

# IN GROUPE DENMARK PS

## Certificate Practice Statement (CPS)

<b>Document information</b>			
<b>No. of pages :</b> 49	<b>Reference :</b> N/A	<b>Department :</b> eID Development	<b>Classification :</b> <b>Public</b>
<b>Creation date :</b> 17/02/2025		<b>Last saved update:</b> February 25	<b>Version:</b> 1.0



# Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## Version history

Version	Date	Author	Description of update Updated paragraphs
1.0	17/02/2025 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.		
	Cliquez ou appuyez ici pour entrer une date.		

## CONTENTS

Contents.....	2
<b>1 INTRODUCTION .....</b>	<b>12</b>
<b>1.1 Overview .....</b>	<b>12</b>
<b>1.2 Document name and identification .....</b>	<b>12</b>
<b>1.3 PKI participants .....</b>	<b>13</b>
1.3.1 Certification authorities .....	13
1.3.2 Registration authorities.....	13
1.3.3 Subscribers .....	14
1.3.4 Relying parties.....	14



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

1.3.5	Other participants .....	14
1.3.5.1	Signing service .....	14
1.3.5.2	Certificate Revocation Status Service .....	15
1.3.5.3	Repository Service .....	15
1.3.5.4	Remote QSCD Service.....	15
<b>1.4</b>	<b>Certificate usage.....</b>	<b>16</b>
1.4.1	Appropriate certificate uses .....	16
1.4.2	Prohibited certificate uses.....	16
<b>1.5</b>	<b>Policy administration .....</b>	<b>16</b>
1.5.1	Organization administering the document.....	16
1.5.2	Contact person .....	16
1.5.3	Person determining CPS suitability for the policy.....	16
1.5.3.1	General considerations on Certification Practice .....	16
1.5.4	CPS approval procedures.....	16
<b>1.6</b>	<b>Definitions and acronyms .....</b>	<b>16</b>
<b>2</b>	<b>PUBLICATION AND REPOSITORY RESPONSIBILITIES.....</b>	<b>19</b>
<b>2.1</b>	<b>Repositories.....</b>	<b>19</b>
<b>2.2</b>	<b>Publication of certification information .....</b>	<b>19</b>
<b>2.3</b>	<b>Time or frequency of publication .....</b>	<b>20</b>
<b>2.4</b>	<b>Access controls on repositories .....</b>	<b>20</b>
<b>3</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>20</b>
<b>3.1</b>	<b>Naming .....</b>	<b>20</b>
3.1.1	Types of names .....	20
3.1.2	Need for names to be meaningful .....	20
3.1.3	Anonymity or pseudonymity of subscribers.....	20
3.1.4	Rules for interpreting various name forms .....	20
3.1.5	Uniqueness of names .....	21
3.1.6	Recognition, authentication, and role of trademarks .....	21
<b>3.2</b>	<b>Initial identity validation .....</b>	<b>21</b>
3.2.1	Method to prove possession of private key .....	21
3.2.2	Authentication of organization identity .....	21
3.2.3	Authentication of individual identity .....	21



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

3.2.4	Non-verified subscriber information .....	21
3.2.5	Validation of authority .....	21
3.2.6	Criteria for interoperation .....	21
<b>3.3</b>	<b>Identification and authentication for re-key requests .....</b>	<b>22</b>
3.3.1	Identification and authentication for routine re-key .....	22
3.3.2	Identification and authentication for re-key after revocation .....	22
<b>3.4</b>	<b>Identification and authentication for revocation request.....</b>	<b>22</b>
<b>4</b>	<b>CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .....</b>	<b>22</b>
<b>4.1</b>	<b>Certificate Application.....</b>	<b>22</b>
4.1.1	Who can submit a certificate application .....	22
4.1.2	Enrolment process and responsibilities.....	23
<b>4.2</b>	<b>Certificate application processing .....</b>	<b>23</b>
4.2.1	Performing identification and authentication functions .....	23
4.2.2	Approval or rejection of certificate applications .....	23
4.2.3	Time to process certificate applications .....	23
<b>4.3</b>	<b>Certificate issuance.....</b>	<b>23</b>
4.3.1	CA actions during certificate issuance .....	23
4.3.2	Notification to subscriber by the CA of issuance of certificate .....	24
<b>4.4</b>	<b>Certificate acceptance.....</b>	<b>24</b>
4.4.1	Conduct constituting certificate acceptance .....	24
4.4.2	Publication of the certificate by the CA .....	24
4.4.3	Notification of certificate issuance by the CA to other entities .....	25
<b>4.5</b>	<b>Key pair and certificate usage .....</b>	<b>25</b>
4.5.1	Subscriber private key and certificate usage.....	25
4.5.2	Relying party public key and certificate usage .....	25
<b>4.6</b>	<b>Certificate renewal.....</b>	<b>25</b>
4.6.1	Circumstance for certificate renewal .....	25
4.6.2	Who may request renewal .....	25
4.6.3	Processing certificate renewal requests.....	25
4.6.4	Notification of new certificate issuance to subscriber .....	25
4.6.5	Conduct constituting acceptance of a renewal certificate .....	26



