Paperless

Paperless Trust Services

Trust Service Practice Statement

Document Name	Paperless Trust Services - Trust Service Practice Statement
Abbreviation	TSPS
OID	1.3.6.1.4.1.64134.1.2.1
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 Trust Service Practice Statement (TSPS) of the Trust Service Provider (TSP) Paperless GmbH, describing its current practice in the provision of the qualified trust services described in Section 1.1.1.

These services are offered in an integrated fashion, with qualified timestamps only being issued for inclusion in electronic signatures & seals, and certificates only being issued when necessary for signing or sealing processes. These short-lived processes are initialized by API tenants (see Section 1.3.5.1) on behalf of a natural person, and executed interactively in a web-based environment.

All services are offered non-discriminatorily and provided in accordance with the requirements of eidas(), the German Vertrauensdienstegesetz (VDG) and Vertrauensdiensteverordnung (VDV), as applicable for everyone who is within the TSP's publicly declared field of operation and that agrees to abide by their obligations as specified in the TSP's terms and conditions.

The present document follows the structure outlined in RFC3647 [1], with some additions to incorporate timestamping and signing practices (e.g. subsections in Section 3 and Section 7 concerning signing and signatures).

For sections concerning the TSP's certification practice, this document may reference a relevant Certificate Policy (CP) or Certification Practice Statement (CPS). The current version of these documents is linked in Section 1.1.1. See Section 2 for information on the publication of these documents.

For certificates without their own CPS (including Certificate Authority (CA) & service certificates), the present document serves as CPS.

The present document includes the TSP's TSA and PKI Disclosure Statements. An outline of the relevant sections is given in Appendix A and Appendix B, respectively.

1.1 Overview

1.1.1 Provided Trust Services

1.1.1.1 Issuance of qualified signing certificates

ETSI CP: `QCP-n-qscd` as per ETSI EN 319 411-2 [2] / `0.4.0.194112.1.2`
TSP CP/CPS: CP/CPS (Qualified Signing) / `1.3.6.1.4.1.64134.1.2.2.1`

1.1.1.2 Issuance of qualified sealing certificates for production of qualified electronic seals

ETSI CP: `QCP-l-qscd` as per ETSI EN 319 411-2 [2] / `0.4.0.194112.1.3`
TSP CP/CPS: CP/CPS (Qualified Sealing) / `1.3.6.1.4.1.64134.1.2.2.2`

1.1.1.3 Issuance of qualified sealing certificates for production of advanced electronic seals

These certificates require the same identity verification steps as qualified sealing certificates for qualified seal creation, but the key does not reside in a Qualified Signature Creation Device (QSCD), meaning that only advanced electronic seals can be created.

ETSI CP: `QCP-l` as per ETSI EN 319 411-2 [2] / `0.4.0.194112.1.1`
TSP CP/CPS: CP/CPS (QCP-l Sealing) / `1.3.6.1.4.1.64134.1.2.2.4`

1.1.1.4 Remote creation of qualified electronic signatures

(using `QCP-n-qscd` certificates issued by the TSP)

1.1.1.5 Remote creation of qualified electronic seals

(using `QCP-l-qscd` certificates issued by the TSP)

1.1.1.6 Issuance of qualified timestamps

(using `best-practices-ts-policy` certificates as per ETSI EN 319 421 [3], issued by the TSP)

1.1.2 Application Infrastructure

The TSP operates all systems described in this document as a unified application deployed in at least two georedundant installations/nodes.

Each application node integrates CA, RA, OCSP, TSU, SSA, and SCA functions and features a service Hardware Security Module (HSM) for service and CA functions, and a QSCD for qualified signature & seal creation.

The machine accessible interface (API) to contact the services of the TSP does not use the protocol defined in ETSI TS 119 432, but is offered as a REST-compliant JSON API.

1.1.3 Public Key Infrastructure

The TSP operates a Public Key Infrastructure (PKI) for issuing qualified signing & sealing certificates (Section 7.1.5, Section 7.1.7, Section 7.1.6), as well as qualified timestamping certificates (Section 7.1.3).

The PKI consists of a single root CA and four intermediate CAs, one for each type of end-entity certificate.

A publicly-accessible OCSP responder is provided for each CA (see Section 4.10, Section 7.1.4).

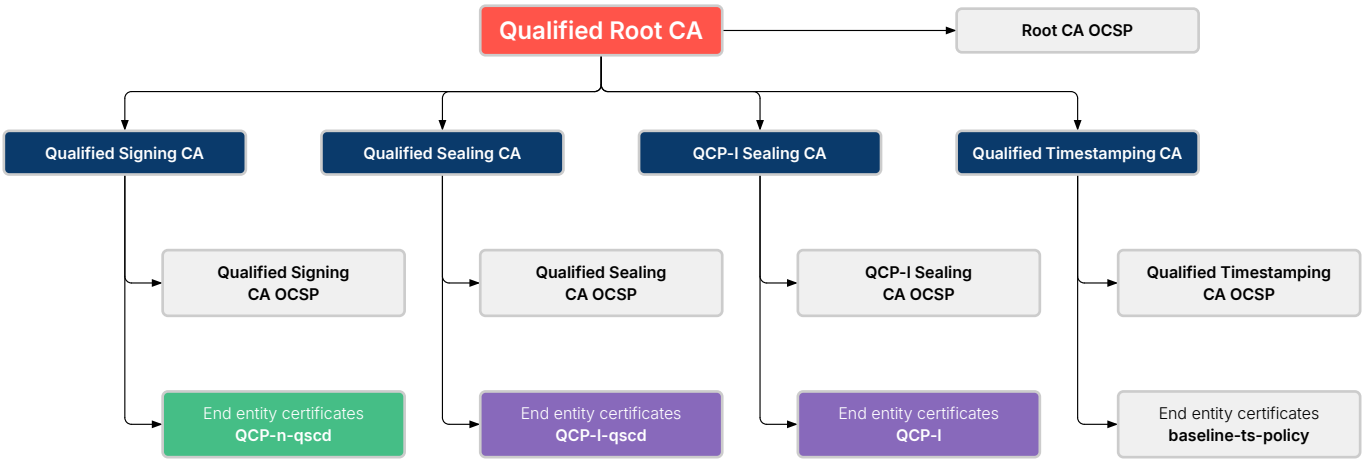

Figure 1: Structure of the PKI operated by the TSP. Certificates issued to natural person subjects are highlighted in green, those issued to legal person subjects in purple. Other certificates are issued to the TSP itself.

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 document regulates the relationships between the following parties:

- Certification Authorities
- Registration Authorities
- Subjects and subscribers
- Relying parties
- Other participants

Obligations and warranties of each participant are described in Section 9.6.

1.3.1 Certificate Authorities

The TSP exclusively operates a Public Key Infrastructure, consisting of the CAs and listed in Section 1.1.3.

1.3.2 Registration Authorities

The TSP uses external identity proofing service providers as the Registration Authority Services and operates its own internal Registration Authority.

The Registration Authority performs the following functions:

- Identifies the subscriber or subject who submitted a certificate request in accordance with the rules and procedures established by the TSP.
- Verifies the subject's identity at time of registration by appropriate means, collects and validates either direct evidence or an attestation from an authorized source, of the identity and if applicable, any specific attributes of subjects to whom a certificate is issued.

1.3.3 Subjects & Subscribers

The subject is the entity identified in a certificate as the holder of the corresponding private key. The subject may be a) a natural person, or b) a legal entity. The subject is the entity whose identity are bound to the certificate by the TSP.

The subscriber is the entity that enters into an agreement with the Trust Service Provider for the issuance of a certificate. The subscriber accepts the obligations defined by the TSP's Certificate Policy (CP) and Certification Practice Statement (CPS), authorizes the TSP to issue a certificate for a given subject and is responsible for the use and management of that certificate in accordance with the TSP's terms. The subscriber may be the same entity as the subject (for personal certificates), or a different entity acting on behalf of the subject, such as a legal representative applying for a certificate for a legal person (e.g. company seal).

Certificates that the TSP issues for itself or persons belonging to it (as a subject) are requested, validated and handled according to the TSP's defined processes for the selected type of certificates. The Registration Officer(s) that verifies the identity shall not be the natural person to whom the certificate is issued to (as a subject).

1.3.4 Relying Parties

Any natural person or legal entity that relies on the trust services the TSP provides is a relying party.

Obligations of Relying Partys (RPs) are described in Section 9.6.2.

1.3.5 Other participants

1.3.5.1 API Tenants

The TSP provides its services to API tenants, which are legal entities that integrate the TSP's trust services into their own applications and processes via API.

1.4 Certificate Usage

Signing and sealing certificates are only ever used for signing and sealing, as described in the relevant CPS.

The TSP holds the private keys on behalf of subjects for all signing and sealing certificates.

CA certificates are used exclusively by the TSP for signing subordinate certificates. OCSP responder certificates are used exclusively by the TSP for signing OCSP responses on behalf of a specific CA. Timestamping certificates are used exclusively by the TSP for signing qualified timestamps, which are embedded in electronic signatures.

