statements are regularly audited by internal auditor.

[REQ 8.1-02] An external conformity assessment shall be undertaken of the CA's overall system by a conformity assessment body, cf. 8.2-01, at least once a year.
Den Danske Stat acting as qualified trust service provider offering qualified trust services is conformity assessed 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 shall be as defined in eIDAS article 3, letter 18).
A conformity assessment body is selected based on the eIDAS requirements to ensure assessment of qualified trust services under EU regulation.

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.
The external audit / CAB and the internal audit shall cooperate.

8.4 Topics covered by assessment

[REQ 8.4-01] The conformity assessment body shall ensure that the CA meets the requirements for qualified trust service providers, cf. eIDAS and requirements in this CP.
The Conformity Assessment Body are auditing that the Den Danske Stat is fulfilling requirements in the CP's.

[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.
The PKI System complies with relevant regulations where applicable. This is documented by providing an auditor signed assessment report under these CP's, that do not contradict with said statement.

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.
Irregularities reported by CAB will be on the agenda on the next Den Danske Stat management meeting.

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.
Den Danske Stat management will inform the Supervisory Authority operated by the Agency for Digitisation about conditions which might affect the continued service.

Den Danske Stat will inform the CAB in writing of the tasks required by the CAB.

[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.
A Conformity Assessment Body is conducting an annual audit and delivers a Conformity Assessment Report to Den Danske Stat 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.**

The conformity assessment body is instructed to perform the assessment according to the requirements in trust policies and national/EU guidance.

9 Other business and legal matters

[REQ 9-01] The CA organization shall be reliable and non-discriminatory.
See REQ 9-02.

[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.
Den Danske Stat's services are accessible to all applicants whose activities fall within the declared field of operation and that agree to abide by their obligations as specified in the Terms and Conditions [T&C].
This includes that Den Danske Stat's webpage are compliant with the Danish law "LOV nr. 692 af 08/06/2018 - Lov om tilgængelighed af offentlige organers websteder og mobilapplikationer".

[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.
See REQ 9-02.
The trust services and its user interfaces have all undergone thorough user experience and accessibility testing in accordance with the Danish law on web accessibility that is inspired by EN 301 549 and WCAG 2.1 AA. This to ensure that the CA services and end-user products are accessible for persons with disabilities.

[REQ 9-04] The CA shall support a 'PKI disclosure statement', cf. ETSI EN 319 411-1. The PKI disclosure statement should be structured according to annex A in ETSI EN 319 411-1.
The Den Danske Stat's "PKI disclosure statement" [PDS] is made public on https://ca1.gov.dk.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

N/A. The CP does not pose any policy requirements.

9.1.2 Certificate access fees

N/A. The CP does not pose any policy requirements.

9.1.3 Revocation or status information access fees

N/A. The CP does not pose any policy requirements.

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.
Den Danske Stat defrays all expenses related to system auditing either directly or via contracts with subtractors.

9.1.5 Refund policy

N/A. The CP does not pose any policy requirements.

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.
Den Danske Stat is as the Danish State a public self-ensured entity.

[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.
As a public authority Den Danske Stat is self-insured and does therefore not adhere to insurance requirements in the certificate policies.

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.
As the Danish state action as the Den Danske Stat it is assessed that Den Danske Stat have the required stability and financial recourses to be in compliance with implemented certificate policies.

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. The CP does not pose any policy requirements.

9.3.2 Information not within the scope of confidential information

N/A. The CP does not pose any policy requirements.

9.3.3 Responsibility to protect confidential information

N/A. The CP does not pose any policy requirements.

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.
Den Danske Stat has appointed a Data Protection Officer (DPO) and has implemented data processing agreements with subcontractors which includes clauses mandated by GDPR.

[REQ 9.4.1-02] Moreover, the confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber or between distributed CA system components.
A Data Processing Impact Assessment (DPIA) and risk assessments are maintained to ensure that personal data is protected at an adequate level.

[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.
See REQ 9.4.1-02.

9.4.2 Information treated as private

N/A. The CP does not pose any policy requirements.

9.4.3 Information not deemed private

N/A. The CP does not pose any policy requirements.

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.
Private information is protected under the instructions from the data controller Agency for Digitisation, and private information are only used for providing trust services and qualified trust services.

[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.
Private information is protected under the instructions from Agency for Digitisation, and private information are only used for providing trust services and qualified trust services.

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
Data retention policies are communicated via Terms and Conditions [T&C].

