Paperless

Qualified Signing Certificates

Certificate Policy & Certification Practice Statement

Document Name	Certificate Policy & Certification Practice Statement - Qualified Signing Certificates
Abbreviation	CP/CPS (Qualified Signing)
OID	1.3.6.1.4.1.64134.1.2.2.1
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

The present document is the combined Certificate Policy (CP) and Certification Practice Statement (CPS) (as per ITU-T Rec. X509 [1]) 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 signing certificates to natural persons for use in the production of qualified electronic signatures.

As a CP, this document further constrains the requirements laid out in ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3] for the `QCP-n-qscd` policy (`0.4.0.194112.1.2`).

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-n-qscd.pdf
- https://repo.paperlesstrust.de/cps/qcp-n-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 stored during identity verification and (with the exception of the document number) included in the issued certificate:

- `countryName`: Country of residence as contained in identity document, as two-letter (`alpha-2`) code as per ISO 3166-1 [4]. If no country of residence exists or can be determined, `"ZZ"` is included.
- `givenName`: Given name(s) as contained in identity document. Multiple names are concatenated using single spaces (`" "`). See Table 1.
- `surname`: Optionally, surname(s) as contained in identity document. Multiple names are concatenated using single spaces (`" "`). See Table 1.

- `nameSuffix`: Optionally, name suffix(es) as contained in identity document (e.g. a birth name). Multiple suffixes are concatenated using single spaces (`" "`). Only included in certificate in `commonName`, see Table 1.
- `commonName`: Combination of other naming attributes as per Table 1.
- Number of identity document used for verification (not included in certificate)

Additionally, the V4 UUID associated with the signer's TSP account is included in the certificate. This is generated by the TSP and permanently and uniquely associated with a single natural person's account.

`givenName`	`surname`	Resulting `commonName`
×		`givenName` + `nameSuffix`
×	×	`givenName` + `surname` + `nameSuffix`

Table 1: Valid combinations of subject name attributes for natural persons. `nameSuffix` is ommitted if not present.

All included name data (`givenName`, `surname`, `commonName`) is encoded identically, as specified on the identity document.

3.2 Initial Identity Verification

This is documented in the TSPS.

3.2.1 Email Verification

This is documented in the TSPS.

3.2.2 Identity Verification

The identity of subjects is 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] using an appropriate identity document, either in person by a Registration Officer (RO) employed by the TSP according to a defined procedure (Section 3.2.2.1), or remotely, by an appropriate and authorized subcontracted third party (Section 3.2.2.2). The identity of subjects is valid until the expiration date of the identity document used for identification.

3.2.2.1 Identity Verification by RO

When the identity verification is carried out manually by a TSP RO, the identity of the person to be identified (iP) is verified using valid, nationally recognized identity document.

All natural persons who are in possession of a valid identity document that is acceptable for the procedure can be identified. Valid German identity cards, other equivalent German identity documents, foreign official identity cards equivalent to German identity cards, and passports are considered acceptable identity documents, provided that these documents contain a photograph of the holder.

An RO can either be an employee of Paperless GmbH or a trained employee of a delegated registration office (e.g., companies, local authorities, or other contractual partners) authorized by Paperless GmbH.

In both cases, a uniform, standardized procedure applies:

1. Presentation and verification of a valid ID document,
2. Comparison of the photograph with the person present,
3. Verification of essential security features,
4. Entry of personal data in the designated Paperless form,
5. Upload of images of the front and back of the ID card,
6. Answering questions regarding suspected fraud,
7. Completing the process with the qualified electronic signature (QES) of the form by the RO.

Once identification has been completed, the identification data is transmitted to the TSP digitally and automatically. The naming and expiration information contained in the presented identity document is used for certificate issuance (see Section 3.1, Section 7.1). The identification data record serves as proof of the identification carried out and confirms the applicant's details if they match. Data collection is limited to essential data that clearly documents the identification (the data described in Section 3.1 and images of the ID document of the identified person).

3.2.2.2 Identity Verification by a subcontracted third party

For remote identification, the TSP uses subcontracted third-parties.

The TSP maintains overall responsibility and ensures that all subcontracted parties meet the relevant eIDAS and – if applicable – national or EU requirements, including 6.3.2 Signer authentication (SRC_SA) of EN 419 241-1 by requiring a valid eIDAS certificate ("Modulbestätigung"), as well as the provision of the corresponding conformity assessment report to the CAB and the national supervisory body. Manual testing of the subcontracted third parties' services with regard to relevant requirements is performed by the TSP.