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

4.6.6	Publication of the renewal certificate by the CA .....	26
4.6.7	Notification of certificate issuance by the CA to other entities .....	26
<b>4.7</b>	<b>Certificate re-key .....</b>	<b>26</b>
4.7.1	Circumstance for certificate re-key.....	26
4.7.2	Who may request certification of a new public key.....	26
4.7.3	Processing certificate re-keying requests.....	26
4.7.4	Notification of new certificate issuance to subscriber .....	26
4.7.5	Conduct constituting acceptance of a re-keyed certificate .....	26
4.7.6	Publication of the re-keyed certificate by the CA.....	26
4.7.7	Notification of certificate issuance by the CA to other entities .....	27
<b>4.8</b>	<b>Certificate modification.....</b>	<b>27</b>
4.8.1	Circumstance for certificate modification.....	27
4.8.2	Who may request certificate modification.....	27
4.8.3	Processing certificate modification requests .....	27
4.8.4	Notification of new certificate issuance to subscriber .....	27
4.8.5	Conduct constituting acceptance of modified certificate.....	27
4.8.6	Publication of the modified certificate by the CA .....	27
4.8.7	Notification of certificate issuance by the CA to other entities .....	27
<b>4.9</b>	<b>Certificate revocation and suspension .....</b>	<b>27</b>
4.9.1	Circumstances for revocation .....	28
4.9.2	Who can request revocation .....	28
4.9.3	Procedure for revocation request.....	28
4.9.4	Revocation request grace period .....	28
4.9.5	Time within which CA must process the revocation request.....	28
4.9.6	Revocation checking requirement for relying parties.....	28
4.9.7	CRL issuance frequency (if applicable).....	28
4.9.8	Maximum latency for CRLs (if applicable).....	28
4.9.9	On-line revocation/status checking availability .....	28
4.9.10	On-line revocation checking requirements .....	28
4.9.11	Other forms of revocation advertisements available .....	29
4.9.12	Special requirements re key compromise .....	29
4.9.13	Circumstances for suspension.....	29



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

4.9.14	Who can request suspension.....	29
4.9.15	Procedure for suspension request.....	29
4.9.16	Limits on suspension period.....	29
<b>4.10</b>	<b>Certificate status services.....</b>	<b>29</b>
4.10.1	Operational characteristics.....	29
4.10.2	Service availability.....	30
4.10.3	Optional features.....	30
<b>4.11</b>	<b>End of subscription.....</b>	<b>30</b>
<b>4.12</b>	<b>Key escrow and recovery.....</b>	<b>30</b>
4.12.1	Key escrow and recovery policy and practices.....	30
4.12.2	Session key encapsulation and recovery policy and practices.....	30
<b>5</b>	<b>FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....</b>	<b>30</b>
<b>5.1</b>	<b>General.....</b>	<b>30</b>
<b>5.2</b>	<b>Physical controls.....</b>	<b>30</b>
5.2.1	Site location and construction.....	30
5.2.2	Physical access.....	31
5.2.3	Power and air conditioning.....	31
5.2.4	Water exposures.....	31
5.2.5	Fire prevention and protection.....	31
5.2.6	Media storage.....	31
5.2.7	Waste disposal.....	31
5.2.8	Off-site backup.....	31
<b>5.3</b>	<b>Procedural controls.....</b>	<b>31</b>
5.3.1	Trusted roles.....	31
5.3.2	Number of persons required per task.....	31
5.3.3	Identification and authentication for each role.....	31
5.3.4	Roles requiring separation of duties.....	31
<b>5.4</b>	<b>Personnel controls.....</b>	<b>32</b>
5.4.1	Qualifications, experience, and clearance requirements.....	32
5.4.2	Background check procedures.....	32
5.4.3	Training requirements.....	32



