# IN GROUPE DENMARK PS

# Advanced Certification Practice Statement (ACPS)

| Document information | | | |
|---|---|---|---|
| No. of pages :<br>49 | Reference :<br>N/A | Department :<br>eID Development | Classification :<br>Public |
| Valid from:<br>31/08/2025 | | | Version:<br>1.0.0 |

| Version history | | | |
|---|---|---|---|
| **Version** | **Date** | **Author** | **Description of update<br>Updated paragraphs** |
| 1.0 | 15/07/2025 00:00 | KJAERGAARD Jan | Initial version |
| | Cliquez ou appuyez ici pour entrer une date. | | |
| | Cliquez ou appuyez ici pour entrer une date. | | |
| | Cliquez ou appuyez ici pour entrer une date. | | |
| | Cliquez ou appuyez ici pour entrer une date. | | |

# CONTENTS

# 1 INTRODUCTION

## 1.1 Overview

IN Groupe Denmark A/S has established a trust service provider, which provides trust services, that meet the requirements in the eIDAS regulation [eIDAS]. The services include:

- Certificate service for issuance of qualified and advanced certificates.
- Management of remote qualified signature creation devices
- Qualified timestamping service

The services offer private and public organizations within the EU Internal Marked the necessary trust service infrastructure to create advanced and qualified electronic signatures.

While the eIDAS regulation [eIDAS] supports trust services for management of remote qualified electronic signature creation devices, the current standard for Trusted List [TL] does not yet support all types of trust services and as such, the management of remote qualified electronic creation devices is notified to the Danish Supervisory Body as part of the certification services.

The practice statements are organized as follow:

- TSP Practice Statement (TSP PS)
  describes how the general security requirements for a TSPs are met.
- Certification Practice Statement (CPS)
  describes how specific requirements concerning being Certification Authority issuing qualified certificates are met.
  This document references TSP PS when suitable.
- Advanced Certification Practice Statement (ACPS) - this document
  describes how specific requirements concerning being a Certification Authority issuing advanced certificates are met.
  This document references TSP PS when suitable.
- Remote Qualified Signature Creation Device Practice Statement (rQSCD PS)
  describes how specific requirement for management of remote qualified signature creation device are met.
  The document references TSP PS when suitable.
- Time stamp Authority Practice Statement (TSA PS)
  describes how specific requirement concerning being a Time Stamp Authority are met.
  The document references TSP PS when suitable.

This ACPS cover the certificate policy defined by NCP+ in [EN 319 411-1].

## 1.2 Document name and identification

This document is named as In Groupe Denmark ACPS and is associated with a version number in the form x.y, with x being the major number and y a sub number.

## 1.3 PKI participants

The PKI participants of the of the TSP consist of the entities which provides a role in providing the overall services as well as entities consuming the services, i.e. relying parties or end user subjects.

- Certification authorities
- Registration Services
- Subjects
- Relying parties
- Other parties:
  - Certificate Revocation Status Service
  - Repository Service
  - Time Stamp Service
  - Remote QSCD Services

### 1.3.1 Certification authorities

The TSP Certification Authority has established a key hierarchy for issuance of certificates for its services and for subjects.

- Root Certificate
  - Qualified Issuing CA
    - Qualified Subject Certificates for natural person
    - Qualified OCSP responder Certificate
  - Qualified TimeStamping Unit
  - CRL.
  - Advanced Issuing CA
    - Advanced Subject Certificates for natural person
    - Advanced OCSP responder Certificate

The Root Certificate is a self-signed certificate constituting the top of the key hierarchy. It is used for issuing intermediate certificates for the TSP and other services. In addition, it is used to issue the certificate for the QTSP Qualified TimeStamping Unit. The Root Certificate is also used to issue CRL covering revocation status information of the issued certificates.

The Qualified Issuing CA is used to issue qualified subject certificates for natural persons. It is also used to issue certificates for an OCSP Responder (Qualified OCSP responder Certificate) providing revocation status information on subject certificates. The Qualified Issuing CA appears on the EU Trust List.

The qualified certificates for natural person are issued to subjects for use with the Remote QSCD Services.

The Advanced Issuing CA is used to issue advanced subject certificates for natural persons. It is also used to issue certificates for an OCSP Responder (Advanced OCSP responder Certificate) providing revocation

status information on subject certificates. The Advanced Issuing CA appears on the EU Trust List as a non-qualified trust service.

The advanced certificates for natural person are issued to subjects for use with the Remote QSCD Services.

### 1.3.2 Registration authorities

The TSP relies on external entities for subject registration for issuance of an advanced certificate. The entity performing the registration can be one of:

(a) A notified electronic identification means which meets the requirements in the regulation [eIDAS], Article 8 with assurance level substantial or high.
(b) By using other identification methods which ensure the identification of the person with a substantial or high level of confidence, the conformity of which shall be confirmed by a conformity assessment body or an authorised system auditor.

Before allowing a notified electronic identification scheme to be used by the TSP, the TSP checks in Official Journal of the European Union, on whether the scheme is notified and that the level of assurance is substantial or high[1].

