Paperless

Qualified Sealing Certificates for the production of Qualified Electronic Seals

Certificate Policy & Certification Practice Statement

Document Name	Certificate Policy & Certification Practice Statement - Qualified Sealing Certificates for the production of Qualified Electronic Seals
Abbreviation	CP/CPS (Qualified Sealing)
OID	1.3.6.1.4.1.64134.1.2.2.2
Author	Paperless GmbH - Frankfurt am Main, Germany
Owner	Security Officer (SO)
Classification	public
Version	1.0
Date of Publication	2025-10-01

Contents

1 Introduction 3
1.1 Overview 3
1.2 Document Name and Identification 3
1.3 PKI Participants 3
1.4 Certificate Usage 3
1.5 Policy Administration 3
1.6 Definitions and Acronyms 3
2 Publication and Repository Responsibilities 4
2.1 Reponsibilities 4
2.2 Frequency of Publication 4
2.3 Access Control 4
3 Identification & (Re-)Authentication 4
3.1 Naming 4
3.2 Initial Identity Verification 5
3.3 Identification and Authentication for Signing & Sealing 5
3.4 Identification and Authentication for Re-key Requests 5
3.5 Identification and Authentication of Revocation Requests 5
4 Certificate Life-Cycle 5
5 Facility, Management, and Operational Controls 5
6 Technical Security Controls 6
6.1 Key Pair Generation and Installation 6
6.2 Private Key Protection & Cryptographic Module Engineering Controls 6
6.3 Other Aspects of Key Pair Management 6
6.4 Activation Data 6
6.5 Computer Security Controls 7
6.6 Life Cycle Security Controls 7
6.7 Network Security Controls 7
6.8 Timestamping 7
7 Profiles 7
7.1 Certificate Profiles 7
7.1.1 Root CA Certificates 7
7.1.2 Intermediate CA Certificates 7
7.1.3 Qualified Sealing Certificates for the production of Qualified Electronic Seals 7
7.2 Signature Profiles 9
8 Compliance Audit and Other Assessment 9
9 Other Business and Legal Matters 9
Bibliography 10
Revision History 11

1 Introduction

The present document is the combined Certificate Policy (CP) and Certification Practice Statement (CPS) of the Trust Service Provider (TSP) Paperless GmbH describing – in combination with the Trust Service Practice Statement (TSPS) – its current practice in the issuance of qualified sealing certificates to legal persons for use in the production of qualified electronic seals.

As a CP, this document further constrains the requirements laid out in ETSI EN 319 411-1 [1] and ETSI EN 319 411-2 [2] for the `QCP-l-qscd` policy (`0.4.0.194112.1.3`).

1.1 Overview

This is documented in the TSPS.

1.2 Document Name and Identification

The information on the name and the identification of this document is present on the title page.

1.3 PKI Participants

This is documented in the TSPS.

1.4 Certificate Usage

This is documented in the TSPS.

1.5 Policy Administration

The present document is administered by:

Paperless GmbH
Große Friedberger Strasse 13-17
60313 Frankfurt am Main
trust@paperless.io
+49 69 348765460

Any changes made are approved by TSP management and checked to be consistent with the TSP's practices.

1.6 Definitions and Acronyms

CA – Certificate Authority

CP – Certificate Policy

CPS – Certification Practice Statement

DTBSR – Data To Be Signed Representation: The digest of the DTBS which is cryptographically signed

HSM – Hardware Security Module

LoIP – Level of Identity Proofing

OID – Object Identifier

QSCD – Qualified Signature Creation Device

RO – Registration Officer

SAM – Signature Activation Module

SO – Security Officer

T&C – Terms and Conditions

TSP – Trust Service Provider

TSPS – Trust Service Practice Statement

2 Publication and Repository Responsibilities

All documentation regarding the TSP's trust services, including other versions of the present document and past and present Certificate Authority (CA) & service certificates, is publicly and internationally available 24 hours per day and 7 days per week at following locations:

- https://repo.trust.paperless.io
- https://repo.paperlesstrust.de

Upon system failure, service or other factors which are not under the control of the TSP, the TSP applies best endeavours to ensure that this information service is not unavailable for longer than 24 hours.

