Agency for Digital Government

DEN DANSKE STAT

Certification Practice Statement

Version: 2.0

Author: Danish Agency for Digital Government, Den Danske Stat

Date: 12-02-2026

Den Danske Stat Trust Services

CONTENTS

Changelog

Version	Dato	Description
2.0	12-02-2026.	Initial version based on introduction of certificate policy covering all certificate types issued by Den Danske Stat.

1. Introduction

1.1. Overview

The Agency for Digital Government has established a trust service provider Den Danske Stat, which provides certification services which meet 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 management of remote QSCD.
This document, being a CPS, describes Participants of the Certification Authority. There are supplementary practice documents describing the other trust services.

The provided infrastructure uses two certificate hierarchies to issue qualified and public certificates for electronic services. Qualified certificates and non-qualified certificates are issued to natural persons, legel persons and natural person associated with a legal person using the certificate policies referenced in [CP]. 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) certification(1) major-ver(2) minor-ver(0).

1.3. PKI participants

The PKI Participants of the Den Danske Stat are the entities which consume services or provide services which allow the Den Danske Stat to provide certification services.

The PKI Participants are identified as the following:

- Certificate Authorities
- Registration Authorities (eID Services, Connection Service and MitID Erhverv)
- Subscribers
- Relying Parties
- Other Participants
    - Certificate Revocation Service
    - Certificate Revocation Status Service
    - Repository Services

1.3.1. Certificate Authorities

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 a subordinate CA certificate to issue subject certificates.

The CA system also provides OCSP and time stamp service certificates as illustrated below.

- 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 person
    - OCES employee
    - OCES organization
    - OCES OCSP Responder for subject certificates
  - OCES OCSP Responder for CA certificates

Den Danske Stat has been assessed for conformity under the regulation [eIDAS] and to meet the requirements 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.

Consult [GRPS] clause 7.1.1 for general considerations on Organization reliability.

Den Danske Stat relies on eID services provided by Local IdPs, MitID and MitID Erhverv. In addition, Den Danske Stat has entered into 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 local IdP's, MitID and MitID Erhverv eID service to provide subject registration information.

1.3.2. Registration authorities

1.3.2.1. IDENTITY PROVIDERS

The Login Service acts as broker for other Identity Providers, including Local IdPs, MitID and MitID Erhverv. All supported IdPs are required to be NSIS notified to the Danish supervisory body and appear on the national Danish list for approved identity services meeting requirements in NSIS. This list is available here:

https://digst.dk/nsis/

Identity Providers used by the Login Service are required to be NSIS notified with an assurance level of at least substantial. Since NSIS assurance level substantial does not meet the requirements in [eIDAS] article 24.1 for natural persons, identities which are created in MitID Erhverv using a local IdP and which intends to use the Signing Service for qualified signing, are required to conduct an additional identity proofing. This, activation flow, requires the subject to log on to MitID Erhverv using MitID to ensure that MitID Erhverv marks the subject to be eligible to receive a qualified certificate. See also 1.3.2.3. If the activation flow is not conducted, the subject may only carry out an advanced signature with an OCES certificate.

1.3.2.2. CONNECTION SERVICE

The purpose of the Connection Service is to enrol legal persons (organisations) into MitID Erhverv. This covers verification of the authorised representative, registration in the MitID Erhverv application and appointment of an organisation administrator, who can then manage the organisation within MitID Erhverv.

The Connection Service leverages on the Danish Central Business Register (CVR) for information on the organisation to be enrolled. For some organisations the information in the CVR contains the authorised representative and the enrolment is fully automatic. For organisations, where the authorised representative is not available in the CVR, a manual verification of supplied documentation is conducted prior to enrolment of the organisation.

The CVR is in Denmark considered by law to be an authoritative source for company information.

The involved processes and the Connection Service application are described in internal detailed documents which are conformity assessed to be conformant to [ETSI TS 119 461] with LoIP Extended.

During enrolment, the full name and CVR number are collected from the CVR.

1.3.2.3. MITID ERHVERV

Once an organisation has been enrolled to MitID Erhverv, natural persons (e.g. employees) can be associated with the organisation.

Identity verification of the natural person to be associated with the organisation is conducted by an eID scheme, which may be MitID. These schemes have been conformity assessed to meet the requirements in eIDAS article 24.1.

During the association, the natural person must use a private eID with an assurance level of at least substantial to log in to MitID Erhverv. This serves as identity verification with regard to MitID Erhverv.

MitID Erhverv allows for Local IdMs and Local IdPs which are NSIS approved to create eIDs for natural persons associated with legal persons within MitID Erhverv. As Local IdMs and Local IdPs which are NSIS approved may not meet the requirements in eIDAS 24.1, MitID Erhverv requires that before a subject created by these systems, can be granted a qualified certificate, the subject must complete an activation flow by using MitID to log on to MitID Erhverv. By performing a log on using one of these schemes, MitID Erhverv acknowledges that the subject has been identified to meet the requirements in eIDAS 24.1.

The involved processes and the MitID Erhverv application are described in detailed internal documents which are audited to be conformant to NSIS assurance level at least substantial. The NSIS report is available to the trust service provider's assessment body.

MitID Erhverv is used to issue long term advanced and qualified certificates.
The services exposed by MitID Erhverv are available as a WEB Browser based application accessible at:

https://MitID-Erhverv.dk
It may be used through MitID Erhverv GUI or via a WEB-Services API (MitID Erhverv API).

1.3.2.4. AUTHORISED REPRESENTATIVE

For organisations with only one registered authorised representative in CVR, typically smaller organisations, it is possible to leverage on this information from the CVR through the Login Service, without requiring the organisation to be connected to MitID Erhverv. The only thing the authorised representative is required to do is to use his or her private MitID as authentication and identification means.

With private MitID as authentication and identification means, the natural person due to MitID being NSIS notified and eIDAS 24.1 conformity assessed, has been identity verified and authenticated with an assurance level of at least substantial. Since the CVR is by Danish law, considered as an authoritative source, the binding between the natural person and the legal person is established and the authorised representative is capable to perform a qualified signature as a natural person associated to the legal person (employee). See 1.3.3.

Since, in this case, the binding between the natural person and the legal person is conducted using CVR, revocation of the binding shall be conducted within CVR. Revocation of short-term certificates is conducted by following the procedure described in 1.3.6.1.