Before allowing other identification methods, the TSP checks the conformity assessment report issued by a conformity assessment body. The report shall indicate that the subject has been identity verified with level of confidence at least substantial.

### 1.3.3 Subscribers

Subscribers are natural persons who receives an advanced certificate in a signature session flow. The subscriber is identified by a Registration Authority and has accepted the TSPs Term and Conditions prior the issuance of the certificate.

Since the TSP only issue certificates to natural persons, subscriber and subject is the same entity in this document and the terms are used interchangeably.

### 1.3.4 Relying parties

The certificates issued by the TSP is used for creation of advanced electronic signatures. The relying parties are natural and legal persons, that relies on these signatures. Therefor the relying parties shall ensure that the signing certificate content is as stated in [Profile] and that the certificate was valid at the time the signature was created.

[1] For instance, it can be checked that the Danish eID scheme MitID is notified with assurance level substantial and high in e.g.: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202405468&qid=1731325587133

## 1.3.5 Other participants

### 1.3.5.1 Signing service

The signing service is used by relying parties to have subjects sign specific documents. It relies on Registration Authorities for subject identification and uses received subject attributes to create a subject key pair on the remote QSCD service and have a certification request generated containing relevant subject attributes. The certification request is submitted to the CA for issuance of a certificate and upon receival of a certificate, it is submitted to the remote signing service. The signing service activates the signature key on the remote QSCD service creating a raw signature value, which the signing service inserts into the document. Based on the signature type, the signing service adds additional data to the document. Upon completion of the signature, the subject key pair is destroyed by the remote QSCD service.

The high-level steps through a signature flow are:

- 
- The relying party uploads a document for signing and signature type (B, T, LT or LTA) to the signing service and receives a signature session identifier from the signing service.
- The relying part redirects the subject to the signature service using the signature session identifier.
- The subject is presented with the document for signing by the signing service. The user reads the document and the TSP terms and conditions, which are to be accepted.
- The user is authenticated by the Registration Authority and proceeds to sign the document.
- The signing service verifies the origin integrity of the subject attributes received from the Registration Authorities and
    - Creates a key pair for the subject using the remote QSCD service.
    - Creates a certification request using the remote QSCD service which provides proof of possession of the private key by the remote QSCD service.
    - The certification request is submitted by the signing service to the CA for certificate issuance.
    - The CA verifies the certification request is submitted by the signature service and checks relevant attributes before a certificate is issued and returned to the signing service.
    - The signing service returns the certificate to the remote QSCD service and request the remote QSCD service to create a raw signature. The signature is added to the signed document.
    - The signing service forms the signature type by reaching out to the TSA to gather time stamp tokens.
    - The subject is presented with the option to download the signed document, and the relying party is informed that the document has been signed.
    - The signing service requests the remote QSCD to destroy the subject's key pair.
- The relying part fetches the signed document.

### 1.3.5.2 Certificate Revocation Status Service

Subject certificates are issued for a certificate session have a short validity. Since certificates are issued after a subject verification or electronic identification and only used to create advanced electronic signatures

during a signature session, these certificates cannot be revoked. Revocation status information is however made available as an OCSP service.

#### 1.3.5.3 Repository Service

The TSP provides a repository where all versions of practice statements, profiles and terms and conditions can be found.

#### 1.3.5.4 Remote QSCD Service

Subject key pairs are generated, activated and destroyed using a remote QSCD Service.

## 1.4 Certificate usage

### 1.4.1 Appropriate certificate uses

Subject certificates issued by the TSP can be used for advanced electronic signatures.

### 1.4.2 Prohibited certificate uses

The subject certificates can only be used for the cases described in section 1.4.1. In particular, subject certificates can-not be used to issue sub-ordinate certificates.

## 1.5 Policy administration

### 1.5.1 Organization administering the document

This document is administered by IN Groupe Denmark A/S.

### 1.5.2 Contact person

The contact person is Head of Security, Risk & Compliance.

### 1.5.3 Person determining CPS suitability for the policy

The Head of Security, Risk & Compliance determines if the ACPS is suitable for the chosen policy.

#### 1.5.3.1 General considerations on Certification Practice

This ACPS meets the requirements in the policy NCP+ from [EN 319 411-1]. As such  al requirements in the policies NCP+ and NCP from [EN 319 411-1] are implemented.

The ACPS follows the structure described in [RFC 3647].

The ACPS is accompanied by a profile [Advanced] document specifying the format details of certificates and OCSP. This includes signature algorithms.

### 1.5.4 CPS approval procedures

See [TSP PS] concerning detail on practice statement approval procedures.

