Paperless

Advanced Signing Certificates

Certificate Policy & Certification Practice Statement

Document Name	Certificate Policy & Certification Practice Statement - Advanced Signing Certificates
Abbreviation	CP/CPS (Advanced Signing)
OID	1.3.6.1.4.1.64134.1.2.2.3
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 . . . 3
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 . . . 4
3.2.1 Email Authentication . . . 4
3.2.2 Identity Verification . . . 4
3.2.3 Second Factor Creation . . . 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 . . . 5
6.1 Key Pair Generation and Installation . . . 5
6.2 Private Key Protection & Cryptographic Module Engineering Controls . . . 5
6.3 Other Aspects of Key Pair Management . . . 5
6.4 Activation Data . . . 5
6.5 Computer Security Controls . . . 5
6.6 Life Cycle Security Controls . . . 6
6.7 Network Security Controls . . . 6
7 Profiles . . . 6
7.1 Certificate Profiles . . . 6
7.1.1 Root CA Certificates . . . 6
7.1.2 Intermediate CA Certificates . . . 6
7.1.3 Advanced Signing Certificates . . . 6
7.2 Signature Profiles . . . 7
8 Compliance Audit and Other Assessment . . . 7
9 Other Business and Legal Matters . . . 7
Bibliography . . . 8
Revision History . . . 9

1 Introduction

The present document is the 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 advanced signing certificates to natural persons for use in the production of advanced electronic signatures.

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

1.6 Definitions and Acronyms

CA – Certificate Authority

CP – Certificate Policy

CPS – Certification Practice Statement

HSM – Hardware Security Module

OID – Object Identifier

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/lcp.pdf

- https://repo.paperlesstrust.de/cps/lcp.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 provided by the API tenant during the creation of the signing process and used in the issuance of certificates:

- `commonName`: An arbitrary name chosen by the API tenant, representing the subject. Not verified by the TSP.
- `emailAddress`: The email address supplied by the API tenant, verified during identity verification and authentication. Note that this attribute of the subject name, but in the `subjectAltName` extension, as described in Section 7.1.

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.

3.2 Initial Identity Verification

This is documented in the TSPS.

3.2.1 Email Authentication

This is documented in the TSPS.

3.2.2 Identity Verification

Subjects are primarily identified by their email address, which is verified during the identity verification and authentication steps outlined in the TSPS.

Email address and name (see Section 3.1) are provided by the API tenant starting the signing process.

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.

Keys held by the TSP on behalf of subjects for the production of advanced signatures and seals are generated in a Hardware Security Module (HSM) as described in Section 6.1 and stored in an encrypted form in a database operated by the TSP.

The key material only leaves the HSM in an encrypted form. The wrapping key used for the encryption and decryption is held to the same standard as the CA and service keys described in the TSPS.

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

Activation of advanced signing & sealing requires the wrapped and exported private key, held by the TSP in a database after the initial key generation.

Signature activation requests are only processed if the authentication and authorization steps described in Section 3.3 have been completed.

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.

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 Advanced Signing Certificates

Attribute	Value
`version`	V3 (`0x2`)
`serial_number`	Cryptographically random 128-bit number
`issuer`	See Qualified Intermediate CA subject in TSPS.
`subject`	See Table 2.
`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 3.
`signature_algorithm`	ECDSA w/ SHA256 (`1.2.840.10045.4.3.2`)
Signed by	Advanced Intermediate CA (see Section 7.1.2)

Table 1: Attributes of advanced signing certificates

Name	OID	Value
`commonName`	`2.5.4.3`	See Section 3.1
`serialNumber`	`2.5.4.5`	V4 UUID uniquely identifying person

Table 2: Subject name attributes used in advanced signing certificates

Name	OID	Notes	Crit.
`subjectKeyIdentifier`	`2.5.29.14`	Calc. as per RFC5280 [1, 5.2.1.2]	
`àuthorityKeyIdentifier`	`2.5.29.35`	Calc. as per RFC5280 [1, 5.2.1.1]	
`basicConstraints`	`2.5.29.19`	`CA == false`, no `pathLenConstraint`	×
`keyUsage`	`2.5.29.15`	`nonRepudiation`	×
`subjectAltName`	`2.5.29.17`	`rfc822Name`: Subject email address, see Section 3.1	
`certificatePolicies`	`2.5.29.32`	`LCP` (`0.4.0.2042.1.3`)	
`authorityInfoAccess`	`1.3.6.1.5.5.7.1.1`	`ocsp` (`1.3.6.1.5.5.7.48.1`): URL to OCSP responder	

Table 3: Extensions included in advanced 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).

Issuance of long-term certificates requires the signer to be authenticated using a second factor as per Section 3.

For short-term certificates, the validity duration is at most .
For long-term certificates, the validity duration is at most .

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

Revision History

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