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.

1.5.1 Policy approval procedures

The present document is approved by the management of the TSP. All changes to the present document must be approved by the management of the TSP.

The management of the TSP is responsible for ensuring the suitability of this document and that the present document is implemented.

This document and its related documents are reviewed annually by the management of the TSP.

1.6 Definitions and Acronyms

CA – Certificate Authority

CMS – Cryptographic Message Syntax

CP – Certificate Policy

CPS – Certification Practice Statement

CRL – Certificate Revocation List

DTBS – Data To Be Signed: The data structure which is actually cryptographically signed (after digesting), which contains the SDR

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

HSM – Hardware Security Module

IRT – Incident Response Team

NTP – Network Time Protocol

NTS – Network Time Security

OCSP – Online Certificate Status Protocol

OID – Object Identifier

PKI – Public Key Infrastructure

QSCD – Qualified Signature Creation Device

RO – Registration Officer

RP – Relying Party

SD – Signer's Document: The input document a subject wishes to sign, e.g. a PDF.

SDR – Signer's Document Representation: A digest of the SD, which is supplied to the Trust Service Provider by an API tenant.

SO – Security Officer

T&C – Terms and Conditions

TSA – Timestamping Authority

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 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/tsps.pdf
- https://repo.paperlesstrust.de/tsps.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

The steps and actions described in this section take place in interaction with the subscriber using a self-describing web-based interface, where the subscriber is interactively guided through the process and the required identity verification and authentication steps in order to authorize operations described in Section 4.

3.1 Naming

This is documented in the relevant CPS.

3.2 Initial Identity Verification

All activities performed by users in interaction with the TSP (identity verification, certificate issuance, signing, sealing, etc.) are performed as part of specific processes associated with an account belonging to a natural person. This account may be associated with multiple identity verification results or signing certificates, or authorized to produce seals on behalf of legal entities.

The only way to create such an account is the creation of a signing or identity verification process by an API tenant. During the creation of a signing process, the subject is identified by email address. If no account associated with the requested email address exists, an account is automatically created. Upon opening the web interface of the signing process, the user is guided through the following authentication steps.

3.2.1 Email Verification

All interactions with the TSP by subscribers require a verified email address. The email address is used as primary contact for the subscriber.

If performed by the TSP, this verification is achieved by delivering a URL containing a unique, cryptographically pseudo-random token of sufficient length via email. Verification can only be completed by exchanging this token for a session cookie, which can only be done once per token.

The responsibility for performing this verification and delivering a process token to the owner of the email address may be delegated to the tenant requesting the process. This may be desirable if the signing process is part of a larger process which implements an equivalent email verification scheme.

3.2.2 Identity Verification

This is documented in the relevant CPS.

3.2.3 Authentication Token Creation

After any successful identity verification step, the user may be prompted to create an authentication token if no non-revoked tokens are associated with the user already. The user may choose between Webauthn Passkeys or a TOTP token. The TSP encourages the use of Passkeys.

This allows reusing identity verifications and certificates created during one process and sessions in future processes and sessions (see Section 3.3.1).

In case access to the configured authentication tokens is lost, the token may be revoked using a publicly-accessible account revocation form (see Section 4.9.1.1). This also revokes all certificates and identity verifications associated with the account.

3.3 Identification and Authentication for Signing & Sealing

These identification and authentication steps are performed in order to produce an electronic signature as a natural person, or an electronic seal on behalf of a legal person.

3.3.1 Authentication

If the account associated with the signing or sealing process is associated with any non-revoked authentication token, a successful authentication is required before continuing.

If the token was created in the same process and session (e.g. during the first signing process), this step is ommitted.

3.3.2 Sealing Authorization

No sealing authorization is required in signing processes.

In order to electronically seal on behalf of a legal person subject, a natural person must be authorized to do so.

During the enrollment of a legal entity subject the identity of both the legal entity subject and a set of natural persons initially authorized to produce seals is verified as per Section 3.2.2.

These authorized sealers may then optionally be able to authorize other natural persons in a hierarchical manner similar to a PKI without manual TSP intervention, or revoke previously issued authorizations. These authorization and revocation processes require authentication equivalent to that required for production of a seal.

Sealing requires a valid, non-revoked sealing authorization. If a sealing authorization was issued by another authorized sealer, the sealing authorization is only considered valid if the sealing authorization of the authorizing sealer is considered valid.

Revocation of a sealer's sealing authorization revokes all authorizations issued by the sealer.

3.3.3 Certificate Usage or Re-key

A previously issued certificate (and associated keypair) may be used for signing/sealing if it:

- is of the required profile for the signature/seal to be produced; and
- is associated with the natural person intending to create the signature in case of signing processes or a legal entity the user is authorized to produce seals on behalf of in case of a sealing process; and
- has not been revoked; and
- has not expired and will not expire until the expiration date of the present signing/sealing process (24h after creation); and
- was created either:
    - during the current process and session; or
    - in an earlier process or session, and the user has authenticated themselves during the current session using a non-revoked authentication token.

If no usable certificates are available, the user is prompted to create a new certificate, which may require additional identification (see Section 3.4).

3.4 Identification and Authentication for Re-key Requests

These identification and authentication steps are performed if a new signing certificate has to be issued to a natural person.

3.4.1 Authentication

As described in Section 3.3.1.

3.4.2 Sealing authorization

No sealing authorization is required for rekeying as part of signing processes.

For sealing processes, the personal account associated with the sealing process needs to be authenticated and authorized to the same level as required for seal production (see Section 3.3.2).

3.4.3 Signature Activation

For some subject keys, additional authentication steps are performed and activation data collected, as described in Section 6.4 of the relevant CPS.

3.4.4 Identity Verification

No identity verification is required for rekeying as part of sealing processes.

For signing processes, previous identity verification results ("identity attestations") may be reused if they fulfill the following criteria:

- Are of the required quality for the type of certificate required (see Section 3.2.2 and the relevant CPSs)

- The identity attestation has not expired (see Section 3.2.2/CPSs for semantics of identity verification result expiration)
- The identity attestation has not been revoked
- The identity attestation was either:
  - created during the current process and session, or:
  - created in an earlier process or session, and the user has authenticated themselves during the current session with a non-revoked authentication token (see Section 3.3.1).

If no identity verification results can be reused, identity verification is performed as described in Section 3.2.2.

3.5 Identification and Authentication of Revocation Requests

These identification and authentication steps are performed if a subscriber wishes to revoke a certificate or their entire account.

3.5.1 Single Certificate Revocation

Users may – as part of an active signing or sealing process – choose to revoke a specific certificate if data contained in the certificate is found to be incorrect, or if activation data specific to the certificate was lost or compromised.

This option is available to natural persons authenticated to same level required to use the certificate in question for signing, or authorized to use use the certificate in question for sealing (see Section 3.3).

3.5.2 Personal Account Revocation

If data associated with a natural person's account was lost or compromised (such as a lost authentication token), natural persons may revoke their account using a publicly available form. This requires an email confirmation as described in Section 3.2.1. Second factor authentication is not required.

3.5.3 Other Circumstances

For received revocation requests that can not be resolved automatically, TSP Registration Officers (ROs) confirm the identity of the entity requesting the revocation using a method described in Section 3.2.2 of the relevant CPS.

4 Certificate Life-Cycle

The TSP maintains a database of its issued certificates throughout their life-cycle and keeps the database updated according to certificate status.

The steps and actions described in this section take place in interaction with the subscriber using a self-describing web-based interface, where the subscriber is interactively guided through the prerequesite steps described in Section 3 before guiding the subscriber through certificate issuance, revocation or key usage steps. The TSP ensures that the user interface is well designed and easy to use to avoid any problems and misunderstandings. The the user is provided with sufficient information to understand the process of generating, augmenting and validating the signature.

4.1 Certificate Application

No manual or explicit certificate applications by subjects are offered.

Instead, the need for and lack of a usable certificate during a signing or sealing process (see Section 3.3.3) is considered to constitute a certificate application.

Before conducting any identification, authentication or certificate issuance, the subscriber needs to accept the terms and conditions of the TSP and the subscriber agreement. For legal person subjects this authorizes the issuance of certificates on behalf of the legal person (see Section 3.2.2 in CPS).

4.2 Certificate Application Processing

Certificates are exclusively and automatically issued after the TSP checked the request is accurate, authorized and complete as part of running signing or sealing processes after all required authentication and identity verification steps have been completed successfully (see Section 3).

The certificate subject name is constructed as described in Section 3.1 of the relevant CPS, using the latest available identity verification result.

The process used for initial verification of the subject's identity and attributes must still be an applicable process for identity proofing as at the time issuing the certificate.

4.3 Certificate Issuance

After the required authentication and identity verification steps have been completed successfully, the TSP generates a keypair on behalf of the subject and issues the required certificate.

No certificates are issued which exceed the lifetime of the TSP's signing certificate. For details on validity periods, see the corresponding CPS.