## 1.6 Definitions and acronyms

| Term | Definition |
|---|---|
| Activation data | Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share). |
| Authentication | The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual CA-certificate or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender. |
| CA-certificate | A certificate for one CA's public key issued by another CA. |
| Certificate policy (CP) | A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. |
| Certification path | An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path. |
| Certification Practice Statement (CPS) | A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. |

| Term | Definition |
|---|---|
| Identification | The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes:<br>(1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and<br>(2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems |
| Issuing certification authority (issuing CA) | In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority). |
| Participant | An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity. |
| PKI Disclosure Statement (PDS) | An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS. |
| Policy qualifier | Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information. |
| Registration authority (RA) | An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.] |

| Term | Definition |
|---|---|
| Relying party | A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably. |
| Relying party agreement (RPA) | An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates. |
| Set of provisions | A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a CP or CPS employing the approach described in this framework. |
| Subject certification authority (subject CA) | In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority). |
| Subscriber | A subject of a certificate who is issued a certificate. |
| Subscriber Agreement | An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates. |
| Validation | The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants. |

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

See [TSP PS] concerning repositories.

This Advanced Certification Practice Statements is published at the repository together with PKI Disclosure agreement and terms and conditions.

## 2.2 Publication of certification information

CA certificates are available on the repository and on the List of Trusted List.

Subject certificates are not published as the key usage does not require that.

## 2.3 Time or frequency of publication

The documents in the repository are published after approval.

## 2.4 Access controls on repositories

The repository is made available on the web site without any restrictions. Cyber security events may impose geographical restrictions.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### 3.1.1 Types of names

The TSP issues subject certificates with the following name attributes:

- Country name
- Common name
- Given name
- Sur name
- Pseudonym
- Serial number

See [Advanced] for details on conditions for when the subject name attributes are used.

### 3.1.2 Need for names to be meaningful

The TSP receives names from the Registration Authorities, who has ensured that the names are meaningful by looking into e.g. official documents, authoritative sources etc.

### 3.1.3 Anonymity or pseudonymity of subscribers

The Registration Authorities provides information to the TSP if the subject shall be anonymized and pseudonym used. If this is the case Common name, Given name, Sur name are not used and Pseudonym will take the value *Pseudonym*.

See [Advanced] for details on subject attributes.

### 3.1.4 Rules for interpreting various name forms

The are no policy requirements for interpreting various name forms.

### 3.1.5 Uniqueness of names

The subject serial number, provided by the Registration Authorities, is used to ensure that the entire subject Name object is unique and only assigned to one subject.

### 3.1.6 Recognition, authentication, and role of trademarks

The TSP has defined trademarks.

For subjects and trademarks held as part of their names, it is the responsibility of the subject during registration at the Registration Authority to ensure that any trademarks are properly registered. The TSP will use name attributes as received from the Registration Authorities.

## 3.2 Initial identity validation

### 3.2.1 Method to prove possession of private key

Root certificates, CA certificates and TSA certificates are created using approved key signing ceremony scripts, which ensures that private keys are controlled by the TSP. The scripts ensures that certificate requests are created with correct content.

For subject certificates, once a subject has been verified by the Registration Authorities, the TSP uses a QSCD managed by the TSP to generate a subject key pair and creates a certification request which is signed by the subject private key to provide proof of possession.

### 3.2.2 Authentication of organization identity

N/A. The TSP does not issue subject certificates to legal persons or natural persons associated with a legal person.

### 3.2.3 Authentication of individual identity

Subject identification is carried out by Registration Authorities. See section 1.3.2.

### 3.2.4 Non-verified subscriber information

Non-verified subject information is not used.

### 3.2.5 Validation of authority

N/A.

### 3.2.6 Criteria for interoperation

N/A.

## 3.3 Identification and authentication for re-key requests

The TSP does not support re-key for an issued certificate.

### 3.3.1 Identification and authentication for routine re-key

N/A.

### 3.3.2 Identification and authentication for re-key after revocation

N/A.

## 3.4 Identification and authentication for revocation request

The TSP issues short term certificates, which can-not be revoked.

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## 4.1 Certificate Application

The TSP issues certificates as part of a signature flow based on subject attributes received from the Registration Authority. Since the attributes are used within a few seconds to issue a certificate, the received attributes are considered correct at the time of certificate issuance.

The TSP only supports certificate issuance based on fresh information received from the Registration Authorities during a signature session. Information received during one session are not used for sub-sequent sessions.

Subject key pairs are generated by the remote QSCD service operated by the TSP.

### 4.1.1 Who can submit a certificate application

The TSP issues certificates to subjects, who has been passed the processes provided by the Registration Authorities connected to the TSP and who has accepted the TSP terms and conditions.

### 4.1.2 Enrolment process and responsibilities

See section 1.3.5.1 for the steps carried out by the TSP during subject enrolment.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

The certificate application is created by the TSP after receival of subject attributes from the Registration Authorities. The Registration Authorities are responsible for subject identification and authentication.

### 4.2.2 Approval or rejection of certificate applications

The TSP creates a certificate application after it has received subject information from the Registration Authorities.

Before the certificate application is created, the TSP conducts the following actions:

a) The TSP checks that the information received from the Registration Authority is from a registered Registration Authority.
b) The TSP checks that the information received from the Registration Authority is not altered during transmission.
c) The TSP checks that the information received from the Registration Authority is bound to a specific session.
d) The received information is issued within a few minutes from the current TSP time.
e) The received information has the expected level of assurance, at least substantial.
f) The received information contains the relevant subject attributes to form all subject attributes as required by the certificate profile.