The current version of the present document may be found at the following locations:

- https://repo.trust.paperless.io/cps/qcp-l-qscd.pdf
- https://repo.paperlesstrust.de/cps/qcp-l-qscd.pdf

2.1 Reponsibilities

The TSP is committed to publish every version of:

- The Trust Service Practice Statement (TSPS)
- All Certificate Policys (CPs) and Certification Practice Statements (CPSs)
- The Terms and Conditions (T&C)
- Subscriber agreement
- The privacy policy
- The accessibility statement

The TSP reserves the right to publish new versions of the documentation without prior notice. The TSP will notify subscribers before changes are made affecting the acceptance of the service.

Following the publication, all versions of this document are communicated to employees of the TSP and external parties as relevant.

2.2 Frequency of Publication

The TSP regularly reviews its policies, procedures and public documentation, including the present document.

Any changes made as a result of these reviews or when otherwise necessary are immediately published as described in Section 2.1.

There is no minimum publication interval.

2.3 Access Control

Access to development and publication repositories related to the administration of the published documentation and certificate information is limited to trusted TSP personnel and requires multi-factor authentication.

3 Identification & (Re-)Authentication

3.1 Naming

For a complete list of utilized attributes and the corresponding Object Identifiers (OIDs), consult Section 7.1.

The following information is collected and verified during the enrollment of a legal entity:

- `countryName`: Country the legal entity is registered in, as per ISO 3166 [3]
- `organizationName`: Full registered name of the legal entity, e.g. as included in a trade register
- `organizationalUnitName`: Optional additional specifier chosen by the enrolling legal entity
- `organizationIdentifier`: Identifier adherent to the legal person semantics identifier defined in ETSI EN 319 412-1 [4], including for instance the identifier of the legal entity in some trade register.
- `commonName`: Some representable name of the subject, summarizing both `organizationName` and `organizationalUnitName`. Chosen by the enrolling legal entity and checked to be a reasonable identifier by the enrolling Registration Officer (RO).

3.2 Initial Identity Verification

Subjects are verified to an extended Level of Identity Proofing (LoIP) as per ETSI TS 119 461 [5] and a high assurance level as per ETSI EN 419 241-1 [6].

For the initial identity verification, the TSP requires information on the identity of the legal person, provided by a natural person who is authorized to represent the legal person (representative), such as trusted register numbers or equivalent identifying information. Identity verification of legal entities is always carried out by TSP personnel (ROs). No third-party provider is involved in this process.

The representative's identity must verified as described in Section 3.2 of the CP/CPS for qualified signing, provide relevant evidence of their authorization to represent the legal entity, especially for the issuance of certificates on behalf of the legal entity, and confirm the information provided by signing it with a qualified electronic signature. The TSP verifies the power of representation on the basis of the register and/or articles of association and/or official seals and documents.

In the case of commercial organizations, the identification of the subject is verified with a certified extract from a commercial or association register. In the case of public organizations, the identification of the subject is verified with an official seal and the signature of an authorized representative on the setup order.

The `organization` certificate attribute is populated directly from the proof of organization.

The `organizationIdentifier` certificate attribute uniquely identifies the organization and is constructed based on information from the proof of organization, as per the "legal person semantics" identifier semantics defined in ETSI EN 319 412-1 [4].

The `organizationalUnit` and `commonName` certificate attributes can be set freely by the subject within reasonable boundaries. Names that suggest non-existent official or authorization relationships are not permitted, nor are discriminatory or otherwise misleading statements.

The TSP performs a formal plausibility and admissibility check before approval, with at least dual control.

After successful identity verification, the naming data for the subject and organizational metadata is stored in the TSP's database. The representative is registered as an authorized sealer.

The TSP contractually ensures that all future authorized sealers are allowed to authorize the issuance of certificates on behalf of the legal entity.

The ROs of the TSP repeat the organization identity verification at least every 48 months as described in Section 3.2. The TSP may block accesses to its services as a precautionary measure until clarification when discrepancies occur, while contacting the subject for clarification.

3.3 Identification and Authentication for Signing & Sealing

This is documented in the TSPS.

3.4 Identification and Authentication for Re-key Requests

This is documented in the TSPS.

3.5 Identification and Authentication of Revocation Requests

This is documented in the TSPS.

4 Certificate Life-Cycle

This is documented in the TSPS.

5 Facility, Management, and Operational Controls

This is documented in the TSPS.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

This is documented in the TSPS.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

For general provisions, including the protection of CA and service keys, see the TSPS. This section of the present document describes the protection of keys managed by the TSP on behalf of subjects.