The TSP provides the capability to check and test all the certificate types that the TSP issues. For that, the production environment is used for testing purposes with real data and full adherence to the applicable certificate policy. Certificates issued for testing are revoked immediately upon completion of the tests.

4.3.1 Key Generation

This is documented in the relevant CPS.

4.3.2 Certificate Signing

After key generation, a certificate is issued by the TSP and signed by the appropriate CA (see Section 1.1).

The certificate is stored in the TSP's database and associated with the keypair and account associated with the running signing or sealing process. The generated key is only used in conjunction with the issued certificate for signing or sealing operations.

4.3.3 Certificate Notification

Certificates are only issued as part of running signing or sealing processes. After successful issuance, the certificate is immediately presented to the subscriber.

No further issuance notification is performed.

4.4 Certificate Acceptance

Since certificates are only issued during signing or sealing processes, the subscriber is immediately presented a confirmation dialog to determine whether the certificate may be used for signing or sealing.

This confirmation dialog displays the subject name attributes included in the certificate and allows the subscriber to download the certificate.

If information in the certificate is discovered to be incorrect, the subscriber may choose to revoke the certificate (and the identity verification result used for naming, see Section 4.9.1.2).

A failure to do so is deemed to constitute acceptance of the certificate.

4.5 Key Pair and Certificate Usage

After certificate generation, the subscriber is shown a confirmation dialog which allows the subscriber to inspect the Signer's Document Representation (SDR) supplied to the TSP and a link to download the original Signer's Document (SD) supplied by the API tenant responsible for starting the process.

The subscriber is shown all usable certificates for the current process and after explicit confirmation with which certificate they wish continue with the signature or seal creation process, the TSP constructs the Data To Be Signed (DTBS) for the signature and signs the Data To Be Signed Representation (DTBSR) using the key associated with the certificate chosen by the subscriber in the confirmation dialog. For details regarding the required signature activation data, see Section 6.4 of the relevant CPS. The TSP systems ensure the correct DTBS, certificate, key are used by storing records within a relational database with ACID properties using appropriate transaction isolation levels and referential integrity constraints like foreign keys.

4.6 Certificate Renewal

Certificate renewal is not offered for subject signing & sealing certificates.

The TSP may renew its own CA and service certificates as described in Section 5.6.

4.7 Certificate Rekey

Certificate rekeying (i.e. the issuance of a new certificate, including a new key, to a person who has previously been issued a certificate) is performed identically to the initial issuance described in Section 4.3.

Certificate rekeying is performed if no previously issued certificate is usable for the present process, for instance due to expiration or revocation. No attributes are reused from the previously issued certificate, all certificate attributes (including names, serial number and expiration date) are determined as for a newly issued certificate.

No previously issued certificates are used to authenticate the request.

The TSP may rekey its own CA and service certificates as described in Section 5.6.

4.8 Certificate Modification

No certificate modification is performed.

If the information contained in the certificate becomes incorrect, e.g. due to a name change, the certificate will have to be revoked by the subscriber. The subscriber may request this either during a running signing process (when presented with the certificate to be used, see Section 4.9.1.2) or preventively at any time (see Section 4.9.1.1).

4.9 Certificate Suspension & Revocation

All end-entity certificates issued to subjects, including short-term ones, may be revoked. No “validity assured” certificates are issued.

Revocation request by subjects or third parties are checked to be from an authorized source as per Section 3.5. After successful authentication and authorization, the status of the certificates, including the revocation date, is recorded in the certificate database immediately and propagated to the OCSP responders within at most 15 minutes. (see Section 4.10).

All revocations are final, no suspensions (temporary revocations) are offered.

4.9.1 Revocation by Subject

4.9.1.1 Personal Account Revocation

If a (natural) person believes or suspects that a credential used to access their account or a certificate, such as an authentication token or signature activation PIN may have been lost, misused or compromised, they may request a revocation using a publicly accessible form using their email address.

Upon successful authentication (see Section 3.5.2), they are prompted to give a reason and – if known – a revocation date, asked to confirm the account revocation and informed of the consequences. Upon confirmation:

- All signing & sealing certificates the account had access to with expiration dates after the given revocation date are marked as revoked, immediately preventing further signatures.
- All identity verifications associated with the account are revoked, immediately preventing the issuance or renewal of certificates utilizing these identity verifications.
- All sealing authorizations associated with the account, and all their descendant authorizations are revoked. This immediately prevents all sealing processes associated with the account, or other accounts authorized by the account, from continuing.
- All two factor tokens associated with the account are revoked.

This leaves the account in a state comparable to a new account, requiring new identity verification and certificate issuance for further signing.

The reason given by Online Certificate Status Protocol (OCSP) responders for these revocations is `keyCompromise` or `cessationOfOperations` as per RFC5280 [4].

4.9.1.2 Single Signing Certificate Revocation

If a single signing certificate issued to a natural person contains an error or a mistake, e.g. if data was entered incorrectly during the identity verification or certificate issuance process, or if the information is no longer correct, such as in case of a name change, the subscriber may choose to revoke the certificate before signing. The subscriber is prompted to select a reason for revocation: either `keyCompromise` (if signature activation data was lost or compromised) or `superseded` (in case information was corrected), as per RFC5280 [4].

After successful revocation of the certificate, the subscriber will be prompted to create a new certificate, where the error may be corrected (see Section 4.3).

4.9.1.3 Legal Entities & Other Circumstances

If a person authorized to produce seals on behalf of a legal person suspects their account or signature activation data associated with a sealing certificate may have been compromised, they are encouraged and obliged to revoke their (personal) account as described in Section 4.9.1.1. This triggers a revocation of all sealing certificates the subscriber had access to. No automated mechanism is offered to revoke single sealing certificates for correction purposes, as the information contained therein does not change without manual intervention by the TSP.

For such a case, as well as other circumstances that are not satisfyingly covered by the mechanisms described above, e.g. the compromise of the email adress associated with an account, revocation requests may be sent via email to support@paperless.io or to the postal address of the TSP. These revocation requests are handled by a trained RO, responsible for confirming the authenticity of the request.

The steps taken by TSP personnel during this process are recorded. The TSP endeavour to confirm any revocation request within 24 hours. Should that not be possible, the reason is recorded.

4.9.2 Revocation by the TSP

The TSP is committed to revoke any non-expired certificate if it is no longer compliant with the certificate policy under which it was issued, based on cryptography that is no longer fit for purpose, or if the TSP is made aware of misuse by authorities or other third parties. This includes both end-entity certificates issued to subjects, as well as service & CA certificates used by the TSP itself. Potential revocation reasons include: `superseded`, `keyCompromise`, `cessationOfOperations` or `caCompromise`.

Should the algorithms or parameters used become insufficient for the remaining usage period of any key or certificate, the revocation of the affected certificates will be scheduled and subscribers and relying parties informed in advance.

In the event end-entity certificates are revoked by the TSP, the affected subjects & subscribers are notified by email.

As described in Note 1, OCSP responder certificates can not be checked for revocation using OCSP. For intermediate OCSP responders (which do not offer an alternative revocation method such as a Certificate Revocation List (CRL)), the TSP is committed to revoke the issueing CA whenever the OCSP responder's certificate requires revocation.

4.10 Certificate Status Services (OCSP & CRLs)

The TSP operates at least two georedundant OCSP responders as per RFC6960 [5] for all CAs (roots & intermediates). These responders are publicly and internationally available free of charge, 24 hours a day, 7 days per week. In the case of disruption, the trust provider endeavours that service is restored within at most 4h.

The revocation status of all subject signing & sealing, timestamping, and intermediate CA certificates may be checked using the OCSP responder indicated in the certificate (see Section 7.1).

OCSP responder and root CA certificates can not be checked for revocation using OCSP. For OCSP responders responding on behalf of intermediate CAs, the TSP is committed to revoke the issueing CA's certificate if the responder's certificate requires revocation.

For each root CA, the TSP maintains a CRL containing the serial numbers of revoked root CA OCSP responders. The CRL is publicly available to the same standard as the OCSP responders, at a location indicated in the root OCSP responder certificate (see Section 7.1).

All certificates issued by the TSP are only ever checkable for revocation using at most one method (via an OCSP responder or using a CRL), never both.

Certificate status information is securely transmitted to and synchronized with the OCSP responders via an authenticated and encrypted channel. OCSP responses are cryptographically signed using a keypair residing in a suitable HSM (see Section 6.2) and a certificate issued by the issuing CA. The nonce extension described in RFC6960 [5] is supported.

Root OCSP responder CRLs are signed under dual control by trusted personnel, using the offline root CA key. This process is carried out as part of a documented procedure at least yearly, and whenever necessary due to a revocation, with a `nextUpdate` of at most 1 year after the issuing date.

OCSP responders and CRLs are available for at least 10 years after the end of the validity of the CA's certificate. The time used for the generation of OCSP responses is kept synchronized with UTC to the same standard as the TSP's timestamping facilities (see Section 6.8). For non-issued certificates, the OCSP responders respond with a "revoked" status as per the extended revocation definition found in RFC6960 [5]. Requests for non-issued certificates are logged and the frequency of such requests monitored.