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

5.4.4	Retraining frequency and requirements .....	32
5.4.5	Job rotation frequency and sequence .....	32
5.4.6	Sanctions for unauthorized actions .....	32
5.4.7	Independent contractor requirements .....	32
5.4.8	Documentation supplied to personnel.....	32
<b>5.5</b>	<b>Audit logging procedures .....</b>	<b>32</b>
5.5.1	Types of events recorded .....	32
5.5.2	Frequency of processing log.....	32
5.5.3	Retention period for audit log.....	33
5.5.4	Protection of audit log.....	33
5.5.5	Audit log backup procedures .....	33
5.5.6	Audit collection system (internal vs. external) .....	33
5.5.7	Notification to event-causing subject.....	33
5.5.8	Vulnerability assessments .....	33
<b>5.6</b>	<b>Records archival.....</b>	<b>33</b>
5.6.1	Types of records archived .....	33
5.6.2	Retention period for archive.....	33
5.6.3	Protection of archive.....	33
5.6.4	Archive backup procedures .....	33
5.6.5	Requirements for time-stamping of records .....	33
5.6.6	Archive collection system (internal or external).....	34
5.6.7	Procedures to obtain and verify archive information .....	34
<b>5.7</b>	<b>Key changeover.....</b>	<b>34</b>
<b>5.8</b>	<b>Compromise and disaster recovery .....</b>	<b>34</b>
5.8.1	Incident and compromise handling procedures.....	34
5.8.2	Computing resources, software, and/or data are corrupted .....	34
5.8.3	Entity private key compromise procedures .....	34
5.8.4	Business continuity capabilities after a disaster .....	34
<b>5.9</b>	<b>CA or RA termination .....</b>	<b>35</b>
<b>6</b>	<b>TECHNICAL SECURITY CONTROLS.....</b>	<b>35</b>
<b>6.1</b>	<b>Key pair generation and installation .....</b>	<b>35</b>



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

6.1.1	Key pair generation .....	35
6.1.2	Private key delivery to subscriber .....	36
6.1.3	Public key delivery to certificate issuer .....	36
6.1.4	CA public key delivery to relying parties .....	36
6.1.5	Key sizes .....	36
6.1.6	Public key parameters generation and quality checking.....	36
6.1.7	Key usage purposes (as per X. v key usage field) .....	37
<b>6.2</b>	<b>Private Key Protection and Cryptographic Module Engineering Controls .....</b>	<b>37</b>
6.2.1	Cryptographic module standards and controls.....	37
6.2.2	Private key (n out of m) multi-person control.....	37
6.2.3	Private key escrow .....	37
6.2.4	Private key backup .....	37
6.2.5	Private key archival .....	37
6.2.6	Private key transfer into or from a cryptographic module .....	37
6.2.7	Private key storage on cryptographic module .....	37
6.2.8	Method of activating private key .....	38
6.2.9	Method of deactivating private key.....	38
6.2.10	Method of destroying private key .....	38
6.2.11	Cryptographic Module Rating .....	38
<b>6.3</b>	<b>Other aspects of key pair management .....</b>	<b>38</b>
6.3.1	Public key archival.....	38
6.3.2	Certificate operational periods and key pair usage periods.....	38
<b>6.4</b>	<b>Activation data.....</b>	<b>38</b>
6.4.1	Activation data generation and installation.....	38
6.4.2	Activation data protection .....	38
6.4.3	Other aspects of activation data .....	38
<b>6.5</b>	<b>Computer security controls .....</b>	<b>39</b>
6.5.1	Specific computer security technical requirements .....	39
6.5.2	Computer security rating.....	39
<b>6.6</b>	<b>Life cycle technical controls.....</b>	<b>39</b>
6.6.1	System development controls.....	39
6.6.2	Security management controls .....	39