In case any of the above actions is not completed successfully, a certificate application is not created.

### 4.2.3 Time to process certificate applications

A certificate application is processed within a few seconds.

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

Once TSP has received information on the subject identity from the Registration Authorities, see section 4.2.2, the TSP

- uses a QSCD operated by the TSP to generate a subject key pair.
- creates a certification request with subject attributes received from the Registration Authority and signs it with the subject private key.
- issues the subject certificate and signs it with the relevant CAs private key.

- stores the certificate at the QSCD operated by the TSP.

The TSP software and hardware are deployed in a secure environment, and it is only the software which can trigger the above steps.

The subject serial number is randomly generated by the TSP software.

The TSP uses a QSCD is conformant to [EN 419 241-1] using a cryptographic module conformant to [EN 419 221-5] which ensures that the subject's key pair are protected in confidentially. The subject private keys remain in the cryptographic module and are never transported to other devices.

The validity of subject certificates is counted in minutes, see [Advanced] for details, and a new issuing CA is created well in advance to CA certificate expiry to ensure that subject certificates are not issued with a validity beyond the CA certificate.

The TSP checks that the subject identification carried out by the Registration Authority matches the level of assurance required for issuing the requested type of certificate. For advanced certificates, the level of assurance must be at least substantial. The [Advanced] document describes the profile of the issued certificate, including the certificate policy.

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

The subject is notified during the signature flow, that the signature has been created and implicitly that a certificate has been issued.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

The TSPs terms and conditions [T&C] includes subject obligations as part of certificate issuance. The subject will be prompted to accept the terms and conditions every time a certificate is issued. The TSP records which version of the terms and conditions the subject has accepted and maintains this during the period stated in the terms and conditions.

The terms and conditions are available at the Repository and made available for the subject during certificate issuance. In both cases, the transfer of the terms and conditions from the TSP to the subject is protected by TLS, which in particular ensures the integrity of the terms and conditions.

### 4.4.2 Publication of the certificate by the CA

The TSP does not publish subject certificates.

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

The TSP does not notify other entities of issued certificates.

## 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage

The terms and conditions, [T&C], describes obligations for the subject. As subject private keys are managed by the TSP and can only be used for signature generation, the subject is asked to pay special attention to the registration conducted at the Registration Authority and to ensure that authentication means are protected.

Subject private keys are managed by the TSP on behalf of the subject. The TSP has established systems, procedures and protocols, to ensure that the subject is always in sole control of the private keys. The TSP operates the remote QSCD in conformance with [TS 119 431-1].

### 4.5.2 Relying party public key and certificate usage

The terms and conditions, [T&C], describes obligations for the relying parties, who are instructed to validate the advanced signature before it is trusted.

## 4.6 Certificate renewal

The TSP does not support certificate renewal.

### 4.6.1 Circumstance for certificate renewal

N/A.

### 4.6.2 Who may request renewal

N/A.

### 4.6.3 Processing certificate renewal requests

N/A.

### 4.6.4 Notification of new certificate issuance to subscriber

N/A.

### 4.6.5 Conduct constituting acceptance of a renewal certificate

N/A.

### 4.6.6 Publication of the renewal certificate by the CA

N/A.

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

N/A.

## 4.7 Certificate re-key

The TSP does not support certificate re-key.

### 4.7.1 Circumstance for certificate re-key

N/A.

### 4.7.2 Who may request certification of a new public key

N/A.

### 4.7.3 Processing certificate re-keying requests

N/A.

### 4.7.4 Notification of new certificate issuance to subscriber

N/A.

### 4.7.5 Conduct constituting acceptance of a re-keyed certificate

N/A.

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

N/A.

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

N/A.

## 4.8 Certificate modification

The TSP does not support certificate modification.

### 4.8.1 Circumstance for certificate modification

N/A.

### 4.8.2 Who may request certificate modification

N/A.

### 4.8.3 Processing certificate modification requests

N/A.

### 4.8.4 Notification of new certificate issuance to subscriber

N/A.

### 4.8.5 Conduct constituting acceptance of modified certificate

N/A.

### 4.8.6 Publication of the modified certificate by the CA

N/A.

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

N/A.

## 4.9 Certificate revocation and suspension

The TSP only issues short-term certificates with a validity as specified in [Advanced]. They are created, used and destroyed as part of one signing session. The certificates cannot be revoked or suspended.

The certificates are issued on the current ACPS at the time of issuance.

In case the TSP notifies any problems during certificate issuing, this will be audit logged by the TSP audit system.

In case the TSP wants to provide information in relation to problems with non-revocable certificates, this is provided using the TSP Repository. Subjects may use the TSP contact information to request information from the TSP related to the noticed problems.

### 4.9.1 Circumstances for revocation

N/A.

### 4.9.2 Who can request revocation

N/A.

### 4.9.3 Procedure for revocation request

N/A.