9.4.6 Disclosure pursuant to judicial or administrative process

N/A. The CP does not pose any policy requirements.

9.4.7 Other information disclosure circumstances

N/A. The CP does not pose any policy requirements.

9.5 Intellectual property rights

[REQ 9.5-01] The Danish Agency for Digitisation holds all rights to this certificate policy. Use of this CP's policy-OID in certificates is subject to written agreement with the Danish Agency for Digitisation.
Den Danske Stat will not issue any certificate (except for internal test purposes) which includes Policy-OIDs before the Den Danske Stat is approved as qualified TSP.
Den Danske Stat has obtained the required approvals to use of CP's policy-OID in certificates under this CPS.

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.
Den Danske Stat has the ultimate responsibility of compliance to the implemented certificate policies. Subcontractors' compliance is controlled via written contracts.

[REQ 9.6.1-02] The CA shall provide all its certificate services consistent with its CPS.
All trust services (non-qualified and qualified) are provided in compliance with the applicable trust service policies requirements.

[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.
Den Danske Stat's liability is stated in the PKI Disclosure Statement [PDS].

[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.
Den Danske Stat's liability is stated in the PKI Disclosure Statement [PDS].

9.6.2 RA representations and warranties

N/A. The CP does not pose any policy requirements.

9.6.3 Subscriber representations and warranties

N/A. The CP does not pose any policy requirements.

9.6.4 Relying party representations and warranties

N/A. The CP does not pose any policy requirements.

9.6.5 Representations and warranties of other participants

N/A. The CP does not pose any policy requirements.

9.7 Disclaimers of warranties

N/A. The CP does not pose any policy requirements.

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.
Any liability limitation will be published in Den Danske Stat Terms and Conditions [T&C] and/or in the PKI disclosure statements [PDS].

[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.
See REQ 9.8-01.

9.9 Indemnities

N/A. The CP does not pose any policy requirement.

9.10 Term and termination

9.10.1 Term

N/A. The CP does not pose any policy requirements.

9.10.2 Termination

N/A. The CP does not pose any policy requirements.

9.10.3 Effect of termination and survival

N/A. The CP does not pose any policy requirements.

9.11 Individual notices and communication 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.
Den Danske Stat has procedures for the support requests received from customers or other relying parties.

9.12 Amendments

9.12.1 Procedure for amendment

N/A. The CP does not pose any policy requirements.

9.12.2 Notification mechanism and period

N/A. The CP does not pose any policy requirements.

9.12.3 Circumstances under which OID must be changed

N/A. The CP does not pose any policy requirements.

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.
Den Danske Stat has procedures for the resolution of complaints and disputes received from customers or other relying parties.

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.
These procedures include ultimately that a dispute can be solved in a Danish court.

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.
Compliance with regulation of processing personal data is ensured via DPIA and compliance with eIDAS is ensured via conformance assessment reports from an approved Conformance Assessment Body according to eIDAS article 21.

[REQ 9.15-02] In particular, the CA shall provide evidence of how it meets applicable data protection legislation within its registration process.
Den Danske Stat maintains a data protection impact assessment for the PKI System.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

N/A. The CP does not pose any policy requirements.

9.16.2 Assignment

N/A. The CP does not pose any policy requirements.

9.16.3 Severability

N/A. The CP does not pose any policy requirements.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

N/A. The CP does not pose any policy requirements.

9.16.5 Force Majeure

N/A. The CP does not pose any policy requirements.

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.
All subcontractors running services on behalf of the Den Danske Stat are controlled via written contracts.

[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.
Den Danske Stat management is organized in the Agency for Digitisation such that conflicts of interest among staff including management is avoided.

[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.
See REQ 9.17-02.

[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.
See REQ 9.17-02.

[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.
Den Danske Stat provides a test environment for service providers such that integration to the services in the PKI System can be tested.
Third parties can validate and test all types of issued certificates via OCSP, CRL (http) and LDAP.

[REQ 9.17-06] Any test certificates should clearly indicate that they are for testing purposes.
Test certificates are provided and tested using a separate PKI environment.
All CA certificates used for test includes the subject name attribute organizationUnitName which contain the value 'Test – 'followed by an indication of the test environment that has issued the certificate.
Since CA subject name appears as issuer name in the subject certificate, all certificates related to the test environment will have an indication that the certificate is issued by a test system.
[CERTPROF] specifies this throughout the documents.

[REQ 9.17-07] Certificates for testing purposes may not be issued under the same root CA as certificates for subjects.
Test certificates are provided and tested using a separate PKI environment.