The currently operational OCSP responders are available at the following locations:

OCSP Responder for Qualified Root CA:

- http://qualified-root-g1.ocsp.trust.paperless.io
- http://qualified-root-g1.ocsp.paperlesstrust.de

OCSP Responder for Qualified Signing CA:

- http://qcp-n-qscd-ca-g1.ocsp.trust.paperless.io
- http://qcp-n-qscd-ca-g1.ocsp.paperlesstrust.de

OCSP Responder for Qualified Sealing CA:

- http://qcp-l-qscd-ca-g1.ocsp.trust.paperless.io
- http://qcp-l-qscd-ca-g1.ocsp.paperlesstrust.de

OCSP Responder for QCP-l Sealing CA:

- http://qcp-l-ca-g1.ocsp.trust.paperless.io
- http://qcp-l-ca-g1.ocsp.paperlesstrust.de

OCSP Responder for Qualified Timestamping CA:

- http://qualified-tsa-ca-g1.ocsp.trust.paperless.io
- http://qualified-tsa-ca-g1.ocsp.paperlesstrust.de

4.11 End Of Subscription

If a subject or subscriber wishes to end the use of the TSP's services before the expiration of their certificate, they may choose to revoke their account as described in Section 4.9.

4.12 Key Escrow & Recovery

All subject keys are held by the TSP on the subjects behalf. No additional key escrow or recovery functionality is offered.

5 Facility, Management, and Operational Controls

In the area of security management, the TSP aligns its practices with internationally recognized standards, in particular ISO/IEC 27001, as well as with all standards mandated by applicable laws and regulations.

The TSP maintains an Information Security Policy governing all aspects of information security relevant to its trust services. The policy is subject to regular review as defined in the Trust Services Schedule document (at least annually), and additionally whenever significant changes occur, to ensure its continued suitability, adequacy, and effectiveness, as well as to ensure that the TSP's configuration and practices match the policy. Responsibility of the content for the Information Security Policy, lies with the designated SOs. TSP's management approves, oversees and ensures that the Information Security Policy is effectively communicated and made known throughout the organization. Supervisory bodies are notified by management at least one month before implementing any change and three months before planned cessation.

The TSP conducts regular risk assessments to identify, analyze, and evaluate risks associated with trust services, considering both business and technical aspects. Based on the results, suitable risk treatment measures proportionate to the identified risks are determined, documented, and implemented in accordance with TSP's Information Security Policy and this document within the Risk Assessment document of the TSP. A residual risk analysis is also performed and documented, ensuring that any remaining risks are explicitly identified and, where appropriate, formally accepted. Risk assessments are carried out as defined in the Trust Services Schedule document of the TSP and are formally approved by TSP's management body.

The TSP maintains a Asset Management Policy which ensures a detailed inventory of assets, each classified in accordance with the results of the risk assessment exist. The policy is reviewed at intervals defined in the Trust Services Schedule document and additionally whenever significant changes occur, to ensure its continued suitability, adequacy, and effectiveness.

5.1 Physical Security Controls

The TSP maintains a Physical and Environmental Security Policy which has been audited by a recognized conformity assessment body and defines the physical security measures to protect the TSP's facilities, systems, and equipment against unauthorized access, damage, and interference in accordance with applicable requirements from ETSI EN 319 401 [6], ETSI EN 319 411-1 [7], ETSI EN 319 421 [3] and Regulation (EU) 910/2014[8] as amended by Regulation (EU) 2024/1183[9] ("eIDAS 2.0").

The TSP servers providing trust services are located in at least two geo-redundant commercial data centers that

- meet the requirements of ETSI EN 319 411-1 [7].
- are ISO 27001 certified.
- are reviewed by a qualified auditor on every re-certification of the TSP.

Root CA keys are held physically isolated from normal operations and require multiple designated TSP employees in authorized roles to access or use.

5.2 Procedural Controls

Access to TSP hardware and software systems is managed based on the "least privileges" principle and require strong identification & authentication of authorized TSP personnel, incl. multi-factor authentication. Access by a given TSP employee is limited to the level necessary for the execution of the designated roles of the employee.

Access rights are reviewed regularly and when required as part of organisational or personnel changes. All changes are reviewed and documented. All accesses and activities by TSP personnel on production systems are logged.

Intermediate CA certificate issuance using the root CA keys is only possible under dual control by two sufficiently authorized TSP employees. The same applies for the restoration of HSM backups (the installation of existing intermediate CA keys into an HSM), and the creation of new backups of HSMs holding CA key material.

5.3 Personnel Controls

The TSP fulfills the requirements for personnel from ETSI EN 319 401 [6], ETSI TS 119 431-1 [10], ETSI TS 119 431-2 [11], ETSI EN 319 411-1 [7], ETSI EN 319 411-2 [2] and ETSI EN 319 421 [3]. The TSP maintains an internal personnel security policy that defines the requirements for personnel in trusted roles.

If the TSP or its employees apply for a certificate, all processes and controls and described in this document or the corresponding CPSs apply without exception, including identity validation.

5.3.1 Qualifications, Experience, and Clearance Requirements

The TSP ensures that all personnel in trusted roles possess the necessary expertise, qualifications, experience, and reliability to support the trustworthiness of operations. Personnel are free from conflicting commercial or financial interests that might impair impartiality.

Trusted role holders and subcontractors are trained in applicable security and personal data protection rules as appropriate for the service and job function. Records documenting personnel qualifications and training are maintained and made available to supervisory bodies upon request.

The reliability of employees is determined from required documents including, but not limited to, certificates of conduct, education certificates, creditworthiness information, curriculum vitae, and confirmations of education and prior employment. Each entry in a certificate of conduct is reviewed individually by the Head of Trust Service Provider for approval or rejection. If a country does not issue certain forms of verification (e.g. certificate of conduct), alternative measures providing equivalent assurance are applied.

Before starting work at the TSP, new employees sign confidentiality agreements and independence statements. Management acquires and maintains sufficient knowledge and experience in relation to the trust services offered, including risk assessment and safety procedures.

5.3.2 Personnel Verification Procedures

The TSP verifies the background and identity of personnel in trusted roles prior to granting access. This includes: Confirmation of identity, confirmation of previous employment, verification of recommendations, confirmation of educational degrees, verification of criminal records.

Background checks are repeated at least every two years. The TSP does not appoint any person known to have been convicted of a serious crime or other offense that could affect suitability for the role. No personnel are granted access to Trusted Functions before completion of all required checks.

5.3.3 Training Requirements

The TSP ensures that all personnel in trusted roles have adequate knowledge, training, and experience for their duties as described in role descriptions and employment contracts. Training covers, at a minimum:

- Regulations, procedures, and documentation related to the occupied position
- Responsibilities arising from assigned roles and tasks
- Information security policies
- Personal Data Protection
- Disaster recovery procedures
- Security controls and processes implemented by the TSP, including CA operations

5.3.4 Training Frequency and Retraining Requirements

Initial training is provided prior to assuming a role. Regular and event-driven retraining is performed to maintain competence. Retraining occurs as required by organizational or individual needs, at least once per year, and whenever there are significant changes to the Practice Statement, Certificate Policy, information security policy, or new threats and security practices.

5.3.5 Job Rotation Frequency and Sequence

The TSP documents and performs job rotation of employees as necessity arises, based on organizational needs or employee request. No fixed frequency is mandated; changes of roles are recorded.

5.3.6 Sanctions for Unauthorized Actions

All personnel are bound by contractual obligations to perform duties according to internal rules and applicable policies. Violations are subject to disciplinary sanctions, up to and including termination of employment or contract. The TSP reserves the right to exclude unreliable employees from certification-related activities and to prosecute unauthorized actions to the fullest extent of applicable law.

5.3.7 Contracts with Personnel and Independent Contractors

Independent contractors and their personnel are subject to the same privacy protection, confidentiality, and verification requirements as employees. Contracts include explicit obligations of confidentiality, independence, and compliance with all TSP policies. Contractors applying for access, operations, or audit roles must provide proof of qualifications equivalent to internal personnel, demonstrate a clean criminal record, and sign confidentiality and independence statements.

5.3.8 Documentation Available to Personnel

The TSP provides all relevant personnel with access to current documentation necessary to fulfill their roles, including:

- this document and related Certificate Policies
- All internal policies and procedures, including the Information Security Policy and topic specific policies
- System documentation
- Emergency and disaster recovery procedures;
- Description of responsibilities and obligations associated with the role

On their first day of work, employees receive an introduction and access to security policies, security concepts, workspace security rules, and risk management documentation. All personnel are required to read and understand these documents during their onboarding. Changes to security-relevant documentation are communicated to all employees, and awareness is refreshed in recurring annual trainings.

5.4 Audit Logging Procedures

The TSP systems log all events in association with the trust services. The logs at appropriate locations (databases, log files, logging systems) and are kept accessible as defined in the internal Evidence Retention Policy document of the TSP event after the activities of the TSP have ceased, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service taking into consideration the confidentiality and integrity of current logs.