### 4.9.4 Revocation request grace period

N/A.

### 4.9.5 Time within which CA must process the revocation request

N/A.

### 4.9.6 Revocation checking requirement for relying parties

N/A.

### 4.9.7 CRL issuance frequency (if applicable)

N/A.

### 4.9.8 Maximum latency for CRLs (if applicable)

N/A.

### 4.9.9 On-line revocation/status checking availability

N/A.

### 4.9.10 On-line revocation checking requirements

N/A.

### 4.9.11 Other forms of revocation advertisements available

N/A.

### 4.9.12 Special requirements re key compromise

N/A.

### 4.9.13 Circumstances for suspension

N/A.

### 4.9.14 Who can request suspension

N/A.

### 4.9.15 Procedure for suspension request

N/A.

### 4.9.16 Limits on suspension period

N/A.

## 4.10 Certificate status services

### 4.10.1 Operational characteristics

The TSP provides certificate revocation status information for subject certificates through OCSP. As subject certificates cannot be revoked, the service is only provided for relying parties, which has a need to obtain revocation status.

OCSP responses are signed by the private key for the OCSP Responder certificate to ensure the revocation status information is protected in integrity. The OCSP Responder certificate provides assurance of origin from the TSP.

The OCSP Responder provides status information for CA certificates managed by the TSP and answer with status code ‘Good’ even if the certificate is expired.

For non-issued certificates the OCSP Responder follows [RFC6960] and responds with ‘revoked’.

The OCSP Responder url is publicly available on the internet. Cyber security events may impose geographical restrictions.

OCSP responses, see [Advanced], include the extension ArchiveCutOff set to the time and date from issuing CA notBefore.

For Certification Authority certificate revocation status information is provided through CRL.

### 4.10.2 Service availability

The TSP revocation status information is available 24/7 at the url for OSCP and CRL specified in [Advanced].

### 4.10.3 Optional features

N/A.

## 4.11 End of subscription

N/A.

## 4.12 Key escrow and recovery

### 4.12.1 Key escrow and recovery policy and practices

The TSP does not use key escrow or perform backup of subject private keys. It is not needed as the TSP only issues short-term signature

### 4.12.2 Session key encapsulation and recovery policy and practices

N/A.

# 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

## 5.1 General

See [TSP PS] section 5, 6.3 and 7.3.

## 5.2 Physical controls

### 5.2.1 Site location and construction

See [TSP PS] section 7.6.

### 5.2.2 Physical access

See [TSP PS] section 7.6.

### 5.2.3 Power and air conditioning

See [TSP PS] section 7.6.

### 5.2.4 Water exposures

See [TSP PS] section 7.6.

### 5.2.5 Fire prevention and protection

See [TSP PS] section 7.6.

### 5.2.6 Media storage

See [TSP PS] section 7.3.

### 5.2.7 Waste disposal

See [TSP PS]

### 5.2.8 Off-site backup

See [TSP PS]

## 5.3 Procedural controls

### 5.3.1 Trusted roles

See [TSP PS] section 7.4.

### 5.3.2 Number of persons required per task

See [TSP PS] section 7.4.

### 5.3.3 Identification and authentication for each role

See [TSP PS] section 7.4.

### 5.3.4 Roles requiring separation of duties

See [TSP PS] section 7.4.

## 5.4 Personnel controls

### 5.4.1 Qualifications, experience, and clearance requirements

See [TSP PS] section 7.2.

### 5.4.2 Background check procedures

See [TSP PS] section 7.2.

### 5.4.3 Training requirements

See [TSP PS] section 7.2.

### 5.4.4 Retraining frequency and requirements

See [TSP PS] section 7.2.

### 5.4.5 Job rotation frequency and sequence

See [TSP PS] section 7.2.

### 5.4.6 Sanctions for unauthorized actions

See [TSP PS] section 7.2.

### 5.4.7 Independent contractor requirements

See [TSP PS] section 7.2.

### 5.4.8 Documentation supplied to personnel

See [TSP PS] section 7.2.

## 5.5 Audit logging procedures

### 5.5.1 Types of events recorded

See [TSP PS] section 7.10.

### 5.5.2 Frequency of processing log

See [TSP PS] section 7.10.

### 5.5.3 Retention period for audit log

See [TSP PS] section 7.10.

### 5.5.4 Protection of audit log

See [TSP PS] section 7.10.

### 5.5.5 Audit log backup procedures

See [TSP PS] section 7.10.

### 5.5.6 Audit collection system (internal vs. external)

See [TSP PS] section 7.10.

### 5.5.7 Notification to event-causing subject

See [TSP PS] section 7.10.

### 5.5.8 Vulnerability assessments

See [TSP PS] section 7.10.

## 5.6 Records archival

See [TSP PS] section 7.10.

### 5.6.1 Types of records archived

See [TSP PS] section 7.10.

### 5.6.2 Retention period for archive

See [TSP PS] section 7.10.

### 5.6.3 Protection of archive

See [TSP PS] section 7.10.

### 5.6.4 Archive backup procedures

See [TSP PS] section 7.10.