1.3.3. Signing Service

Den Danske Stat issues short term qualified 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 or local IdPs and redirects the signee to the relevant service for authentication. Once the signee is authenticated information is provided back to the Login Service. The Login Service queries MitID Erhverv if the authenticated subject is either associated to any legal entities or is authorized to seal on behalf of any legal entities. The subject is displayed a list of identities covering the natural person, natural persons associated with legal persons and legal persons for which the authenticated subject can create a signature or seal. The subject selects the relevant identity, and the Login component forms a SAML Assertion with the selected identity and returns that 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.

The Signing Service is used to issue short term advanced and qualified certificates.

1.3.3.1. EIDAS ARTICLE 24.1

Before a qualified certificate can be issued, the CA shall ensure that the requirements in [eIDAS], article 24 are fulfilled. In particular, the CA is responsible for verification of the identity and special attributes associated with the subject.

The identity verification processes for MitID and MitID Erhverv have been conformity assessed to meet the requirements in [ETSI TS 119 461] for extended LoIP. This allows the TSP to issue qualified certificates if MitID and MitID Erhverv is used as identity provider.

For NSIS notified Local IdPs, this is not considered sufficient by the TSP to issue a qualified certificate and only OCES certificates can be issued. If the Local IdP is conformity assessed to meet the requirements in [ETSI TS 119 461] the TSP may issue qualified certificates.

1.3.4. Subscribers

The subscribers of certificates issued to a natural person are natural persons, which meet the requirements as stated in the previous section. For other certificates, the subscriber is the organization requesting the certificate.
Subscribers are eligible for 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.

1.3.5. Relying parties

The Relying Parties of certificates issued by the Den Danske Stat are natural and legal persons, who rely 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 [Profile].
- The validity of the certificate is checked through the certificate revocation services (e.g. CRL and OCSP) mentioned in section 0.
- 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.

1.3.6. Other participants

1.3.6.1. CERTIFICATE REVOCATION

Subscribers can revoke long term OCES and qualified certificates issued to legal persons or natural persons associated with a legal person through MitID Erhverv. 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

Short-term certificates contain the "validity assured" extension (**ext-etsi-valassured-ST-certs**) can - due to the implications of this extension, by nature - not be revoked.

1.3.6.2. 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.

1.3.6.3. 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 this is available at **https://www.ca1.gov.dk/**

1.4. Certificate usage

1.4.1. Appropriate certificate uses

The certificates can be used for securing sender authenticity and message authenticity and integrity as set forth in the Terms and Conditions [T&C].

The validity of subject certificates is described [Profile], which states that certificates are issued with a validity ranging from 12 hours to 3 years.

1.4.2. Prohibited certificate uses

OCES certificates can be used for securing sender authenticity and message authenticity and integrity as set forth in the Terms and Conditions [T&C].

Subject certificates shall not be used for signing subordinate certificates as expressed in the certificate extension basicConstraints where CA is set to FALSE. See [Profile] for details.

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 [NSIS] Level of Assurance at least substantial with the addition for qualified certificates that the identity verification process meets the requirements in [ETSI TS 119 461] for extended LoIP.

The Qualified Signature Creation Device manages the subject's 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.

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

1.5. Policy administration

1.5.1. Organization administrating the document

Agency for Digital Government 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

Den Danske Stat trust services are offered by the Agency for Digital Government on behalf of the Danish state. The issuance of OCES certificates is carried out after the Danish Supervisory Body has approved a

conformity assessment report and that the certificate issuance service appears on the LoTL[1] (List of Trusted Lists) as a non-qualified service.

Den Danske Stat TSP provides a conformity assessment report each year to the Danish Supervisory Body at the Danish Agency for Digital Government.

Each Year, Den Danske Stat TSP submits a report to the Danish Supervisory Body containing:

- Certification Practice Statement
- Conformity Assessment report received from Conformity Assessment Body
- Declaration from the CA's management indicating that CA's overall data, system and operational security are considered adequate and that the CPS addresses all requirements of this CP and that the CA complies with its own CPS.

The Danish State TSP acting as a state institution is self-insured and no additional evidence is provided.

The report will be partly in Danish (declaration from CA management) and partly in English (CPS) according to the requirements.

1.5.4. CPS approval procedures

Consult [GRPS] clause 6.1 for general considerations on Trust Serve Practice Statements.

Den Danske Stat has defined and maintains a CPS, this document, which addresses all requirements in the applicable certificate policy. The structure of the CPS follows outline provided in [RFC3647] and includes all applicable requirements sections in the relevant CP's for all CA-hierarchies in the PKI System.
The certificate profile [Profile] document is published at Den Danske Stat TSPs repository and describes the signature parameters for all usages of root, intermediate certificates and OCSP responder certificates when issuing certificates, CRLs and OCSP responses.

[1] The LoTL can be retrieved at https://ec.europa.eu/tools/lotl/eu-lotl.xml

1.6. Definitions and Acronyms

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.
Employee	Natural person associated with legal person. In MitID Erhverv that is the used term.
Identity Provider (IdP)	Identity Provider provides electronic identification and authentication services.
Login service	NemLog-in Login broker acting as Registration Authority for subjects that get certificates issued through the Signing Service. It leverages on MitID.
OCSP	Online Certificate Status Protocol providing revocation status for requested certificates.
Organization	Legal person. In MitID Erhverv that is the used term.
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 between 12 hours (if extension **ext-etsi-valassured-ST-certs** extension is present in certificate) and 10 days (if extension **ext-etsi-valassured-ST-certs** extension is absent in certificate).
Signing Service	The Signing Service provided by Den Danske Stat offering subjects to create qualified signatures.
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 electronic signature being 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

Consult [GRPS] clause 6.2 for general considerations on Terms and Conditions.

The terms and conditions include all required elements, including:

- indication of what constitutes certificate acceptance
- the period of time for which the records are retained
- the subscriber's and where applicable the subject's obligations
- the notice to relying parties

The document [Profile] describes the content of all roots, intermediates and subject certificates issued by Den Danske Stat TSP. This includes signature algorithms and parameters.

Consult [GRPS] clause 6.1 for general considerations on trust service practice statements and publication in TSP repository.

The terms and conditions for the individual certificate types are available on a 24/7 basis in the TSP repository.

2.2. Publication of certification information

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.