5.5 Records Archival

The TSP ensures that all records related to data issued or received are archived in accordance with documented processes and procedures. The archiving process safeguards the confidentiality, integrity, and availability of all retained records throughout their defined retention period.

Records relating to the operation of trust services are retained to provide evidence of correct and compliant service operation and is made available upon lawful request, including for the purpose of legal or regulatory proceedings.

Back-up copies of all essential information and software are created on a regular basis to ensure continuity of operations. The backups enable the TSP to recover essential data and software following a disaster or media failure. The effectiveness of back-up and recovery arrangements is verified through periodic testing.

The TSP maintains an internal Evidence Retention Policy which defines the detailed retention periods for all records.

Requests for information may be submitted through the contact channels specified in this document. The TSP verifies the requester's authorization prior to the disclosure of any information.

5.6 Key Changeover

CA and service keys are rotated as described in Section 6.1.

5.7 Compromise and Disaster Recovery

The TSP maintains a comprehensive Incident Response Policy that defines the processes for detecting, reporting, managing, and recovering from security incidents, compromises, or disasters. The policy forms the integral part of the TSP's incident response management.

All TSP personnel are trained and authorized to declare incidents. Upon declaration, an Incident Response Team (IRT) is convened to coordinate containment, eradication, and recovery activities.

If a compromise of a trust service, certificate, or cryptographic key is suspected or confirmed, the IRT executes the corresponding documented recovery procedure without undue delay. This includes notifying supervisory bodies, affected subscribers and relying parties, and publishing revocation information as required.

All incidents and corresponding response actions are recorded in the internal tracking system and reviewed following closure to identify root causes, verify corrective measures, and prevent recurrence.

5.8 CA, RA or TSA Termination

The TSP has a termination plan in case of cessation of the company operations.

Before the TSP terminates a CA Service, the following procedures will be executed:

- Information of the Supervisory Body at least three months in advance
- Information of all subscribers and subjects and other entities with whom the TSP has established relations at least two months in advance
- Information of the public by publishing a notice on the website at least one month in advance
- Making arrangements with other Trust Service Providers to transfer the provision of services for its existing customers
- Revocation of all CA and TSA certificates
- Destroying the CA and TSA private keys, including backup copies or keys withdrawn from use in such a manner that they cannot be used or retrieved
- Secure disposal or destroying or zeroization of any hardware appliances related to the TSPs trust services
- Termination of subcontractor contracts related to the process of issuing qualified certificates

The TSP tries to reduce potential disruptions as a result of the cessation of its Trust Services.

The TSP has arrangements to finance all requirements in case of bankruptcy, or for any other financial gaps.

The issued certificate databases, together with the revocation information (including revocation status for unexpired certificates) and PKI infrastructure certificates, are transferred to the reliable party authorised by the Supervisory Body.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

CA and service (OCSP and timestamping) keys are generated in a physically secured environment (see Section 5.1) by trusted personnel (see Section 5.3). CA and timestamping key pairs are created using a 2-of-4 quorum, according to a defined procedure. Root CA key material is kept offline and in a secure location only accessible to trusted personnel. It is only retrieved when required for the issuance of CA & OCSP certificates, as well as CRL generation, as part of documented procedures.

A report stating that the key generation ceremony was carried out correctly and in accordance with the defined procedure is produced during the ceremony and includes:

- The time and date of the ceremony
- The personnel involved, their roles and responsibilities
- The steps performed during the ceremony
- A complete list of the generated keys, the algorithms used and SHA256 public key fingerprints.
- A complete list of the cryptographic devices used and their configuration

This report is signed by the TSP's security officer and – for ceremonies which include the generation of root CA key material – one or more trustworthy persons independent of the TSP who witnessed the key generation ceremony and can attest to its correct execution.

The algorithms and key lengths used for generating keys, hashes or signatures are selected from algorithms appropriate for the lifetime of the key, compliant with ETSI TS 119 312 [12] and the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA [13].

An appropriate time before the expiration of a CA certificate (at least the maximum validity duration of a certificate profile issued by the CA), the TSP will issue a new certificate according to the same procedures described above.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

This section of the present document describes the protection of keys associated with certificates issued to the TSP. For keys managed on the behalf of subjects, see the relevant CPS.

All key generations and uses are carried out in a secure cryptographic device (HSM compliant with NIST CMVP FIPS 140 2 level 3 (at least) or according to Common Criteria EAL4 augmented by AVA_VAN.4 (at least)), which is operated in a physically secure environment, in accordance with both the general and eIDAS-specific guidance published by the manufacturer.

CA and service keys only leave the cryptographic modules they are generated in as part of encrypted backups taken during the key generation ceremony. These backups are stored on dedicated backup HSMs providing integrity protection, in accordance with manufacturer compliance guidance. These backup HSMs are kept in a physically secure, offline location and only retrieved as part of documented procedures when needed. Encryption and decryption of the key material takes place inside the cryptographic module used for key generation and use. Restoration (installation of the key material into a HSM) requires at least two sufficiently authorized TSP employees. The number of TSP employees authorized to do this is kept to the minimum required to ensure timely and reliable access when needed.

In addition to the general tamper protection provided by the HSM, secure transport modes are used during transport or storage of any HSM in accordance with manufacturer guidance to further prevent unauthorized use and tampering. The information required to recover HSMs from transport mode is not transported together with the physical HSM.

Before retiring a cryptographic device, all contained keys are destroyed and the device is zeroized and decommmissioned as per manufacturer guidance, ensuring that it is impossible to recover any contained keys.

6.3 Other Aspects of Key Pair Management

All private keys that are no longer needed, due to certificate revocation (including those requested by the subject) or expiration, or if the private key's usage period has ended, are destroyed to prevent continued use. This includes all online copies and – after appropriate retention periods – backups.

All keys are only used for a single purpose:

- Root CA keys are only ever used for signing intermediate CA and OCSP responder certificates and root OCSP responder CRLs
- Issuing/intermediate CA keys are only ever used for signing end-entity and OCSP responder certificates
- OCSP responder keys are only ever used for signing OCSP responses
- Timestamping keys are only ever used for signing qualified timestamps
- Subject signing keys are only ever used for signing
- Subject sealing keys are only ever used for sealing

No keys are ever used outside of an appropriate cryptographic device operated in a physically secure environment (see Section 6.2 and Section 5.1).

6.4 Activation Data

This is documented in the relevant CPS.

6.5 Computer Security Controls

6.6 Life Cycle Security Controls

6.7 Network Security Controls

The TSP maintains an internal Network Security Policy.

The TSP maintains integrity and confidentiality of all information supplied by the user and of any data flowing between the application and the user.

6.8 Timestamping

The TSP operates a timestamping unit as per ETSI EN 319 422 [14]. Timestamps are issued exclusively for use in signature containers as described in Section 7.2. No publicly accessible time-stamping service is provided.

All timestamps are sealed using a single key generated by the TSP exclusively for this purpose as described in Section 6.1 and a single certificate as described in Section 7.1.3, issued by the TSP. All timestamps issued are qualified timestamps as per Regulation (EU) 910/2014[8] as amended by Regulation (EU) 2024/1183[9] ("eIDAS 2.0"). As described in Section 7.1.3, timestamping certificates include the `privateKeyUsagePeriod` extension, limiting the usability of the private key. No timestamps are issued after the private key associated with the issuing certificate has reached the end of its lifetime, and a new key is generated and certified sufficiently early before this date to ensure service continuity.

The clock used for the issuance of timestamps is kept synchronized with UTC as distributed by the Physikalisch-Technische Bundesanstalt (or an equivalent UTC(k) laboratory as identified by the BIPM's Circular T[1] using the Network Time Protocol (NTP) as per RFC5905 [15] & Network Time Security (NTS) as per RFC8915 [16]. The minimum polling interval is at least hourly.

Clock synchronization is monitored and no timestamps are issued if clock synchronzation to the stated accuracy in the timestamp (see Section 7.3) can not be guaranteed. Leap seconds are inserted at the end of the last minute of a month in UTC. Leap second occurences are logged.

The TSP's system for quality and information security management is appropriate for the time-stamping services it is providing.

[1] https://www.bipm.org/en/time-ftp/circular-t

7 Certificate, Signature, Timestamp, OCSP Response & CRL Profiles

The format and content of the cryptographic objects produced by the TSP are described below. All name attributes and extensions included are described below, with all attributes and extensions present at most once and – unless explicitly described as optional or conditional – exactly once.

7.1 Certificate Profiles

All certificates issued by the TSP are X.509 [17] certificates, adherent to RFC5280 [4] and the relevant certificate profiles.

The exact content of each type of certificate issued by the TSP is given in the tables contained in the sections below. For certificates issued to subjects, the relevant information is contained in the relevant CPS. For certificates issued to the TSP itself, the present document serves as the CPS.

If a profile is changed in a way that it affects the applicability the policy identifiers contained in the certificates are changed accordingly.

No size limits of the kind described in RFC5280 [4] are imposed on any name attributes.