### 5.6.5 Requirements for time-stamping of records

See [TSP PS] section 7.10.

### 5.6.6 Archive collection system (internal or external)

See [TSP PS] section 7.10.

### 5.6.7 Procedures to obtain and verify archive information

See [TSP PS] section 7.10.

## 5.7 Key changeover

The TSP creates new issuing CA with a different subject name and subject public key well in advance of expiry of the existing CA. The creation of the new issuing CA will follow the similar procedures as the existing CA. It will be provided to the TSPs supervisory body for the certificate to be added to the list of trusted lists.

## 5.8 Compromise and disaster recovery

See [TSP PS] section 7.11 for general considerations of compromise and disaster recovery.

In case the TSP identifies compromise, loss or suspected compromise of CA private key, the TSP will revoke the CA certificate and inform the supervisory body of the action and request for the service to be withdrawn from the list of trusted lists. To recover, the TSP will create a new CA with updated common name, see section 6.1.1 and have that to appear on list of trusted lists.

In case the TSP identifies that cryptographic algorithms, or associated parameters used by the TSP for providing CA issuance and revocation status information becomes insufficient for the remaining intended usage period, the TSP will establish a key update of the relevant certificates, see section 6.1.1.

### 5.8.1 Incident and compromise handling procedures

N/A.

### 5.8.2 Computing resources, software, and/or data are corrupted

N/A.

### 5.8.3 Entity private key compromise procedures

N/A.

### 5.8.4 Business continuity capabilities after a disaster

N/A.

## 5.9 CA or RA termination

See [TSP PS] section 7.12.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Key pair generation and installation

### 6.1.1 Key pair generation

See [TSP PS] on how the TSP manage CA cryptographic keys.

For subject key generation the TSP uses a Remote Qualified Signature Creation Device (rQSCD). The rQSCD is compliant with [EN 419 241-2] using a cryptographic module compliant with [EN 419 221-5]. The rQSCD is operated according to [EN 419 241-1] and [TS 119 431-1].

The rQSCD and cryptographic modules are deployed to the TSP protected environment and configured under supervised procedures.

The [Advanced] specifies the key type and cryptographic strength for subject key pair, which is aligned with [TS 119 312].

Subject private keys are generated in a protected environment using a cryptographic module, which ensure they are protected in integrity and confidentiality. The use of approved algorithms ensures the keys are resistant to cryptographic attacks during the life-time of the subject certificate. The private keys never leave the protected environment.

The generation of subject keys takes place during a signature session, when the TSP has received information on the subject from the RA. During the generation, the subject is linked to the key pair.

Once the signature session is completed, the TSP uses the cryptographic module to delete the subject key pair.

The TSP has procedures in place to monitor the certification status of the rQSCD. In case the rQSCD unexpectedly loses the certification status, the TSP will inform its conformity assessment body and supervisory body with a plan on its intension to replace the rQSCD.

The TSP has procedures in place for generation of all CA keys. The generation of CA key pairs is connected to the issuance of the public key certificate and takes place in a physically secured environment and carried out by trusted roles under dual control. For all activities related to key signing ceremony, the number of participants is kept to a minimum following the approved procedures.

The procedures describe the roles, functions and responsibilities and required evidence to be collected. As part of the key signing ceremony a report is produced to prove the ceremony was carried out as stated in the procedure. The report is signed by the trusted role responsible for the security of key signing ceremony and where applicable by an independent witness.

All keys generated by the TSP are carried out using cryptographic algorithms and strength as recommended by [TS 119 312].

The TSP creates a new CA before any active CA certificate expires. In [Advanced] the common name of issuing certificates indicates with a number, starting with roman letter I, the version of the CA. Whenever a new CA is created, the number in the common name will be incremented, and the new certificate will be provided for List of Trusted List. The update will take place timely enough for the supervisory body to approve the new certificate.

### 6.1.2 Private key delivery to subscriber

N/A. The TSP does not deliver private keys to subscribers.

### 6.1.3 Public key delivery to certificate issuer

The TSP generates subject public keys and ensures they are provided to the CA issuing system using secure protocols.

### 6.1.4 CA public key delivery to relying parties

The TSP CA public key is made available for relying parties through the list of trusted lists. In addition, it can be found on the TSPs repository.

### 6.1.5 Key sizes

See 6.1.6 below.

### 6.1.6 Public key parameters generation and quality checking

The subject public key sizes and where applicable for elliptic curve keys domain parameters are described in[Advanced].

### 6.1.7 Key usage purposes (as per X. v key usage field)

The key usage as specified in the certificate extension are described in [Advanced].

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

See section 6.1 for details on private key protection and cryptographic module engineering controls.

### 6.2.1 Cryptographic module standards and controls

N/A.

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

N/A.

### 6.2.3 Private key escrow

N/A.

### 6.2.4 Private key backup

N/A.

### 6.2.5 Private key archival

N/A.

### 6.2.6 Private key transfer into or from a cryptographic module

N/A.

### 6.2.7 Private key storage on cryptographic module

N/A.