Certificates issued through MitID Erhverv can be requested to be published in a repository accessible through LDAP. The subject that retrieves the certificate, determines if it should be published. Published certificates are not deleted.

Advanced and qualified short-term certificates issued during a signing session in the Signing Service are made available for the signer as part of the advanced signature format [AdES].

Certificates issued through MitID Erhverv GUI is available to the subject within the MitID Erhverv GUI.

For certificates issued through MitID Erhverv API, the subscriber is required via the MitID Erhverv terms and conditions to make the certificate available for the subject.

The TSP has not entered any agreements with any other TSP to cross certify any CA certificates.

2.3. Time or frequency of publication

N/A – there is no policy requirements.

2.4. Access control on repositories

N/A – there is no policy requirements.

3. Identification and authentication

3.1. Naming

3.1.1. Type of names

For certificates with an organizationIdentifier, the Connection Service checks that the name of the organisation is registered with the name in CVR or for certificates issued through the Signing Service for authorised representatives, the Login Service queries the CVR through MitID Erhverv. The CVR number will always be included in these certificates as subject organizationIdentifier [Profile].

For certificates issued to a natural person or natural person associated with a legal person, 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

For certificates with an organizationIdentifier, the organizationName is retrieved from CVR during organisation enrolment or for certificates issued through the Signing Service for authorised representatives, the Login Service queries the CVR through MitID Erhverv.

For certificates issued to a natural person, the assessment of the identity verification carried out by MitID as mentioned in 1.3.2 covers that the subject name has been verified via an authoritative source.

For certificates issued to a natural person or natural person associated with a legal person, the Subject DN commonName, surname and givenName attributes will contain the name of the subject as defined by the registered name in CPR or as received in authentication claims from MitID. Nicknames, and names with spelling other than registered are not supported.

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

See section 3.1.2 on the use of pseudonyms.

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

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

Section 1.3.2 describes how the TSP uses identity providers for subject identity verification.

For certificates issued through MitID Erhverv, the subscriber attributes are received from CVR register and the Connection Service. For certificates issued to a natural person associated with a legal person, subject attributes are also retrieved during the association of the employee with the organisation using private MitID.

During a signing session, the Signing Client will redirect the session to the Login Service. The subject submits authentication credentials and upon successful authentication, the Login Service returns a SAML response containing the authentication information including the subject's naming attributes, which will be used for a certificate signing request.

For certificates issued through the Signing Service, subject attributes are received from the Login service. The Login service collects the subject attributes from different sources:

- For certificates issued to a natural person, the Login service uses MitID or a Local IdP.
- For other certificates the Login service uses MitID Erhverv and MitID or a Local IdP.

[Profile] describes the certificate's subject attributes.

MitID, MitID Erhverv and Local IdPs which have been conformity assessed to meet the requirements in [ETSI TS 119 461] with target Extended LoIP and can be used to issue OCES and qualified certificates. Local IdPs which have been audited to meet the requirements in [NSIS] at level substantial or high and not conformity assessed to meet the requirements in [ETSI TS 119 461] can be used to issue OCES certificates.

In the case where subjects are registered as entities associated with the organisation managing the CA on behalf of Den Danske Stat, the registration is conducted by a part of the organisation separated from the part responsible for the management of the CA.

All certificates are issued with a unique identifier by which the subject may be referenced.

By using identity providers, the TSP ensures that registration officers are not the natural person to whom the certificate is issued.

3.2.1. Method to prove possession of private key

For certificates issued through MitID Erhverv, the MitID Erhverv application verifies that the certification request contains proof-of-possession.

3.2.2. Authentication of organization identity

See section 1.3.2.2 on identity verification of legal persons.

3.2.3. Authentication of individual identity

See section 1.3.2.1 on identity verification of natural persons.

The TSP receives the subject naming attributes from the identity provider including identifiers (CPR, MitID-CPR) which uniquely identifies the subject.

3.2.4. Non-verified subscriber information

For certificates issued through the Signing Service, the Subscriber is identified as a natural person. All subscribers are contacted using the mandatory Danish National Digital Mail system (Digital Post)[2].
For all other certificates, an email is registered for the organisation administrator which may be used to contact the organization.

The TSP has a Data Protection Impact Assessment (DPIA) which ensures that registration data is handled with privacy in mind.

The TSP only collects attributes which are required for issue of the intended certificate.

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

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

3.3.1. Identification and authentication for routine re-key

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

3.3.2. Identification and authentication re-key after revocation

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

3.4. Identification and authentication for revocation request

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

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

4. Certificate life-cycle operational requirements

4.1. Certification Application

4.1.1. Who can submit a certification application

Subjects associated with a legal person in MitID Erhverv may have certificates issued to natural persons associated to the legal person or if authorized to the legal person. The certificates can be issued either through MitID Erhverv or through the Signing Service.

4.1.2. Enrolment process and responsibilities

For certificates issued through the Signing Service, the subject is authenticated using the Login service. The Login service uses MitID Erhverv to provide the subject with a list of organisational and employee identities for which the subject is allowed to request a certificate.

For certificates issued through MitID Erhverv, the application verifies that the requester is authorized to apply for the relevant certificate.

All processes used for initial verification of subject's identity and attributes are applicable for identity proofing for the TSP. The TSP has not posed any limits on the validity of the initial identity proofing for issuance of certificates.

4.2. Certification application processing

4.2.1. Performing identification and authentication functions

See sections 1.3.2 and **Fejl! Henvisningskilde ikke fundet.** on subject identification.

For certificates with an organizationIdentifier, MitID Erhverv uses the CVR register, to ensure the subject attributes organizationName matches the CVR number in organizationIdentifier.

For certificates issued to a natural person or a natural person associated with a legal person, the subject specific attributes common name, given name, surname and pseudonym are verified against the CPR register, if CPR number is available. If the CPR number is not available the subscriber has the responsibility of to ensure the attributes are valid, as stipulated in [T&C].

All processes for initial subject verification of the subject's identity and attributes are valid at the time of certificate issuance.

Den Danske Stat TSP does not pose any limit on the validity of the initial identity verification and issues certificates as long as the registration in MitID Erhverv is not revoked, or as long as the subject's electronic identification means with the identity provider is valid.

4.2.2. Approval or rejection of certificate applications

The TSP immediately accepts all certificate applications provided by the Signing Service or MitID Erhverv. Note that certificate applications (CSRs) received by MitID Erhverv are verified by MitID Erhverv and in case the verification fails, a status is immediately returned.