7.1.1 Root CA Certificates

Issued to the TSP and used for signing intermediate CA & OCSP responder certificates as well as root OCSP responder CRLs. The key is kept in a physically secure offline location under at least dual control.

Attribute	Value
`version`	V3 (`0x2`)
`serial_number`	Cryptographically random & unique 128-bit number
`issuer`	See Table 2.
`subject`	See Table 2.
`validity`	20 years
`signature`[2]	EC (`1.2.840.10045.2.1`), NIST P-521 curve (`1.3.132.0.35`)
`subject_public_key_info`	See Section 6.1 for details on key generation.
`extensions`	See Table 3.
`signature_algorithm`	ECDSA w/ SHA512 (`1.2.840.10045.4.3.4`)
Signed by	self-signed

Table 1: Attributes of root CA certificates

Name	OID	Value
`countryName`	`2.5.4.6`	`"DE"`
`organizationName`	`2.5.4.10`	`"Paperless GmbH"`
`organizationalUnitName`	`2.5.4.11`	`"Paperless Trust"`
`organizationIdentifier`	`2.5.4.11`	`"NTRDE-DEM1201.HRB118617"`
`commonName`	`2.5.4.3`	`"Paperless Trust Qualified Root CA G{i}"`

Table 2: Subject name attributes used in root CA certificates

[2] Algorithm identifier for signed public key, referred to simply as `signature` by RFC5280 [4].

Name	OID	Notes	Crit.
subjectKeyIdentifier	2.5.29.14	Calc. as per RFC5280 [4, 5.2.1.2]	
basicConstraints	2.5.29.19	CA == true, no pathLenConstraint	×
keyUsage	2.5.29.15	keyCertSign | crlSign	×
cRLDistributionPoints	2.5.29.31	• http://qualified-root-g{i}.crls.trust.paperless.io/root.crl • http://qualified-root-g{i}.crls.paperlesstrust.de/root.crl	

Table 3: Extensions included in root CA certificates

7.1.1.1 Issued Certificates

Common Name	**Paperless Trust Qualified Root CA G1**
Issued By	Paperless Trust Qualified Root CA G1
Certificate Serial Number	151230755675870799585644096373040895605 / 71:c5:fb:ed:1d:98:13:27:0d:a1:fe:c8:13:1c:56:75
Public Key SHA-256	42:d8:00:57:fe:4f:08:28:8e:6d:36:a1:51:09:c0:a6 f2:ad:26:de:b7:ee:5c:af:5a:8d:be:9f:e6:02:45:2a
Certificate SHA-256	47:09:86:15:f6:6a:1d:f3:9c:a4:50:a1:59:f6:cb:81 93:27:c7:f6:38:cf:85:18:91:da:c8:d7:2d:28:f4:f7
Validity (UTC)	2026-01-22 12:07:24 - 2046-01-17 12:07:24

7.1.2 Intermediate CA Certificates

Issued to the TSP and used for signing end-entity & OCSP responder certificates.

Attribute	Value
`version`	V3 (`0x2`)
`serial_number`	Cryptographically random & unique 128-bit number
`issuer`	See Table 2.
`subject`	See Table 5.
`validity`	10 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 6.
`signature_algorithm`	ECDSA w/ SHA512 (`1.2.840.10045.4.3.4`)
Signed by	Root CA (see Section 7.1.1)

Table 4: Attributes of intermediate CA certificates

Name	OID	Value
`countryName`	`2.5.4.6`	`"DE"`
`organizationName`	`2.5.4.10`	`"Paperless GmbH"`
`organizationalUnitName`	`2.5.4.11`	`"Paperless Trust"`
`organizationIdentifier`	`2.5.4.11`	`"NTRDE-DEM1201.HRB118617"`

`commonName`	`2.5.4.3`	For CA issueing `QCP-n-qscd` certs:
		`"Paperless Trust Qualified Signing CA G{i}"`
		For CA issueing `QCP-l-qscd` certs:
		`"Paperless Trust Qualified Sealing CA G{i}"`
		For CA issueing `QCP-l` certs:
		`"Paperless Trust QCP-l Sealing CA G{i}"`
		For CA issueing `baseline-ts-policy` certs:
		`"Paperless Trust Timestamping CA G{i}"`

Table 5: Subject name attributes used in intermediate CA certificates

Name	OID	Notes	Crit.
`subjectKeyIdentifier`	`2.5.29.14`	Calc. as per RFC5280 [4, 5.2.1.2]	
`àuthorityKeyIdentifier`	`2.5.29.35`	Calc. as per RFC5280 [4, 5.2.1.1]	
`basicConstraints`	`2.5.29.19`	`CA == true`, `pathLenConstraint == 0`	×
`keyUsage`	`2.5.29.15`	`keyCertSign | crlSign`	×
`certificatePolicies`	`2.5.29.32`	As included in issued certificates as described in the relevant CPS.	
`authorityInfoAccess`	`1.3.6.1.5.5.7.1.1`	OCSP: • `http://qualified-root-g{i}.ocsp.trust.paperless.io/` • `http://qualified-root-g{i}.ocsp.paperlesstrust.de/` CA Issuers: • `http://repo.trust.paperless.io/qualified-root-g{i}.crt` • `http://repo.paperlesstrust.de/qualified-root-g{i}.crt`	

Table 6: Extensions included in intermediate CA certificates

7.1.2.1 Issued Certificates

Common Name	**Paperless Trust Qualified Signing CA G1**
Issued By	Paperless Trust Qualified Root CA G1
Certificate Serial Number	290350443331264896134081988330005665975 / `da:6f:76:18:ec:06:d8:99:76:d8:9e:7f:34:0f:18:b7`
Public Key SHA-256	`63:17:60:ec:e6:4c:c3:0f:da:1e:e8:1b:66:31:48:ec bc:1b:72:3c:91:c3:23:c6:b3:f1:a4:fd:62:9b:27:12`
Certificate SHA-256	`3b:e4:9d:13:a2:21:5b:72:69:3b:69:d5:b6:da:a7:ea 19:41:f1:df:76:01:80:33:93:4d:0d:e9:4b:d3:11:21`
Validity (UTC)	2026-01-22 12:13:22 - 2036-01-20 12:13:22

Common Name	**Paperless Trust Qualified Sealing CA G1**
Issued By	Paperless Trust Qualified Root CA G1
Certificate Serial Number	141049610086053488511140397164922114301 / `6a:1d:2a:b1:7f:33:6f:69:30:16:2e:d4:8d:43:90:fd`
Public Key SHA-256	`9a:d2:39:65:95:88:0c:58:8b:00:f2:66:df:67:b9:c1 c3:c7:1d:d2:b4:f1:ea:12:8d:ac:31:7b:c0:6a:fc:80`
Certificate SHA-256	`b5:6c:6c:de:df:54:50:bd:58:6f:c3:dd:3f:95:a7:89 b8:77:cb:bc:1f:39:53:e0:a4:73:67:47:61:49:a2:69`
Validity (UTC)	2026-01-22 12:13:22 - 2036-01-20 12:13:22

Common Name	**Paperless Trust QCP-l Sealing CA G1**
Issued By	Paperless Trust Qualified Root CA G1
Certificate Serial Number	635194770815313783612330184235948298 98 / `2f:c9:68:03:09:05:20:cf:b7:4e:ba:60:eb:c1:c8:4a`
Public Key SHA-256	`d1:72:bb:3f:5b:6e:19:48:dc:a7:c8:43:df:45:14:b6 a1:fb:f1:63:3e:65:25:ba:80:2e:1a:29:bf:2f:f5:05`
Certificate SHA-256	`ae:d8:89:0b:26:c6:a9:45:ff:a9:82:79:e6:9b:12:a5 3a:51:75:28:89:32:eb:c5:e4:f1:32:13:f4:92:26:fa`

Validity (UTC)	2026-01-22 12:13:22 - 2036-01-20 12:13:22

Common Name	**Paperless Trust Qualified Timestamping CA G1**
Issued By	Paperless Trust Qualified Root CA G1
Certificate Serial Number	241127461517810453596594546991543211068 / b5:67:75:b9:10:bb:0f:2e:14:5e:d4:76:91:25:d4:3c
Public Key SHA-256	2d:bb:5d:af:c6:f0:6e:d0:18:b6:10:6f:14:97:1e:b9 c9:c3:72:13:b4:06:fc:c6:5c:5e:6e:d4:88:36:48:0c
Certificate SHA-256	60:9f:2d:a6:4b:e0:cb:47:10:9a:b0:32:bc:10:16:c5 dc:72:d1:2d:4a:38:85:3c:f7:a2:b9:b7:19:4f:1c:9f
Validity (UTC)	2026-01-22 12:13:22 - 2036-01-20 12:13:22

7.1.3 Timestamping Certificates

Certificates generated by the TSP to itself, for the exclusive purpose of generating qualified timestamps for inclusion in signatures (see Section 6.8).