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

6.6.3	Life cycle security controls .....	39
<b>6.7</b>	<b>Network security controls .....</b>	<b>39</b>
<b>6.8</b>	<b>Time-stamping .....</b>	<b>39</b>
<b>7</b>	<b>CERTIFICATE, CRL, AND OCSP PROFILES .....</b>	<b>39</b>
<b>7.1</b>	<b>Certificate profile .....</b>	<b>39</b>
7.1.1	Version number(s) .....	40
7.1.2	Certificate extensions .....	40
7.1.3	Algorithm object identifiers .....	40
7.1.4	Name forms .....	40
7.1.5	Name constraints .....	40
7.1.6	Certificate policy object identifier .....	40
7.1.7	Usage of Policy Constraints extension .....	40
7.1.8	Policy qualifiers syntax and semantics .....	40
7.1.9	Processing semantics for the critical Certificate Policies extension .....	41
<b>7.2</b>	<b>CRL profile .....</b>	<b>41</b>
7.2.1	Version number(s) .....	41
7.2.2	CRL and CRL entry extensions .....	41
<b>7.3</b>	<b>OCSP profile .....</b>	<b>41</b>
7.3.1	Version number(s) .....	41
7.3.2	OCSP extensions .....	41
<b>8</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....</b>	<b>41</b>
<b>8.1</b>	<b>Frequency or circumstances of assessment .....</b>	<b>42</b>
<b>8.2</b>	<b>Identity/qualifications of assessor .....</b>	<b>42</b>
<b>8.3</b>	<b>Assessor's relationship to assessed entity .....</b>	<b>42</b>
<b>8.4</b>	<b>Topics covered by assessment .....</b>	<b>42</b>
<b>8.5</b>	<b>Actions taken as a result of deficiency .....</b>	<b>42</b>
<b>8.6</b>	<b>Communication of results .....</b>	<b>42</b>
<b>9</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>43</b>
<b>9.1</b>	<b>Fees .....</b>	<b>43</b>
9.1.1	Certificate issuance or renewal fees .....	43
9.1.2	Certificate access fees .....	43



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

9.1.3	Revocation or status information access fees.....	43
9.1.4	Fees for other services .....	43
9.1.5	Refund policy.....	43
<b>9.2</b>	<b>Financial responsibility.....</b>	<b>43</b>
9.2.1	Insurance coverage .....	43
9.2.2	Other assets .....	43
9.2.3	Insurance or warranty coverage for end-entities .....	43
<b>9.3</b>	<b>Confidentiality of business information.....</b>	<b>43</b>
9.3.1	Scope of confidential information .....	44
9.3.2	Information not within the scope of confidential information .....	44
9.3.3	Responsibility to protect confidential information .....	44
<b>9.4</b>	<b>Privacy of personal information .....</b>	<b>44</b>
9.4.1	Privacy plan.....	44
9.4.2	Information treated as private .....	44
9.4.3	Information not deemed private .....	44
9.4.4	Responsibility to protect private information.....	44
9.4.5	Notice and consent to use private information .....	44
9.4.6	Disclosure pursuant to judicial or administrative process .....	44
9.4.7	Other information disclosure circumstances .....	44
<b>9.5</b>	<b>Intellectual property rights.....</b>	<b>45</b>
<b>9.6</b>	<b>Representations and warranties.....</b>	<b>45</b>
9.6.1	CA representations and warranties.....	45
9.6.2	RA representations and warranties.....	45
9.6.3	Subscriber representations and warranties.....	45
9.6.4	Relying party representations and warranties .....	45
9.6.5	Representations and warranties of other participants .....	45
<b>9.7</b>	<b>Disclaimers of warranties .....</b>	<b>45</b>
<b>9.8</b>	<b>Limitations of liability.....</b>	<b>45</b>
<b>9.9</b>	<b>Indemnities .....</b>	<b>45</b>
<b>9.10</b>	<b>Term and termination.....</b>	<b>46</b>
9.10.1	Term.....	46
9.10.2	Termination .....	46



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

9.10.3	Effect of termination and survival .....	46
<b>9.11</b>	<b>Individual notices and communications with participants.....</b>	<b>46</b>
<b>9.12</b>	<b>Amendments .....</b>	<b>46</b>
9.12.1	Procedure for amendment .....	46
9.12.2	Notification mechanism and period .....	46
9.12.3	Circumstances under which OID must be changed .....	46
<b>9.13</b>	<b>Dispute resolution provisions .....</b>	<b>46</b>
<b>9.14</b>	<b>Governing law .....</b>	<b>47</b>
<b>9.15</b>	<b>Compliance with applicable law.....</b>	<b>47</b>
<b>9.16</b>	<b>Miscellaneous provisions.....</b>	<b>47</b>
9.16.1	Entire agreement.....	47
9.16.2	Assignment.....	47
9.16.3	Severability.....	47
9.16.4	Enforcement (attorneys' fees and waiver of rights) .....	47
9.16.5	Force Majeure .....	47
<b>9.17</b>	<b>Other provisions .....</b>	<b>47</b>
9.17.1	Organizational .....	47
9.17.2	Additional testing .....	48
9.17.3	Disabilities .....	48
9.17.4	Terms and conditions .....	48
<b>10</b>	<b>References .....</b>	<b>49</b>