4.2.3. Time to process certificate applications

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

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

For certificates issued through MitID Erhverv, the application ensures that the certificate is associated with an organisation or employee identity within MitID Erhverv and that the certificate subject attributes correspond to the identity.

Certificate applications are accepted from the trusted and authorized sources Signing Service and MitID Erhverv. MitID Erhverv checks that if the certificate application is submitted from an organization, that the organization is allowed to provide the application.

Den Danske Stat does not use external registration service providers when issuing certificates.

The Signing Service uses origin authenticated subscriber naming attributes received from the Login Service. Upon receiving these attributes, the Signing Service requests 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 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.

For certificates issued through MitID Erhverv, the application either receives a certification request through the MitID Erhverv API, or the subject uses MitID Erhverv Gui to request a new certificate. When MitID Erhverv receives the certification request, it verifies the subject attributes and requests the CA Service to issue a certificate under the applicable policy. Once the certificate is received by MitID Erhverv it is stored in the MitID Erhverv database and made available to the requester.

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.

The certificate serial numbers of the issued certificates are generated with unpredictable 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.

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.

The TSP manages subject private keys on the user's behalf and does not pass them to the 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.

For certificates issued to a natural person associated with a legal person, the certificate includes subscriber and subject attributes.

Subject certificates include the policy identifiers as required by the [CP]. Consult [Profile] for information on certificate content.

4.3.2. Notification to subscriber by the CA of issuance of certificate

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

Den Danske Stat's Terms and Conditions [T&C] state what is considered to constitute acceptance of the certificate.

For certificates issued to a natural person or a natural person associated with a legal person for authorised representatives through the Signing Service, acceptance of Den Danske Stat's Terms and Conditions [T&C] in the Login Service is an integrated part of the signing session.

For all other certificates, Den Danske Stat's Terms and Conditions [T&C] shall be approved by the subscriber as part of enrolling the organisation using the Connection Service into MitID Erhverv.

For certificates issued through MitID Erhverv GUI, the subject is always required to accept Den Danske Stat's Terms and Conditions [T&C].

For certificates issued through MitID Erhverv API, the subscriber is obliged via terms and conditions [T&C] to inform the subject of his/her obligations.

The Terms and Conditions [T&C] are presented to the subject

- by the Login Service during the signing session, or
- by the Connection Service for subscriber,
- by MitID Erhverv GUI if the certificates are issued through the client.

The subject must accept them for the certificate to be issued.
For certificates issued through the MitID Erhverv API, the organisation using the API is responsible for ensuring that the Terms and Conditions [T&C] are presented to the subject.

All versions of the Terms and Conditions [T&C] are made available on:

https://www.ca1.gov.dk.

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] are an integrated part of a larger agreement complex.

The Login Service, the Connection Service and MitID Erhverv GUI record which version of the Terms and Conditions [T&C], that was accepted by the subject and subscribers. For certificates issued through the MitID Erhverv SDK, the subscriber is by contract obliged to record this information.

The acceptance of the Terms and Conditions [T&C], within the Login Service, Connection Service and MitID Erhverv GUI require the subject/subscriber to tick a check box.

Den Danske Stat has included the contractual requirements for relevant certificate policies in the Terms and Conditions [T&C] which are approved by the subscriber during enrolment using the Connection Service to MitID Erhverv. Traceability is ensured by system logic in combination with audit logging.

For certificates issued to a natural person or a natural person associated with a legal person through the Signing Service for authorised representatives, Subscriber and Subject is always one and the same and the Terms and Conditions [T&C] are to be accepted in the Login Service, during the signature flow.

The Terms and Conditions [T&C] include subject requirements and consent for the CA. Traceability is ensured by system logic in combination with audit logging.

The Terms and Conditions [T&C] are in 2 parts. Part 1 addresses the subscriber, and part 2 addresses the subject. Subscriber accepts both parts whereas the subject accepts part 2.

The Login Service, Connection Service and MitID Erhverv retain 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

Certificates issued through the Signing Service are not published.

Certificates issued through MitID Erhverv may be published in LDAP if the certification request instructs the PKI System to publish the certificate.

4.4.3. Notification of certificate issuance by the CA to other entities

N/A. There is no notification to other participants of issued certificates.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

When the TSP manages the subjects private key as part of the signature solution, this is carried out in accordance with [ETSI TS 119 431-1]. The TSP has a separate practice statement covering management of remote QSCD, [rQSCD PS] as a qualified trust service.

Private keys managed by the TSPs remote QSCD are only used for signature and sealing operations under sole control of the subject.

The TSP currently only issues qualified certificates, where the private key is managed by the TSP.

The TPSs terms and conditions [T&C] comply with applicable requirements from the CP.

4.5.2. Relying Party Public Key and Certificate Usage

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

4.6. Certificate renewal

Certificate renewal is only possible for long term organisational and employee certificates through MitID Erhverv.

The requirements for certificate application and certificate issuance are the same as for the initial issuance.

The subject receiving the certificate is always presented with the current version of the TSPs terms and conditions.

The TSP only renews certificates if the current certificate is not revoked due to a security breach and if the cryptographic security is still sufficient for the new certificate's validity period.

Certificates used by the signing service cannot be renewed.

4.6.1. Circumstances for certification renewal

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

4.6.2. Who may request renewal

Certificate renewal can be issued through the MitID Erhverv API or using MitID Erhverv GUI by an employee, who has the privilege.

4.6.3. Processing certificate renewal requests

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

4.6.4. Notification of new certificate issuance to subscriber

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

4.6.5. Conduct constituting acceptance of a renewal certificate

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

4.6.6. Publication of the renewal certificate by the CA

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

4.6.7. Notification of certificate issuance by the CA to other entities

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

4.7. Certificate re-key

4.7.1. Circumstance certificate re-key

The TSP issues new certificates for new public keys through MitID Erhverv using the same procedures as for certificate renewal.

The TSP issues new certificates for new public keys through the signing service using the same procedures as for initial issuance.