Attribute	Value
`version`	V3 (`0x2`)
`serial_number`	Cryptographically random & unique 128-bit number
`issuer`	See Table 5.
`subject`	See Table 8.
`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 9.
`signature_algorithm`	ECDSA w/ SHA256 (`1.2.840.10045.4.3.2`)
Signed by	Qualified Timestamping Intermediate CA (see Section 7.1.2)

Table 7: Attributes of qualified timestamping certificates

Name	OID	Value
`countryName`	`2.5.4.6`	`"DE"`
`organizationName`	`2.5.4.10`	`"Paperless GmbH"`
`organizationalUnitName`	`2.5.4.11`	`"Paperless Trust"`
`organizationIdentifier`	`2.5.4.11`	`"NTRDE-DEM1201.HRB118617"`
`commonName`	`2.5.4.3`	`"Paperless Trust Qualified Timestamping Authority G{i}"`

Table 8: Subject name attributes used in qualified timestamping certificates

Name	OID	Notes	Crit.
subjectKeyIdentifier	2.5.29.14	Calc. as per RFC5280 [4, 5.2.1.2]	
àuthorityKeyIdentifier	2.5.29.35	Calc. as per RFC5280 [4, 5.2.1.1]	
basicConstraints	2.5.29.19	CA == false, no pathLenConstraint	×
keyUsage	2.5.29.15	nonRepudiation	×
extKeyUsage	2.5.29.37	timeStamping (1.3.6.1.5.5.7.3)	×
certificatePolicies	2.5.29.32	baseline-ts-policy (0.4.0.2023.1.1) CPS: https://repo.trust.paperless.io/tsps.pdf	
qcStatements	1.3.6.1.5.5.7.1.3	As per RFC3739 [18] & ETSI EN 319 412-5 [19]: id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)	
privateKeyUsagePeriod	2.5.29.16	1 year	
authorityInfoAccess	1.3.6.1.5.5.7.1.1	OCSP: • http://qualified-tsa-ca-g{i}.ocsp.trust.paperless.io/ • http://qualified-tsa-ca-g{i}.ocsp.paperlesstrust.de/ CA Issuers: • http://repo.trust.paperless.io/qualified-tsa-ca-g{i}.crt • http://repo.paperlesstrust.de/qualified-tsa-ca-g{i}.crt	

Table 9: Extensions included in qualified timestamping certificates

7.1.3.1 Issued Certificates

Common Name	**Paperless Trust Qualified Timestamping Authority G1**
Issued By	Paperless Trust Qualified Timestamping CA G1
Certificate Serial Number	145735794802079530970937462953459070951 / 6d:a3:b1:70:2b:b6:7e:38:45:a6:f0:6a:02:2c:37:e7
Public Key SHA-256	dc:a1:0a:f3:19:95:68:ec:62:88:ec:d5:9a:d7:64:0c 80:81:55:3d:0f:dd:2e:19:06:67:50:5e:82:23:d6:15
Certificate SHA-256	95:0e:c4:11:ed:f4:4c:95:3d:2c:2f:41:71:fb:c3:38 d1:6c:41:4d:32:be:ce:fe:0b:ef:70:17:94:9e:d5:a3
Validity (UTC)	2026-01-22 12:13:23 - 2028-01-22 12:13:23

7.1.4 OCSP Responder Certificates

Issued by the TSP to OCSP responders operated by the TSP for all issueing CAs. Used exclusively for signing OCSP responses.

Attribute	Value
`version`	V3 (`0x2`)
`serial_number`	Cryptographically random & unique 128-bit number
`issuer`	See Table 5.
`subject`	See Table 11.
`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 9.
`signature_algorithm`	ECDSA w/ SHA512 (`1.2.840.10045.4.3.4`) for root responders ECDSA w/ SHA256 (`1.2.840.10045.4.3.2`) for intermediate responders
Signed by	Issueing CA (intermediates & root) (see Section 7.1.1, Section 7.1.2)

Table 10: Attributes of OCSP responder certificates

Name	OID	Value
`countryName`	`2.5.4.6`	`"DE"`
`organizationName`	`2.5.4.10`	`"Paperless GmbH"`
`organizationalUnitName`	`2.5.4.11`	`"Paperless Trust"`
`organizationIdentifier`	`2.5.4.11`	`"NTRDE-DEM1201.HRB118617"`
`commonName`	`2.5.4.3`	`"Paperless Trust {ca} OCSP Responder G{i}"`

Table 11: Subject name attributes used in OCSP responder certificates

Name	OID	Notes	Crit.
`subjectKeyIdentifier`	`2.5.29.14`	Calc. as per RFC5280 [4, 5.2.1.2]	
`àuthorityKeyIdentifier`	`2.5.29.35`	Calc. as per RFC5280 [4, 5.2.1.1]	
`keyUsage`	`2.5.29.15`	`nonRepudiation`	×
`basicConstraints`	`2.5.29.19`	`CA == false`, no `pathLenConstraint`	×
`extKeyUsage`	`2.5.29.37`	`ocspSigning` (`1.3.6.1.5.5.7.3.9`)	×
`ocsp-noCheck`	`1.3.6.1.5.5.7.48.1.5`	See Note 1. Only present in intermediate CA responder certificates.	
`cRLDistributionPoints`	`2.5.29.31`	• `http://qualified-root-g{i}.crls.trust.paperless.io/root.crl` • `http://qualified-root-g{i}.crls.paperlesstrust.de/root.crl` Only present in root CA responder certificates.	

Table 12: Extensions included in OCSP responder certificates

Note **Note 1**

OCSP responder certificates can not be checked for revocation using OCSP, and therefore include either the `ocsp-noCheck` extension or a CRL distribution point, and lack the `authorityInfoAccess` extension that normally contains the URL to the OCSP responder.

As noted in ETSI EN 319 411-1 [7] and RFC6960 [5], this means that the responder keys for intermediate CA responders are of equivalent importance to the intermediate CA keys, and a compromise of responder keys would necessitate the revocation of the CA certificate.

Root CA responder certificates can be checked for revocation using a CRL.

See Section 4.10 for more information.

7.1.4.1 Issued Certificates

Common Name	**Paperless Trust Qualified Root CA OCSP Responder G1**
Issued By	Paperless Trust Qualified Root CA G1
Certificate Serial Number	424705044853869105046857335725363666 70 / `1f:f3:85:89:d1:0a:74:3b:96:41:31:f6:45:36:f6:4e`
Public Key SHA-256	`4e:77:06:c0:fb:3a:22:f3:14:8d:35:52:af:40:63:e1 cb:cd:53:95:bd:a7:2f:c1:46:a1:85:31:9c:4d:e7:17`
Certificate SHA-256	`c5:1c:7f:3d:6c:6d:11:ac:d2:96:d2:e8:e4:c7:69:24 2d:d2:c0:fa:ba:fd:b9:f3:7e:e5:af:a8:14:fd:db:ab`
Validity (UTC)	2026-01-22 12:13:23 - 2028-01-22 12:13:23

Common Name	**Paperless Trust Qualified Signing CA OCSP Responder G1**
Issued By	Paperless Trust Qualified Signing CA G1
Certificate Serial Number	233585068016144987271739679655797019693 / `af:ba:d9:03:38:a3:71:89:55:cd:8b:e5:f1:19:54:2d`
Public Key SHA-256	`cb:17:25:7f:2f:61:ed:1d:ea:3b:a5:b6:5c:8e:c9:58 06:c6:8b:a0:b8:4f:a9:73:b7:4d:c9:6a:3f:95:6d:ed`
Certificate SHA-256	`0c:33:a4:74:20:0d:f1:77:2b:66:0c:bb:a6:4d:f5:ee a0:bf:29:3b:9a:08:8d:56:14:45:f0:61:2e:77:99:ec`
Validity (UTC)	2026-01-22 12:13:23 - 2028-01-22 12:13:23

Common Name	**Paperless Trust Qualified Sealing CA OCSP Responder G1**
Issued By	Paperless Trust Qualified Sealing CA G1
Certificate Serial Number	337189210546501063553804261747261179787 / `fd:ac:47:9d:cc:ae:91:be:41:d6:11:20:0d:54:07:8b`
Public Key SHA-256	`79:d2:d3:2c:31:66:04:35:46:31:74:93:1d:6b:83:10 90:c8:af:87:fa:1e:80:5e:67:bc:e4:d9:6f:21:86:8a`
Certificate SHA-256	`c7:48:e4:24:ec:c1:6c:72:96:73:cf:fd:d7:5a:5f:ba 06:b8:75:55:30:50:15:dc:40:0a:48:ac:79:17:5a:49`
Validity (UTC)	2026-01-22 12:13:23 - 2028-01-22 12:13:23

Common Name	**Paperless Trust QCP-l Sealing CA OCSP Responder G1**
Issued By	Paperless Trust QCP-l Sealing CA G1
Certificate Serial Number	849316739662316403259696934015256646 08 / `3f:e5:3e:d3:4f:9d:85:91:bd:b1:f7:72:db:ee:3b:60`
Public Key SHA-256	`71:78:bf:6f:a7:00:17:82:78:32:9c:1e:4b:3f:1c:64 dd:3b:de:c0:6a:25:73:06:c2:0b:58:21:7b:16:05:df`

Certificate SHA-256	59:91:b3:41:b9:cc:b6:60:27:82:f2:86:06:50:72:76 5e:90:fd:66:1c:0a:3b:f1:fc:0a:3e:a9:13:8f:58:8e
Validity (UTC)	2026-01-22 12:13:23 - 2028-01-22 12:13:23

Common Name	**Paperless Trust Timestamping CA OCSP Responder G1**
Issued By	Paperless Trust Qualified Timestamping CA G1
Certificate Serial Number	192400559787649852249274219210658746647 / 90:be:ff:fc:25:55:a1:09:53:ff:13:fe:2f:ab:11:17
Public Key SHA-256	c2:b6:84:7a:41:81:5a:18:7e:be:72:e3:40:08:bb:28 d0:2c:78:67:95:c6:41:32:6e:a8:15:74:08:59:09:ad
Certificate SHA-256	24:5d:8e:8f:e5:92:68:4f:b2:87:9c:49:bb:0c:71:cc f0:e3:de:fb:fe:6d:8f:1d:f1:1a:01:a0:f0:94:f3:5d
Validity (UTC)	2026-01-22 12:13:23 - 2028-01-22 12:13:23

7.1.5 Qualified Signing Certificates

This is documented in the relevant CPS.