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

# 1 INTRODUCTION

## 1.1 Overview

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

- Certificate service
- Management of remote qualified signature creation devices
- Time stamp service

The services offer private and public organizations within the EU Internal Market the necessary trust service infrastructure to create 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 QTSPs are met.
- Certification Practice Statement (CPS) - this document  
describes how specific requirements concerning being Certification Authority 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 CPS cover the certificate policy defined in QCP-n-qscd.

## 1.2 Document name and identification

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

	<b>Certificate Practice Statement (CPS)</b>	Reference: N/A
		Version: 1.0
		Creation Date: 17/02/2025
		Last saved update: 19/02/2025

## 1.3 PKI participants

The PKI participants of the of the QTSP 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 QTSP 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
    - OCSP responder Certificate
  - Qualified TimeStamping Unit
  - CR.

The Root Certificate is a self-signed certificate constituting the top of the key hierarchy. It is used for issuing intermediate certificates for the QTSP 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 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.

### 1.3.2 Registration authorities

The QTSP relies on external entities for subject registration for issuance of qualified 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 high.

	<b>Certificate Practice Statement (CPS)</b>	Reference: N/A
		Version: 1.0
		Creation Date: 17/02/2025
		Last saved update: 19/02/2025

- (b) By using other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body.

Before allowing a notified electronic identification scheme to be used by the QTSP, the QTSP checks in Official Journal of the European Union, on whether the scheme is notified and that the level of assurance is high<sup>1</sup>.

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

### **1.3.3 Subscribers**

Subscribers are natural persons who receives a qualified certificate in a signature session flow. The subscribes is identified by a registration authority and has accepted the QTSPs Term and Conditions prior the issuance of the certificate.

Since the QTSP only issue certificates to natural person, subscribers and subjects are the same entity in this document and the terms are used interchangeably.

### **1.3.4 Relying parties**

The certificates issued by the QTSP is used for creation of qualified 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.

### **1.3.5 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 receipt of a certificate, it is submitted to the remote signing service. The signing service activates the signature key on the remote QSCD service creates 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 subject is authenticated by the relying party.

---

<sup>1</sup> 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](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202405468&qid=1731325587133)



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

- 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 redirect the subject with SSO to the signature service using the signature session identifier.
- The subject who is authenticated by the signing service through SSO is presented with the document for signing by the signing service. The user reads the document and the QTSP 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 and OCSP responder to gather time stamp tokens and OCSP responses.
  - 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 request 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 qualified electronic signatures during a signature session, these certificates cannot be revoked. However, to be able to produce advanced electronic signature formats, revocation status information must be available and the QTSP offers this as an OCSP service.

### 1.3.5.3 Repository Service

The QTSP provides 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 1.4 Certificate usage

### 1.4.1 Appropriate certificate uses

Subject certificates issued by the QTSP can be used for qualified 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 CPS is suitable for the chosen policy.

#### 1.5.3.1 General considerations on Certification Practice

This CPS meets the requirements in the policy QCP-n-qscd from [EN 319 411-2]. As such the all QCP-n requirements in [EN 319 411-2] and requirements in the policies NCP+ and NCP from [EN 319 411-1] are also implemented.

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

The CPS is accompanied by a profile [Profile] document specifying the format details of certificates, CRLs, OCSP as well as time stamps. 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



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

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.
CPS Summary (or CPS Abstract)	A subset of the provisions of a complete CPS that is made public by a CA.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

Term	Definition
Identification	<p>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:</p> <ol style="list-style-type: none"><li>(1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and</li><li>(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</li></ol>
Issuing certification authority (issuing CA)	<p>In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).</p>
Participant	<p>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.</p>
PKI Disclosure Statement (PDS)	<p>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.</p>
Policy qualifier	<p>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.</p>
Registration authority (RA)	<p>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.]</p>



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

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 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 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 QTSP issues subject certificates with the following name attributes:

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

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

### 3.1.2 Need for names to be meaningful

The QTSP 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 QTSP 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 [Profiles] for details on subject attributes.