Generating, managing and duplicating electronic signature creation data on behalf of the signatory is only done by the TSP on a Qualified Signature Creation Device (QSCD). The management of the QSCD as a qualified service is only be carried out by the TSP. Keys held by the TSP on behalf of subjects for the production of qualified signatures and seals are generated (and can only be used) in a QSCD.

This QSCD consists of a Signature Activation Module (SAM), certified to be conformant to ETSI EN 419 241-2 [7], installed in a Hardware Security Module (HSM) certified to be conformant to ETSI EN 419 221-5 [8]. This certification includes the signature activation protocol used to protect signature activation data during key generation and usage (see Section 6.4). The TSP regularly reviews the certification of the QSCD and assesses its suitability.

The TSP maintains an internal Operation Security Policy for operating the trusted systems including those containing the QSCD. This policy includes references to detailed operational procedures including instructions for secure handling, administration, maintenance of the TSP's systems and the QSCD. The QSCD is installed and operated in accordance with manufacturer guidance and the certification report to ensure correct and secure deployment and operation. The clock of the HSM hosting the QSCD is synchronized to the host system. The time-keeping of the host system is described in Section 6.8 of the TSPS.

After key generation, the signer's private key is exported by the QSCD in an encrypted form. This is stored in a database operated by the TSP, and supplied when needed during signature activation. This encrypted key can only be used in the QSCD when authorized using the activation PIN held by the signer (see Section 6.4). This ensures the same level of protection as if the key were held in the QSCD itself.

Installation and initialization of the QSCD, as well as the creation and restoration of backups is done under dual control, requiring two different authorized TSP employees. Backups are stored in a backup HSM providing equivalent protection to the live HSM, stored in a secure, offline location.

Exported key material is only duplicated to the extent necessary for replication and backup. Exported keys that are destroyed due to certificate expiration or revocation are also destroyed in all online replicas of the database and – after appropriate retention periods – backups.

6.3 Other Aspects of Key Pair Management

This is documented in the TSPS.

6.4 Activation Data

For long-term signing or sealing keys, the user is prompted for a PIN during key generation. This PIN is required for usage of the key, and ensures that the key remains under the sole control (for natural person subjects) or control (for legal person subjects) of the subject.

For short-term signing keys, a PIN is generated on the subjects device during key generation, which is then used during signing later in the same signing session and destroyed afterwards. This PIN is never stored permanently or transmitted anywhere, with the exception of the signature activation protocol used during key generation and enrollment.

The protocol used for signature activation and key generation using the QSCD is certified as described in Section 6.2. This protocol establishes an authenticated and encrypted channel between the QSCD and the user's device, and protects the signature activation data against forgery, bypass, tampering, duplication, eavesdropping or replay by both third parties, and the TSP itself.

In addition to the PIN and the Data To Be Signed Representation (DTBSR) provided by the signer, the TSP provides the appropriate exported and encrypted private key to be used for signing, and an authorization token authorizing the use of this specific signing key. This token is issued using a key residing in an HSM as described in the TSPS and securely passed to the signer, only after all required identity verification, authentication, and authorization steps have been completed successfully. The key can only be used with the correct PIN and a valid token supplied by the TSP. The TSP ensures the the linked identity verification and authorizations are the same as the one linked to the subject of the used certificate by using a relational database with appropriate referential integrity controls (foreign keys).

Beyond the provisions in Section 6.3, any signing key associated with a short-term certificate (linked directly to identity as per ETSI TS 119 431-1 [9]) is destroyed after the first and only signature activation process. For such short-term signing certificates, the signing process ends at most 30 minutes after the identity verification, and the signature activation data contains identifiers of the signature session and the identity verification process.

6.5 Computer Security Controls

This is documented in the TSPS.

6.6 Life Cycle Security Controls

This is documented in the TSPS.

6.7 Network Security Controls

This is documented in the TSPS.

6.8 Timestamping

This is documented in the TSPS.

7 Profiles

See TSPS for general remarks.

7.1 Certificate Profiles

See TSPS for general remarks.

7.1.1 Root CA Certificates

This is documented in the TSPS.

7.1.2 Intermediate CA Certificates

This is documented in the TSPS.

7.1.3 Qualified Sealing Certificates for the production of Qualified Electronic Seals

Issued by the TSP to legal persons for the exclusive purpose of qualified seal creation. Keys are held in a QSCD by the TSP, at the control of authorized sealers.