4.7.2. Who may request certification of a new public key

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

4.7.3. Processing certificate re-keying requests

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

4.7.4. Notification of new certificate issuance to subscriber

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

4.7.5. Conduct constituting acceptance of a re-keyed certificate

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

4.7.6. Publication of the re-keyed certificate by the CA

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

4.7.7. Notification of certificate issuance by the CA to other entities

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

4.8. Certificate modification

The TSP revokes certificates if the TSP gains knowledge of any changed subject attributes other than the public key.

4.8.1. Circumstances for certificate modification

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

4.8.2. Who may request certificate modification

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

4.8.3. Processing certificate modification requests

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

4.8.4. Notification of new certificate issuance to subscriber

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

4.8.5. Conduct constituting acceptance of modified certificate

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

4.8.6. Publication of the modified certificate by the CA

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

4.8.7. Notification of certificate issuance by the CA to other entities

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

4.9. Certificate revocation and suspension

Certificate can be revoked using the following mechanisms:

- Short-term certificates issued through the Signing Service with the ext-etsi-valassured-ST-certs extension cannot be revoked due to the nature of this extension.
- For certificates issued to a natural person associated with a legal person through MitID Erhverv, the certificate subject can login to MitID Erhverv GUI using the Login service and revoke own certificates.
- For certificates issued to a legal person through MitID Erhverv, an authorized organisation representative can login to MitID Erhverv GUI using the Login service and revoke organisation certificates.
- For certificates issued to a legal person or a natural person associated with a legal person through MitID Erhverv, an organisation certificate authorized to use MitID Erhverv API can use the interface to revoke certificates associated to the organisation.
- Automatically through MitID Erhverv provided the CVR or CPR register indicates relevant subject or subscriber attributes have changed.
- Use the revocation procedures described in [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.

Revocation status information is provided through the applicable urls provided in the certificates for CRLs and OCSP.

If Den Danske Stat becomes aware of circumstances for which a certificate should be revoked, the certificate will be revoked within 12 hours. Den Danske Stat has implemented procedures, [Revocation Procedures], for timely handling of revocation requests from authenticated sources. This includes revocation requests addressed to the support.

Short term certificates issued through the signing service cannot be revoked. In case Den Danske Stat experiences issues with non-revocable certificates, it will make a notification in its repository.

4.9.1. Circumstances revocation

The TSP revokes non-expired long-term certificates if the TSP learns that the certificate is no longer compliant with the CP under which it has been issued or if the used cryptography no longer ensures the binding between the subject and the public key.

MitID Erhverv uses the CVR register to check if the subscriber has changed its name. If this is the case, the MitID Erhverv GUI will notify through the registered emails, that a certificate shall be renewed. If a certificate has not been renewed within 120 days, it will be revoked.

4.9.2. Who can request revocation

See section 4.9 for general considerations of certificate revocation including who can request revocation.

4.9.3. Procedure for revocation request

See section 4.9 for general considerations of certificate revocation including procedures for revocation request.
For legal person certificates and for certificates issued to a natural person associated with a legal person, Den Danske Stat notifies subscribers and subject through registered emails.

Den Danske Stat does not reinstate revoked certificates.

4.9.4. Revocation request grace period

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

4.9.5. Time within which CA must process the revocation request

See section 4.9 for general considerations of certificate revocation including time within which the CA processes the revocation request.

Den Danske Stat does not support planned revocation or support faster revocation times for certain revocation reasons.

The local clock of the equipment running revocation services 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)

The CRL profile as specified in [Profile] for subject certificates, indicates that CRL's are issued within the frequency limits required in the applicable CP's i.e. at least every 24 hours making it compliant with [RFC5280]. If a subject certificate is revoked a new CRL is produced with undue delay.

The CRL profile as specified in [Profile] for intermediate certificates, 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.

Den Danske Stat does not issue cross-certificates to other TSPs.

4.9.8. Maximum latency for CRLs (if applicable)

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

4.9.9. On-line revocation/status checking availability

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

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

4.9.12. Special requirements re-key compromise

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

4.9.13. Circumstances for suspension

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

4.10.1. Operational Characteristics

Den Danske Stat TSP provides revocation status information through CRL and OCSP at the resources stated in the certificate extensions for CRLs and OCSPs.

Certificates issued through the signing service contain the validity assured extension and the TSP does not provide revocation status information for these certificates.

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 profiles as specified in [Profile], describe that OCSP responses are signed by the OCSP responder certificate associated with certificate issuer. This ensures the integrity and authenticity of the OCSP responses.

For certificates where both OCSP and CRLs are provided for revocation status information, the same information will be provided in both sources. While the OCSP responder immediately responds with the correct information, the information in the CRL may be shortly delayed. In case a relying party experiences differences between the information contained in the OCSP Response and latest CRL, the OCSP Response shall be used.

In case the TSP intends to terminate issuance of a CRL, a last version of the CRL is produced and published with the nextUpdate field set to "99991231235959Z".

The last CRL is preserved and available at least until the last issued certificate expires. The duration of various types of issued certificates is listed in the publicly available certificate profile document.

Den Danske Stat maintains termination plans which ensure that all certificates for a CA are revoked before the last CRL is issued.

4.10.2. Service availability

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.

The certificate status services as described in [Profile] are internationally available. Cyber security events may limit the general availability.

4.10.3. Operational features

The TSP provides revocation status information for intermediate and subject certificates, where applicable, through OCSP and CRL.

Revocation status information is provided beyond certificate validity.

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

See section 7.2.2 for additional information on CRL and CRL entry extensions.

The OCSP responder uses the archiveCutOff data set to the CAs certificate notBefore.

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

The TSP does not use key escrow for subject keys. Signing keys are short-term keys and 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

Consult [GRPS] clause 5 for general considerations on Risk Assessment and clause 7.3 for general requirements on Asset management.

5.1. Physical security controls

Consult [GRPS] clause 7.6 for general considerations on Physical and environmental security.

5.1.1. Site location and construction

Consult [GRPS] clause 7.6 for general considerations on Physical and environmental security.

The policy requirements are applied to all locations of the PKI System environments.

5.1.2. Physical access

Consult [GRPS] clause 7.6 for general considerations on Physical and environmental security.

5.1.3. Power and air conditioning

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

5.1.4. Water exposures

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

5.1.5. Fire prevention and protection

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

5.1.6. Media storage

Consult [GRPS] clause 7.3.3 for general considerations on Storage media handling.

5.1.7. Waste disposal

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

5.1.8. Off-site backup

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

5.2. Procedural controls

Consult [GRPS] clause 7.3.2 for general considerations on Assets inventory and classification and clause 7.4 for general considerations on Access control.