### 6.2.8 Method of activating private key

N/A.

### 6.2.9 Method of deactivating private key

N/A.

### 6.2.10 Method of destroying private key

N/A.

### 6.2.11 Cryptographic Module Rating

N/A.

## 6.3 Other aspects of key pair management

See section 6.1 for details on other aspects of key pair management.

### 6.3.1 Public key archival

N/A

### 6.3.2 Certificate operational periods and key pair usage periods

N/A.

## 6.4 Activation data

See section 6.1 for details on activation data.

### 6.4.1 Activation data generation and installation

N/A.

### 6.4.2 Activation data protection

N/A.

### 6.4.3 Other aspects of activation data

N/A.

## 6.5 Computer security controls

See [TSP PS] on section 7.4 and 7.8.

### 6.5.1 Specific computer security technical requirements

N/A.

### 6.5.2 Computer security rating

N/A.

## 6.6 Life cycle technical controls

See [TSP PS] section 7.7.

### 6.6.1 System development controls

N/A.

### 6.6.2 Security management controls

N/A.

### 6.6.3 Life cycle security controls

N/A.

## 6.7 Network security controls

See [TSP PS] section 7.8 for network security controls and [TSP PS] section 7.4 for access controls.

## 6.8 Time-stamping

The TSP has published a practice statement document on its time stamp authority [TSA PS].

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificate profile

The certificate profiles, [Advanced], for subject certificates are created to meet the requirements specified in [RFC5280], [EN 319 411-1]. Certificates are always issued to natural persons with the private key on a QSCD managed by the TSP.

### 7.1.1 Version number(s)

All subject certificates have version v3 (with value 2).

### 7.1.2 Certificate extensions

The following certificate extensions are included in the subject certificates:

- authorityInfoAccess
- authorityKeyIdentifier
- BasicConstraints
- CertificatePolicies
- KeyUsage
- subjectKeyIdentifier

- Validity Assured Certificate

### 7.1.3 Algorithm object identifiers

See [Advanced] for used algorithm identifiers.

### 7.1.4 Name forms

See [Advanced] for certificate subject name.

### 7.1.5 Name constraints

N/A.

### 7.1.6 Certificate policy object identifier

The issued subject certificates meet the policy requirements for NCP+. The identifier for NCP+ is included in the certificates.

### 7.1.7 Usage of Policy Constraints extension

N/A. The extension is not supported.

### 7.1.8 Policy qualifiers syntax and semantics

N/A.

### 7.1.9 Processing semantics for the critical Certificate Policies extension

N/A. No policy requirements.

## 7.2 CRL profile

N/A. The TSP uses OCSP for subject certificates.

### 7.2.1 Version number(s)

N/A.

### 7.2.2 CRL and CRL entry extensions

N/A.

## 7.3 OCSP profile

The OCSP Responder profiles, [Profiles], providing status for subject certificates meets the requirements in [RFC6960].

The OCSP Responder certificates include the certificate extension OCSPnoCheck. The AuthorityInfoAccess extension of the OCSP Responder certificate does not include id-ad-ocsp.

The OCSP Responder responds with the status 'revoked' for certificates which are not (yet) issued by the CA.

The TSP has monitoring on exposed endpoints for detection of potential attacks.

### 7.3.1 Version number(s)

See [Profiles].

### 7.3.2 OCSP extensions

See [Profiles].

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The TSP and its qualified trust service are conformity assessed for compliance with the [eIDAS], the relevant standards and the practices described in [TSP PS] and [TSP CPS].

The provision of the service for issuing advanced certificates uses the same management and organisation as for the qualified service. The service is not assessed by a conformity assessment body.

## 8.1 Frequency or circumstances of assessment

N/A.

## 8.2 Identity/qualifications of assessor

N/A.

## 8.3 Assessor's relationship to assessed entity

N/A.

## 8.4 Topics covered by assessment

N/A.

## 8.5 Actions taken as a result of deficiency

N/A.

## 8.6 Communication of results

N/A.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

The used certificate policy does not pose any requirements on fees.

### 9.1.1 Certificate issuance or renewal fees

N/A

### 9.1.2 Certificate access fees

N/A

### 9.1.3 Revocation or status information access fees

N/A

### 9.1.4 Fees for other services

N/A

### 9.1.5 Refund policy

N/A

## 9.2 Financial responsibility

See [TSP PS] section 7.1.1 for details concerning financial responsibility.

### 9.2.1 Insurance coverage

See [PS] section 7.1.1.

### 9.2.2 Other assets

N/A.

### 9.2.3 Insurance or warranty coverage for end-entities

See [TSP PS] section 7.1.1 for details concerning financial responsibility.

## 9.3 Confidentiality of business information

The used certificate policy does not pose any requirements on confidentiality of business information.

### 9.3.1 Scope of confidential information

N/A.

### 9.3.2 Information not within the scope of confidential information

N/A.

### 9.3.3 Responsibility to protect confidential information

N/A.

## 9.4 Privacy of personal information

See [TSP PS] section 7.13 for considerations on how the TSP handles privacy and personal information.