### 3.1.4 Rules for interpreting various name forms

The are no policy requirements for interpreting various name forms.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### **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 QTSP has defined trademarks.

For subject and trademarks hold 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 QTSP 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 QTSP. 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 QTSP uses a QSCD managed by the QTSP to generate a subject key pair and creates a certification request which is signed by the subject private key to prove proof of possession.

### **3.2.2 Authentication of organization identity**

N/A. The QTSP 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.

	<b>Certificate Practice Statement (CPS)</b>	Reference: N/A
		Version: 1.0
		Creation Date: 17/02/2025
		Last saved update: 19/02/2025

### 3.3 Identification and authentication for re-key requests

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

## 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

### 4.1 Certificate Application

The QTSP 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 QTSP 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 subsequent sessions.

Subject key pairs are generated by the remote QSCD service which is part of the CA.

#### 4.1.1 Who can submit a certificate application

The QTSP issues certificates to subjects, who has been passed the processes provided by the registration authorities connected to the QTSP and who has accepted the QTSP terms and conditions.

	<b>Certificate Practice Statement (CPS)</b>	Reference: N/A
		Version: 1.0
		Creation Date: 17/02/2025
		Last saved update: 19/02/2025

## **4.1.2 Enrolment process and responsibilities**

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

## **4.2 Certificate application processing**

### **4.2.1 Performing identification and authentication functions**

The certificate application is created by the QTSP after receipt 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 QTSP creates a certificate application after it has received subject information from the Registration Authorities.

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

- a) The QTSP checks that the information received from the Registration Authority is from a registered Registration Authority.
- b) The QTSP checks that the information received from the Registration Authority is not altered during transmission.
- c) The QTSP 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 QTSP time.
- e) The received information has the expected level of assurance, high.
- 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 QTSP has received information on the subject identity from the Registration Authorities, see section 4.2.2, the QTSP

- uses a QSCD operated by the QTSP 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.

	<b>Certificate Practice Statement (CPS)</b>	Reference: N/A
		Version: 1.0
		Creation Date: 17/02/2025
		Last saved update: 19/02/2025

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

The QTSP 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 QTSP software.

The QTSP 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 confidentiality. 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 [Profiles] for details, and a new issuing CA is created well in advanced on CA certificate expiry to ensure that subject certificates are not issued with a validity beyond the CA certificate.

The QTSP 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 qualified certificates, the level of assurance must be high. The [Profiles] 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 QTSPs 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 QTSP 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 QTSP 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 QTSP does not publish subject certificates.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

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

The QTSP 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 QTSP and can only be used for signature generation, the subject is asked to pay special attention for the registration conducted at the Registration Authority and to ensure that authentication means are protected.

Subject private keys are managed by the QTSP on behalf of the subject. The QTSP has established systems, procedures and protocols, to ensure that the subject is always in sole control of the private keys. The QTSP operated 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 qualified signature before it is trusted.

## **4.6 Certificate renewal**

The QTSP 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### **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 QTSP 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 QTSP 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 QTSP only issues short-term certificates with a validity as specified in [Profiles]. 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 CPS at the time of issuance.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

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

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



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### **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 QTSP provides certificate revocation status information for subject certificates through OCSP. As subject certificates cannot be revoked, the service is only provided to support data for signature profiles.

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 QTSP.

The OCSP Responder provides status information for CA certificates managed by the QTSP 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 [Profiles], include the extension ArchiveCutOff set to the time and date from issuing CA notBefore.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

For Certification Authority and Time Stamp Authority certificates revocation status information is provided through CRL.

### **4.10.2 Service availability**

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

### **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 QTSP does not use key escrow or perform backup of subject private keys. It is not needed as the QTSP 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### **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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### **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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### **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 QTSP 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 QTSPs gm body and 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 QTSP identifies compromise, loss or suspected compromise of CA private key, the QTSP 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 QTSP 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 QTSP identifies that cryptographic algorithms, or associated parameters used by the QTSP for providing CA issuance and revocation status information becomes insufficient for the remaining intended usage period, the QTSP 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 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 QTSP manage CA cryptographic keys.

For subject key generation the QTSP 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 QTSP protected environment and configured under supervised procedures.

The [Profiles] 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 QTSP 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 QTSP uses the cryptographic module to delete the subject key pair.