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.

5.2.1. Trusted roles

Consult [GRPS] clause 7.2 for general considerations on Human resources.

5.2.2. Number of persons required per task

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

5.2.3. Identification and authentication of each role

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

5.2.4. Roles requiring separation of duties

Consult [GRPS] clause 7.1.2 for general considerations on Segregation of duties.

5.3. Personnel controls

Consult [GRPS] clause 7.2 for general considerations on Human resources.

The TSP relies on subject identification through the use of electronic identity providers as described in section 1.3.

As described in section 1.3.6.1 it is possible to contact the revocation officers of Den Danske Stat.

5.3.1. Qualification, experience and clearance requirements

Consult [GRPS] clause 7.2 for general considerations on Human resources.

5.3.2. Background check procedures

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

5.3.3. Training requirements

Consult [GRPS] clause 7.2 for general considerations on Human resources.

5.3.4. Retraining frequency and requirements

Consult [GRPS] clause 7.2 for general considerations on Human resources.

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

Consult [GRPS] clause 7.2 for general considerations on Human resources.

5.3.7. Independent contractor requirements

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

5.3.8. Documentation supplied to personnel

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

5.4. Audit logging procedures

Consult [GRPS] clause 7.10 for general considerations on Collection of evidence.

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.

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.

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. Subject private keys managed by the TSP are described in [rQSCD PS]. Certificate revocation is logged by the PKI System.

The 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.

The TSP does not provide devices to subjects.

As regarding registration information, 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. For the Connection Service the following applies:

Minutes of meetings (general assembly, board meetings founding meeting), Statutes, Records from CVR and Name from CPR are used as supporting documentation during registration. The name of authorized person, CPR number or birthdate and Authentication tickets from MitID are recorded as unique identification. The Connection Service stores all received information in a database. The Terms and Conditions, [T&C], are accepted during registration and the Connection Service stores the version number of the T&C which was accepted together with which entity who accepted them. The procedures used to validate a legal entity is conformity assessed to meet the requirements in [ETSI TS 119 461] with extended

LoIP. The logs are deleted after 6 months. The system retains in the audit log the type of information presented and who was involved.

The retention policy for audit logs is seven years. No data is planned to be handed over to a third party as part of a termination. In case Den Danske Stat terminates its activities or part if its activities, it is planned not to transfer the relevant activities to other parties.

5.4.1. Types of events recorded

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

5.4.2. Frequency of processing log

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

5.4.3. Retention period for audit log

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

5.4.4. Protection of audit log

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

5.4.5. Audit log back up procedures

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

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

Consult [GRPS] clause 7.10 for general considerations on Collection of evidence.

See section 5.4 on data stored in the audit log.

5.5.1. Types of records archived

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

5.5.2. Retention period for archive

Consult [GRPS] clause 7.10 for general considerations on Collection of evidence.

5.5.3. Protection of archive

Consult [GRPS] clause 7.10 for general considerations on Collection of evidence.

5.5.4. Archive backup procedures

Consult [GRPS] clause 7.11.2 for general considerations on Back up.

5.5.5. Requirements for time-stamping of records

Consult [GRPS] clause 7.10 for general considerations on Collection of evidence.

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

Consult [GRPS] clause 7.10 for general considerations on Collection of evidence.

5.6. Key changeover

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

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

5.7.1. Incident and compromise handling procedures

Consult [GRPS] clause 7.9 for general considerations on Vulnerabilities and Incident management and clause 7.11 for general considerations on Business continuity management.

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.

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.

Via contracts with subcontractors Den Danske Stat ensures that logs and data are 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.

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

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

The subscriber is notified via a relevant channel according to internal security breach procedures. Relying parties are informed through the TSP repository.

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

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.

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

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

5.7.3. Entity private key compromise procedures

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

5.7.4. Business continuity capabilities after a disaster

Consult [GRPS] clause 7.11 for general considerations on Business continuity management.

5.8. CA or RA termination

Consult [GRPS] clause 7.12 for general considerations on TSP termination and termination plans.

6. Technical security controls

Consult [GRPS] clause 7.5 for general considerations on Cryptographic controls.

6.1. Key pair generation and installation

Generation of CA key and revocation status service keys are created securely within cryptographic modules using approved key signing ceremony scripts.

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. 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 as described in [rQSCD PS].

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. Any new PKI System CA certificates will be generated and distributed in accordance with this practise statement. The CA service is planned to cease operation before the expiry of the CA certificate, and the last issued certificates are not allowed to exceed the expiry date of the CA certificate.

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

The key signing ceremony contains the content as required by the policy at the time of executing the ceremony. The key signing ceremony report is signed by a Security Officer and for Root CA also by an independent trustworthy witness.

The TSP does not pre-generate keys.

Den Danske Stat's public keys are published via the EU Commission List of Trusted List which reference the Danish Trusted List.

The TSP provides as a qualified service management of a remote QSCD. The practice statement for this service is described in [rQSCD PS]. This service is used when the TSP generates subject private keys. The TSP does not generate subject private keys, which are not managed by the TSP.

6.1.1. Key pair generation

The PKI Systems [Profile] root CA key pairs are valid for 25 years, and the issuing CA key pairs are valid for 10 years.

6.1.2. Private key delivery to subscriber

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

6.1.3. Public key delivery to certificate issuer

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

6.1.4. CA public key delivery to relying parties

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

6.1.5. Key sizes

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

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)

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

6.2. Private key protection and cryptographic module engineering controls

Den Danske Stat uses the following cryptographic modules which meet the requirement in the following standards:
Den Danske Stat's root keys are generated, protected, and used by cryptographic modules which are certified following Common Criteria (ISO/IEC 15408) for assurance level EAL 4+ using the protection profile [CEN EN 419 221-5].

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 is certified following Common Criteria (ISO/IEC 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.

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

As per design of the cryptographic modules the CA private key, if moved from one cryptographic module to another, or when backed up, is 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.

Backup of CA private keys is 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.

Visual inspection is part of internal compliance reviews and relevant operational procedures to ensure that the seal is not broken.

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.