Attribute	Value
`version`	V3 (`0x2`)
`serial_number`	Cryptographically random & unique 128-bit number
`issuer`	See Section 7.1.2.
`subject`	See Table 2.
`validity`	2 years
`signature`	EC (`1.2.840.10045.2.1`), NIST P-256 curve (`1.2.840.10045.3.1.7`)
`subject_public_key_info`	See Section 6.1 for details on key generation.
`extensions`	See Table 3.
`signature_algorithm`	ECDSA w/ SHA256 (`1.2.840.10045.4.3.2`)
Signed by	Qualified Sealing CA (see TSPS)

Table 1: Attributes of qualified sealing certificates for the production of qualified electronic signatures

Name	OID	Value
`countryName`	`2.5.4.6`	See Section 3.1.
`organizationName`	`2.5.4.10`	See Section 3.1.
`organizationalUnitName`	`2.5.4.11`	See Section 3.1, optional.
`organizationIdentifier`	`2.5.4.11`	See Section 3.1.
`commonName`	`2.5.4.3`	See Section 3.1.

Table 2: Subject name attributes used in certificate

Name	OID	Notes	Crit.
subjectKeyIdentifier	2.5.29.14	Calc. as per RFC5280 [10, 5.2.1.2]	
authorityKeyIdentifier	2.5.29.35	Calc. as per RFC5280 [10, 5.2.1.1]	
basicConstraints	2.5.29.19	CA == false, no pathLenConstraint	×
keyUsage	2.5.29.15	nonRepudiation	×
certificatePolicies	2.5.29.32	QCP-l-qscd (0.4.0.194112.1.3) present doc. (1.3.6.1.4.1.64134.1.2.2.2) CPS: https://repo.trust.paperless.io/cps/qcp-l-qscd.pdf	
qcStatements	1.3.6.1.5.5.7.1.3	As per RFC3739 [11] & ETSI EN 319 412-5 [12]: id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-QcType (0.4.0.1862.1.6): id-etsi-qct-eseal (0.4.0.1862.1.6.2) id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2): id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)“)	
authorityInfoAccess	1.3.6.1.5.5.7.1.1	OCSP (1.3.6.1.5.5.7.48.1): • http://qcp-l-qscd-ca-g{i}.ocsp.trust.paperless.io/ • http://qcp-l-qscd-ca-g{i}.ocsp.paperlesstrust.de/ CA Issuers (1.3.6.1.5.5.7.48.2): • http://repo.trust.paperless.io/qcp-l-qscd-ca-g{i}.crt • http://repo.paperlesstrust.de/qcp-l-qscd-ca-g{i}.crt	

Table 3: Extensions included in certificate

7.2 Signature Profiles

This is documented in the TSPS.

8 Compliance Audit and Other Assessment

This is documented in the TSPS.

9 Other Business and Legal Matters

This is documented in the TSPS.

Bibliography

[1] "ETSI EN 319 411-1: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements." [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.05.01_60/en_31941101v010501p.pdf

[2] "ETSI EN 319 411-2: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates." [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.06.01_30/en_31941102v020601v.pdf

[3] "ISO 3166: Country Codes." [Online]. Available: https://www.iso.org/iso-3166-country-codes.html

[4] "ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures." [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.06.00_20/en_31941201v010600a.pdf

[5] "ETSI TS 119 461: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects." [Online]. Available: https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/02.01.01_60/ts_119461v020101p.pdf

[6] "DIN EN 419 241-1: Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements."

[7] "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing." [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/anssi-cc-pp-2018_02fr_pp.pdf

[8] "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services." [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-PP-2016_05%20PP.pdf

[9] "ETSI TS 119 431-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev." [Online]. Available: https://www.etsi.org/deliver/etsi_ts/119400_119499/11943101/01.03.01_60/ts_11943101v010301p.pdf

[10] "RFC5280: Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile." [Online]. Available: https://www.rfc-editor.org/rfc/rfc5280

[11] "RFC3739: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile." [Online]. Available: https://www.rfc-editor.org/rfc/rfc3739

[12] "ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements." [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/31941205/02.04.01_60/en_31941205v020401p.pdf

Revision History

Version	Date	Change Description
1.0	2025-10-01	Initial release.