The QTSP has procedures in place to monitor the certification status of the rQSCD. In case the rQSCD unexpectedly loses the certification status, the QTSP will inform its conformity assessment body and supervisory body with a plan on its intension to replace the rQSCD. Until the plan has been executed, the statement esi4-qcStatement-4 will not be included in the qualified certificates.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

The QTSP 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 QTSP are carried out using cryptographic algorithms and strength as recommended by [TS 119 312].

The QTSP creates a new CA before any active CA certificate expires. In [Profiles] 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 place timely enough for the supervisory body to approve the new certificate.

### **6.1.2 Private key delivery to subscriber**

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

### **6.1.3 Public key delivery to certificate issuer**

The QTSP 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 QTSP CA public key is made available for relying parties through the list of trusted lists. In addition, it can be found on the QTSPs 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 [Profiles].



### **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 [Profiles].

## **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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 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 QTSP has published a separate practice statement document on its time stamp authority.

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificate profile

The certificate profiles, [Profiles], for subject certificates are created to meet the requirements specified in [RFC5280], [EN 319 411-1], [EN 319 411-2]. Certificates are always issued to natural persons with the private key on a QSCD managed by the QTSP.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### **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:

- AuthenticationContexts
- authorityInfoAccess
- authorityKeyIdentifier
- BasicConstraints
- CertificatePolicies
- KeyUsage
- qc-statements-2
- subjectKeyIdentifier
- Validity Assured Certificate

### **7.1.3 Algorithm object identifiers**

See [Profiles] for used algorithm identifiers.

### **7.1.4 Name forms**

See [Profiles] 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+ and QCP-n-qscd. The identifier for QCP-n-qscd 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.

	<b>Certificate Practice Statement (CPS)</b>	Reference: N/A
		Version: 1.0
		Creation Date: 17/02/2025
		Last saved update: 19/02/2025

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

N/A. No policy requirements.

## **7.2 CRL profile**

N/A. The QTSP 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 unknown for certificates are not (yet) issued by the CA.

The QTSP 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 QTSP and its qualified trust service are conformity assessed for compliance with the [eIDAS], the relevant standards and the practices described in this and other practice documents.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

The result of any assessment is provided for QTSP management and any suggestions for improvement of its practiced are approved by QTSP management.

### 8.1 Frequency or circumstances of assessment

The QTSP is conformity checked against the applicable regulation and standards at least at the interval determined by regulation [eIDAS] or as required by the conformity assessment body.

If the QTSP intends to make major changes to its offering, the conformity assessment body is consulted and jointly it is decided if an additional assessment is required.

### 8.2 Identity/qualifications of assessor

The Conformity Assessment Body (CAB) is accredited according to [ISO/IEC 17065], as required by [EN 319 403], with a focus on meeting the requirements specified in the [eIDAS] regulation.

The CAB is authorized to perform conformity assessments of Qualified Trust Service Providers and their services.

### 8.3 Assessor's relationship to assessed entity

The conformity assessment body is independent of the QTSP.

### 8.4 Topics covered by assessment

The scope of the conformity assessment covers the qualified trust services offered by the QTSP as described in [TSP PS].

### 8.5 Actions taken as a result of deficiency

In case the conformity assessment body identifies any non-conformity during assessment, the QTSP management is informed, and a remediation plan is shared with the conformity assessment body and if required also with the supervisory body.

### 8.6 Communication of results

The QTSP may choose to publish the certification document received by the conformity assessment body.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### **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 QTSP 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 9.5 Intellectual property rights

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

## 9.6 Representations and warranties

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

The QTSPs 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 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 QTSP services this is described in the terms and conditions.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### 9.14 Governing law

This QTSP 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.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

### 9.17.2 Additional testing

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

### 9.17.3 Disabilities

See [TSP PS] section 7.13.

### 9.17.4 Terms and conditions

See [TSP PS] section 6.2.



## Certificate Practice Statement (CPS)

Reference: N/A

Version: 1.0

Creation Date: 17/02/2025

Last saved update: 19/02/2025

## 10 REFERENCES

References	
Text reference	Description
[T&C]	Terms and conditions, <a href="https://pki.ingroupe.dk/repository/">https://pki.ingroupe.dk/repository/</a>
[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]	Certificate profiles, <a href="https://pki.ingroupe.dk/repository/">https://pki.ingroupe.dk/repository/</a>
[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, IN Group Denmark, <a href="https://pki.ingroupe.dk/repository/">https://pki.ingroupe.dk/repository/</a>
[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.