Name	Address	Service Name	Conformity Assessment
Nect GmbH	Großer Burstah 21 20457 Hamburg Germany	Nect Ident	Certificate ID: DSC.1568.07.2025 Certificate Date: 15.07.2025 Expiry Date: 14.07.2027
IDnow GmbH	Auenstraße 100 80469 Munich Germany	Videoldent	Certificate No.: TSP-12353/25-1-1-2 Date of issue: 23.06.2025 Expiry date: 22.06.2027
IDnow GmbH	Auenstraße 100 80469 Munich Germany	Autoldent	Certificate No.: TSP-12353/25-1-2-2 Date of issue: 23.06.2025 Expiry date: 22.06.2027

Table 2: Subcontracted third-parties for identity verification

For these remote identification mechanisms, the subject/subscriber is redirected to the website of the subcontracted third party where the user is guided through the whole identification process.

This process includes the verification of the presented document, as well as a manual or automated face verification.

After successful completion of the identity verification, the user is redirected back to the TSP to continue with the certificate application.

3.2.3 Second Factor Creation

This is documented in the TSPS.

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 Signing Certificates

Issued by the TSP to natural persons for the exclusive purpose of qualified signature creation. Keys are held in a QSCD by the TSP, at the sole control of the subject.

Based on tenant or subscriber preference or other considerations, the TSP may issue long-term or short-term certificates, as described in Note 1.

Attribute	Value
`version`	V3 (`0x2`)
`serial_number`	Cryptographically random & unique 128-bit number
`issuer`	See Section 7.1.2.
`subject`	See Table 4.
`validity`	See Note 1.
`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 5.
`signature_algorithm`	ECDSA w/ SHA256 (`1.2.840.10045.4.3.2`)
Signed by	Qualified Signing CA (see Section 7.1.2)

Table 3: Extensions included in certificate

Name	OID	Value
`countryName`	`2.5.4.6`	See Section 3.1.
`givenName`	`2.5.4.42`	See Section 3.1, conditional.
`surname`	`2.5.4.4`	See Section 3.1, conditional.
`commonName`	`2.5.4.3`	See Section 3.1.
`serialNumber`	`2.5.4.5`	V4 UUID uniquely identifying person

Table 4: Subject name attributes used in qualified signing certificates

Name	OID	Notes	Crit.
`subjectKeyIdentifier`	`2.5.29.14`	Calc. as per RFC5280 [10, 5.2.1.2]	
`àuthorityKeyIdentifier`	`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-n-qscd` (`0.4.0.194112.1.2`) present doc. (`1.3.6.1.4.1.64134.1.2.2.1`) CPS: `https://repo.trust.paperless.io/cps/qcp-n-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-esign` (`0.4.0.1862.1.6.1`)	
`authorityInfoAccess`	`1.3.6.1.5.5.7.1.1`	OCSP (`1.3.6.1.5.5.7.48.1`): • `http://qcp-n-qscd-ca-g{i}.ocsp.trust.paperless.io/` • `http://qcp-n-qscd-ca-g{i}.ocsp.paperlesstrust.de/` CA Issuers (`1.3.6.1.5.5.7.48.2`): • `http://repo.trust.paperless.io/qcp-n-qscd-ca-g{i}.crt` • `http://repo.paperlesstrust.de/qcp-n-qscd-ca-g{i}.crt`	

Table 5: Extensions included in qualified signing certificates

Note **Note 1**

At the API tenant and TSP's discretion, the TSP either issues long-term or short-term certificates. All certificates are revokable, they only differ in the validity duration and signature activation data & key management (see Section 6.4 & Section 6.3).

Long-term certificates are linked to the account of the subject and require authentication using an appropriate authentication token (as described in Section 3 of the TSPS) for use.

Short-term certificates are only usable once, immediately after identity verification (linked directly to identity as per ETSI TS 119 431-1 [9]). These do not require an authentication token, but are limited to a single use and signing session, after which the key associated with the certificate is destroyed (see Section 6.4).

For short-term certificates, the validity duration is at most 1 hour.
For long-term certificates, the validity duration is at most 2 years.

In addition, the validity period of the certificate never exceeds the date of expiration of the identity document used for identity verification (see Section 3).

The validity assured extension `ext-etsi-valassured-ST-certs` as defined in [13] is never used.

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] "X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks." [Online]. Available: https://www.itu.int/rec/T-REC-X.509/en

[2] "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

[3] "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

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

[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

[13] "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

Revision History

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