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

6.2.1. Cryptographic module standards and controls

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

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

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

6.2.3. Private key escrow

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

6.2.4. Private key backup

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

6.2.5. Private key archival

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

6.2.6. Private key transfer into or from a cryptographic module

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

6.2.7. Private key storage on cryptographic module

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

6.2.8. Method of activating private key

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

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

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

6.2.11. Cryptographic Module Rating

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

6.3. Other aspects of key pair management

The TSP has implemented appropriate use of the CAs private signing key and ensures that:

- 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 to 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.

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

See section 6.2 on Private Key Protection and Cryptographic Module Engineering Controls.

The TSP does not issue secure cryptographic devices for subjects.

6.4.1. Activation data generation and installation

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

6.4.2. Activation data protection

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

6.4.3. Other aspects of activation data

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

6.5. Computer security controls

Consult [GRPS] clause 7.5 for general considerations on Access control.

All secure room internal network components are stored inside High Security Zones with the same security requirements as for all devices inside a secure zone.

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.

The cryptographic modules used by Den Danske Stat are operated under dual control, and multifactor authentication is required for all Trusted Roles accessing the modules.

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

Publication of certificates to LDAP is conducted in a fully automated manner by the PKI Systems. There is no system support for any Trusted Roles to publish certificates.

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

6.5.1. Specific computer security technical requirements

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

6.5.2. Computer security rating

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

6.6. Life cycle security controls

Consult [GRPS] clause 7.7 for general considerations on Operation Security, clause 7.6 for general considerations on Physical and environmental security and clause 7.14 for general considerations on Supply Chain.

6.6.1. System development controls

Consult [GRPS] clause 7.7 for general considerations on Operation Security.

6.6.2. Security management controls

Consult [GRPS] clause 6.3 for general consideration on Information security policy and clause 7.7 for general considerations on Operation Security

6.6.3. Life cycle security controls

Consult [GRPS] clause 7.4 for general consideration on Access Control and clause 7.14 for general considerations on Supply Chain.

6.7. Network security controls

Consult [GRPS] clause 7.2 for general considerations on Human resources and clause 7.8 for general considerations on Network security.

All PKI Systems are maintained and protected within secure zones and this includes protection of communications between systems across secure zones and high security zones.

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.

Physical access policy is established to ensure that security zones are limited to authorised personnel and the security practises here for. Critical systems including the root CA are placed in special secure rooms on a separate high-security network and a separate physical security zone.

6.8. Timestamping

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

7. Certificate, CRL, and OCSP profiles

7.1. Certificate profile

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

Public key schemes and algorithms are chosen according to recommendations in [ETSI TS 119 312].

Subject certificates issued by the TSP contain, see [Profile], contains for the issuer field country (DK), organizationName (Den Danske Stat) and commonName. The TSP does not have appropriate registration number which is suitable for inclusion in subject certificates and organizationIdentifier is not used. The value of commonName is specified on [Profile] and is used by the TSP to represent the exact version of the issuing certificates.

The TSP does not provide a legal person identifier as part of the subject certificate issuer field.

All subject certificate attributes for the issuer field only contain one instance of the attribute.

7.1.1. Version number(s)

The certificate profiles, see [Profile], specifies all certificates to be 'V3'.

7.1.2. Certificate extensions

Subject certificates issued through the signing service include the validity assured extensions. The certificates do not contain any location for certificate status information and cannot be revoked. The TSP does not use the validity assured extension in any other certificates.

The certificate profile document [Profile] details which certificate extensions are used by the TSP as well as their criticality.

For qualified certificates the qcStatements are included. It is noted that:

- esi4-qcStatement-1 is included as the certificates are qualified according to [eIDAS].
- esi4-qcStatement-4 is included as the certificates have the private key residing on a QSCD.
- esi4-qcStatement-6 is included as to indicate the QCType which has the value
    - id -etsi-qtc-esign for certificates issued to a natural person and for natural person associated with a legal person
    - id -etsi-qtc-eseal for certificates issued to a legal person

For all subject certificates the qcStatement-2 is included with

- id-etsi-qcs-semanticsId-Natural as semantic identifier for certificates issued to a natural person and for natural person associated with a legal person
- id-etsi-qcs-semanticsId-Legal as semantic identifier for certificates issued to a legal person
- nameRegistrationAuthorities is always https://uid.gov.dk of type URI general-Name

See section 7.1.6 for details certificate policies.

Subject certificates contain authority key identifier with key identifier of the issuers public key.

The content of keyUsage has the values as specified in [ETSI EN 319 412-2].

Subject certificates contain the Authority Information Access extension with access information for issuer and OCSP endpoint. The OCSP endpoint is generally available through the http.

7.1.3. Algorithm object identifiers

See clause 7.1 for information on public key schemes used by the TSP.

7.1.4. Name forms

The certificate profile document, [Profile], specifies the name forms used by the TSP. Each attribute only contains one instance.

In cases where pseudonym is allowed, givenName and surname are not present. Country name is always 'DK'.

Subject serialNumber follows the convention described in the profile document.

For certificates issued to a legal person, the certificate subject commonName is entered into the Connection Service when the organisation is onboarded. The name, as used in certificates, is truncated to 68 characters. If the identity is registered in the CPR register (has a CPR number), givenName will match the CPR register. If the identity is without a CPR number, registration will be performed according to the rules laid out in the Terms and Conditions for MitID Erhverv.

The service provider using the Signing Server, may instruct the Signing Service to use the pseudonym 'Pseudonym' in commonName and leave givenName and surname unused. For certificates issued to a natural person associated with a legal person 'Pseudonym' will also be chosen if the employee within MitID Erhverv is registered as an Anonymous employee.

The certificate profile document describes the sizes of name attributes supported by the TSP. The TSP uses the same language encoding for name attributes.

The organizationName, where applicable, contains the subscriber's registered name.

The organizationIdentifier, where applicable, contains the value NTRDK-xxxxxxxx, where xxxxxxxx is the subjects CVR number registered in Danish Central Business Register.

7.1.5. Name constraints

See section 7.1.4 .

7.1.6. Certificate policy object identifier

See certificate profile, [Profile], for information on used certificate policy identifiers.

7.1.7. Usage of Policy Constraints extension

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

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

The profile document, [Profile], specifies CRL issued by the PKI System is compliant with IETF RFC 5280 [RFC5280]. The CRL are signed by the issuing certificate.

The profile document specifies that CRLs thisUpdate and nextUpdate are encoded in UTCTime format.