### 9.4.1 Privacy plan

N/A.

### 9.4.2 Information treated as private

N/A.

### 9.4.3 Information not deemed private

N/A.

### 9.4.4 Responsibility to protect private information

N/A.

### 9.4.5 Notice and consent to use private information

N/A.

### 9.4.6 Disclosure pursuant to judicial or administrative process

N/A.

### 9.4.7 Other information disclosure circumstances

N/A.

## 9.5 Intellectual property rights

The used certificate policy does not pose any requirements on intellectual property rights.

## 9.6 Representations and warranties

The TSP provides its services as described in the practice documents following the identified policies.

The TSPs is liable for these services as described in the PKI Disclosure Statement (PDS).

### 9.6.1 CA representations and warranties

N/A.

### 9.6.2 RA representations and warranties

N/A.

### 9.6.3 Subscriber representations and warranties

N/A.

### 9.6.4 Relying party representations and warranties

N/A.

### 9.6.5 Representations and warranties of other participants

N/A.

## 9.7 Disclaimers of warranties

The used policies do not provide any additional requirements to disclaimers of warranties. The topic is fully covered in section 9.6.

## 9.8 Limitations of liability

See section 9.17.4 for limitations of liability.

## 9.9 Indemnities

The used certificate policy does not pose any requirements on indemnities.

## 9.10 Term and termination

The used certificate policy does not pose any requirements on term and termination.

### 9.10.1 Term

N/A

### 9.10.2 Termination

N/A

### 9.10.3 Effect of termination and survival

N/A

## 9.11 Individual notices and communications with participants

The used certificate policy does not pose any requirements on individual notices and communications with participants.

## 9.12 Amendments

The used certificate policy does not pose any requirements on amendments.

### 9.12.1 Procedure for amendment

N/A

### 9.12.2 Notification mechanism and period

N/A

### 9.12.3 Circumstances under which OID must be changed

N/A

## 9.13 Dispute resolution provisions

In case a dispute between the parties can't be resolved through negotiations, the applicable contract shall determine the court of location. For subjects using the TSP services this is described in the terms and conditions.

## 9.14 Governing law

This TSP is supervised in Denmark and governed by Danish law.

## 9.15 Compliance with applicable law

See [TSP PS] section 7.13.

## 9.16 Miscellaneous provisions

The used policy does not pose any requirements.

### 9.16.1 Entire agreement

N/A.

### 9.16.2 Assignment

N/A.

### 9.16.3 Severability

N/A.

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

N/A.

### 9.16.5 Force Majeure

N/A.

## 9.17 Other provisions

### 9.17.1 Organizational

See [TSP PS] section 7.1.

### 9.17.2 Additional testing

The TSP has established a dedicated test environment for third parties to check and test the certificates issued by the TSP.

### 9.17.3 Disabilities

See [TSP PS] section 7.13.

### 9.17.4 Terms and conditions

See [TSP PS] section 6.2.

# 10 REFERENCES

| References | |
|---|---|
| **Text reference** | **Description** |
| [T&C] | Terms and conditions, https://pki.ingroupe.dk/repository/ |
| [eIDAS] | 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 |
| [Profiles] | Qualified certificate profiles, https://pki.ingroupe.dk/repository/, IN Groupe Denmark A/S |
| [Advanced] | Advanced certificate profiles, https://pki.ingroupe.dk/repository/, IN Groupe Denmark A/S |
| [RFC3647] | IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework". |
| [RFC6960] | IETF RFC 6960: “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP” |
| [EN 319 401] | ETSI EN 319 401: “Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers”. V3.1.1. |
| [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”. V1.4.1. |
| [EN 319 411-2] | ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates". V2.5.1. |
| [EN 419 241-1] | CEN EN 419 241-1, CEN TC224 WG17, Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements. |
| [EN 419 241-2] | CEN EN 419 241-2, CEN TC224 WG17, Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing |
| [EN 419 221-5] | CEN EN 419 221-5, CEN TC224 WG17, Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, 2016. |
| [TS 119 431-1] | ETSI TS 119 431-1: “Policy and security requirements for trust service providers; Part 1: TSP service operating a remote QSCD/SCDev”. V1.3.1. |
| [RFC5280] | Network Working Group RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” |
| [TSP PS] | Trust Service Provider Practice Statement, https://pki.ingroupe.dk/repository/, IN Groupe Denmark A/S |
| [TSP CPS] | Certification Practice Statement, https://pki.ingroupe.dk/repository/, IN Groupe Denmark A/S |
| [TSA PS] | Time Stamp Authority Practice Statement, https://pki.ingroupe.dk/repository/, IN Groupe Denmark A/S |
| [TS 119 312] | ETSI TS 119 312: “Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites”, V1.5.1 |

| | |
|---|---|
| [EN 319 403] | ETSI EN 319 401: “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers”. V2.3.1. |
| [ISO/IEC 17065] | ISO/IEC 17065: "Conformity assessment -- Requirements for bodies certifying products, processes and services. |