7.2.1. Version number(s)

The profile document, [Profile], specifies that CRLs issued by the PKI System has version number 2.

7.2.2. CRL and CRL entry extensions

The TSP issues CRLs which includes the "ExpiredCertsOnCRL" extension to indicate that revoked certificates are not removed from the CRL.

7.3. OCSP profile

The profile document, [Profile], specifies the OCSP responses generated by the PKI System is compliant with [RFC6960].

OCSP responder certificates include the OCSPnoCheck extension and do not include the AuthorityInformationAcccess extension with id-ad-ocsp accessMethod.

As specified in the profile document, the OCSP responder will return the status unknown in case a request for a certificate that has not been issued.

The OCSP responder 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)

The profile document, [Profile], specifies that OCSP responses issued by the TSP has version number 1.

7.3.2. OCSP extensions

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

8. Compliance audit and other assessments

Consult [GRPS] clause 7.13 for general considerations on compliance.

8.1. Frequency or circumstances of assessment

All common systems under trust service policies and practise statements are regularly audited by internal auditor. Den Danske Stat acting as qualified and non-qualified trust service provider offering qualified trust services is conformity assessed at least once a year.

8.2. Identity/qualifications of assessor

A conformity assessment body is selected based on the eIDAS requirements to ensure assessment of qualified trust services under EU regulation. The Danish Agency for Digital Government as supervisory body is made aware of the selected conformity assessment body.

The CA provides a document to the conformity assessment body stating that in accordance with good auditing practices the conformity assessment body must perform system audits including:

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

Further on the selected conformity assessment body is made aware that it is obligated to report a condition or the conditions to the Danish Agency for Digital Government if the conformity assessment body continues to believe significant weaknesses or irregularities are occurring. In addition, the conformity assessment body is made aware that upon inquiry by the Danish Agency for Digital Government it is obligated to give information on the TSP’s circumstances that have or may have an influence on the TSP’s administration of its task as the issuer of OCES certificates, without prior acceptance by the TSP. The conformity assessment body is, however, obligated to inform the TSP on the inquiry.

In case the TSP chooses to change conformity assessment body, the Danish supervisory body is informed.

8.3. Assessor’s relationship to assessed entity

The external conformity assessment body and the internal audit shall cooperate.

8.4. Topics covered by assessment

The conformity assessment body is granted access to all management meeting protocols on request. The conformity assessment body can participate in management meetings during processing of matters that are of significance to the system audit.

Den Danske Stat does not have annual general assemblies.

The Trust Service 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

Any irregularities reported by Conformity Assessment Body will be on the agenda at the next Den Danske Stat management meeting.

8.6. Communication of results

Den Danske Stat management will inform the Supervisory Authority operated by the Agency for Digital Government about conditions which might affect the continued service.
A Conformity Assessment Body is conducting an annual audit and delivers a Conformity Assessment Report to Den Danske Stat management.

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

9. Other business and legal matters

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

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

Consult [GRPS] clause 7.1.1 for general considerations on Organization reliability.

9.2.1. Insurance coverage

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

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

9.2.3. Insurance or warranty coverage for end-entities

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

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

Consult [GRPS] clause 7.13 for general considerations on Compliance. A Data Processing Impact Assessment (DPIA) and risk assessments are maintained to ensure that personal data is protected at an adequate level.

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

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

9.4.5. Notice and consent to use private information

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

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

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

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

9.9. Indemnities

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

9.10. Term and termination

9.10.1. Term

The TSP provides a PKI disclosure statement, [PDS], at the TSP repository. The statement follows the structure outlined in [ETSI EN 319 411-1].

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

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 procedures

Consult [GRPS] clause 7.1.1 for general considerations on Organization reliability and clause 6.2 for general considerations on Terms and Conditions.

9.14. Governing law

Den Danske Stats' dispute procedures ultimately state that a dispute can be solved in a Danish court.

9.15. Compliance with applicable law

Consult [GRPS] clause 7.13 for general considerations on Compliance.

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

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

9.17.1. Disabilities

Consult [GRPS] clause 7.13 for general considerations on Compliance.

9.17.2. Organizational

Consult [GRPS] clause 7.1 for general considerations on Internal organization.

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

9.17.3. Additional testing

Den Danske Stat provides a test environment for third parties to check and test all the certificate types issued by the TSP. The production environment is not used for issuance of test certificates.

References

Term	Reference
[CP]	Common Public Certificate Policy for OCES and Qualified Certificates, Agency for Digital Government, version 8, 2026. https://certifikat.gov.dk/
[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 with amendments specified in REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
[GRPS]	Den Danske Stat, Practice Statement on General Security Requirements for Trust Service Providers, Agency for Digital Government, version 1.0, https://ca1.gov.dk/
[Profile]	Den Danske Stat, Certificate Profile, Agency for Digital Government, https://ca1.gov.dk/
[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
[T&C]	Den Danske Stat, Terms and Conditions, Agency for Digital Government. https://ca1.gov.dk/
[ETSI TS 119 461]	ETSI TS 119 461, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects, ETSI ESI, Version 2.1.1, February 2025. https://www.etsi.org/standards
[NSIS]	National Standard for Identiteters Sikringsniveauer (NSIS), Agency for Digital Government, version 2.1, June 2024. https://digst.dk/nsis/
[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 1.5.1, April 2025. https://www.etsi.org/standards
[ETSI TS 119 431-1]	ETSI TS 119 431-1, Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev, ETSI ESI, Version 1.3.1, December 2024. https://www.etsi.org/standards
[rQSCD PS]	Den Danske Stat, Management of remote QSCD Practice Statement, Agency for Digital Government, Version: 1.0. https://ca1.gov.dk/
[Revocation Procedures]	Den Danske Stat, Revocation Procedures, are described at: https://www.ca1.gov.dk/spaerringsprocedure/
[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

Term	Reference
[BCP]	Den Danske Stat, 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.
[FIPS 140-2]	FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, National Institute of Standards and Technology (NIST), USA, May 2001
[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**
[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 2.4.1, June 2025. **https://www.etsi.org/standards**
[ETSI TS 119 312]	ETSI TS 119 312, Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, ETSI ESI, Version 1.5.1, December 2024. **https://www.etsi.org/standards**
[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**
[PDS]	Den Danske Stat, PKI Disclosure Statement. **https://ca1.gov.dk/**