7.1.6 Qualified Sealing Certificates for the production of Qualified Electronic Seals

This is documented in the relevant CPS.

7.1.7 Qualified Sealing Certificates for the production of Advanced Electronic Seals

This is documented in the relevant CPS.

7.2 Signature Profiles

All signatures (and seals) created using TSP services are detached (no encapsulated content) Cryptographic Message Syntax (CMS) containers as defined in RFC5652 [20] and of the `CAdES-B-T` class as defined in ETSI EN 319 122-1 [21]. Signatures are created in conformance with the `eu-advanced-x509` (`0.4.0.19431.2.1.2`) policy described in ETSI TS 119 431-2 [11]. The attributes included are given below.

The electronic signatures and seals uniquely link to and identify the signatory using the included end-entity certificate, a digest of which is part of the signed attributes using the `ESSCertIDV2` extension.

Attribute	Value
`version`	`0x3`
`digest_algorithms`	SHA-256 (`2.16.840.1.101.3.4.2.1`)
`encapsulated_content_info`	`content_type`: `data` (`1.2.840.113549.1.7.1`) `content`: none
`certificates`	Certificate Chain, including: • Root CA certificate • Intermediate CA certificate • End-entity (signing or sealing) certificate
`crls`	none
`signer_infos`	Single entry as shown in Table 14

Table 13: Content of the `SignedData` structure that constitutes the signature

Attribute	Value
`version`	`0x1`
`sid`	Issuer & serial number of signing/sealing certificate
`digest_algorithm`	SHA-256 (`2.16.840.1.101.3.4.2.1`)
`signature_algorithm`	ECDSA w/ SHA256 (`1.2.840.10045.4.3.2`)
`signed_attrs`	DTBS, see Table 15
`unsigned_attrs`	See Table 16
`signature`	Signature of DTBSR

Table 14: Content of the `SignerInfo` data structure contained in signatures

Name	OID	Notes
`contentType`	`1.2.840.113549.1.9.3`	`data` (`1.2.840.113549.1.7.1`)
`messageDigest`	`1.2.840.113549.1.9.4`	SDR (digest of document to be signed)
`signingCertificateV2`	`1.2.840.113549.1.9.16.2.47`	ESSCertIDV2 containing digest of signing/sealing certificate

Table 15: Signed signature attributes

Name	OID	Notes
`timeStampToken`	`1.2.840.113549.1.9.16.2.14`	Signed timestamp token, issued by Time-stamping Authority (TSA) operated by the TSP, as described in Section 7.3

Table 16: Unsigned signature attributes

7.3 Timestamp Profile

Timestamps are issued as defined in RFC3161 [22]: as `SignedData` CMS containers as defined in RFC5652 [20] with an encapsulated content of type `TSTInfo`. The attributes included are given below and follow the profile described in ETSI EN 319 422 [14].

Attribute	Value
`version`	`1`
`policy`	`0.4.0.2023.1.1` (`best-practices-ts-policy` as per ETSI EN 319 421 [3])
`message_imprint`	SHA-256 digest of `signature` field of containing CMS container
`accuracy`	<=1s
`extensions`	See Table 18
`gen_time`	See Section 6.8 for details regarding clock synchronization
`serial_number`	128 bit serial number generated randomly using HSM
`ordering`	`false`
`nonce`	none
`tsa`	Subject of issueing certificate (see Section 7.1.3)

Table 17: Content of the `TSTInfo` structure being signed

Name	OID	Notes	Crit.
`qcStatements`	`1.3.6.1.5.5.7.1.3`	`etsi-tsts-EuQCompliance` (`0.4.0.19422.1.1`)	

Table 18: Extensions included in timestamp tokens

7.4 OCSP Profile

The OCSP profile follows RFC6960 [5].

Attribute	Value
`tbs_response_data`	See Table 20
`signature_algorithm`	ECDSA w/ SHA256 (`1.2.840.10045.4.3.2`)
`signature`	Signature of `tbs_response_data`, using OCSP responder private key.
`certs`	Certificate Chain, including: • CA certificate • OCSP responder certificate

Table 19: Content of the `basicResponse`-type OCSP response returned by the TSP.

Attribute	Value
`version`	`0x0`
`responder_id`	Subject name of OCSP responder, see Section 7.1.4.
`produced_at`	Timestamp of response production
`responses`	Certificate status for each certificate serial number requested, see Section 4.10.
`response_extensions`	See Table 21

Table 20: Signed OCSP response data

Name	OID	Notes	Crit.
`ocsp-extended-revoke`	`1.3.6.1.5.5.7.48.1.9`	See Section 4.10	
`ocsp-nonce`	`1.3.6.1.5.5.7.48.1.2`	Present if extension was included in request, contains nonce included in request	
`ocsp-archive-cutoff`	`1.3.6.1.5.5.7.48.1.6`	`notBefore` date of responder's CA	

Table 21: Extensions included in OCSP responses

7.5 CRL Profile

The TSP regularly publishes CRLs, as defined in RFC5280 [4], for certificates which cannot otherwise be revoked, namely OCSP responder certificates responding on behalf of root CAs, and the root CA certificates themselves.

The TSP will publish new CRLs in case of a relevant revocation and at regular intervals between 6 months and 1 year.

The composition of the published CRLs is shown below.

Attribute	Value
`tbs_cert_list`	See Table 23
`signature_algorithm`	ECDSA w/ SHA512 (`1.2.840.10045.4.3.4`)
`signature`	Signature of `tbs_cert_list`, using root CA keys.

Table 22: Content of the CRLs published by the TSP for root CAs.

Attribute	Value
`version`	V2 (`0x1`)
`signature`	ECDSA w/ SHA512 (`1.2.840.10045.4.3.4`)
`issuer`	Subject of root CA certificate, see Section 7.1.1.
`this_update`	Time of generation
`next_update`	365 days after generation
`revoked_certificates`	List of revoked root OCSP responder certificates and – potentially – the serial of the root CA certificate itself in case of a CA revocation.
`crl_extensions`	See Table 24

Table 23: Signed CRL content

Name	OID	Notes	Crit.
`expiredCertsonCRL`	`2.5.29.60`	`notBefore` date of root CA	

Table 24: Extensions included in CRLs

8 Compliance Audit and Other Assessment

8.1 Compliance with applicable law

This Trust Service Provider's Policy and/or Practice Statement, as well as all associated rights and obligations, are aligned with the relevant requirements of the Regulation (EU) No. 910/2014, Art. 21 of Regulation (EU) No. 2022/2555 and any other binding standards. Conformity with these legal and regulatory obligations is assessed through biennial external audits performed by an independent and duly qualified auditor. The TSP informs the supervisory body at the latest one month before any planned audits and invites the supervisory body to participate as an observer. The TSP allows the competent supervisory body and a CAB to audit the compliance with the requirements of the eIDAS Regulation.

The TSP has appointed an internal auditor ("Revisor") with the necessary experience and qualification related to public key infrastructures, secure operation of information technology systems and information security in general who conducts internal reviews and audits in accordance with its internal review schedule. The TSP does not begin to provide trust services before the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1). The TSP uses the EU trust mark exclusively for its qualified trust services in compliance with Article 23(1)–(2) eIDAS and only after the qualified status has been indicated in the trusted lists referred to in Article 22(1) of Regulation (EU) No. 910/2014. The trust mark is displayed in the required design and minimum size, and always linked to the relevant trusted list.

8.2 Notification of Changes

Changes regarding service delivery are made in consultation with the CAB and appropriate supervisory body. The TSP informs the supervisory body at least one month before implementing any change in the provision of its qualified trust services.

Notifications to the supervisory body cover at least significant changes to: service descriptions, policies, practice statements and terms and conditions; the technical architecture or trustworthy systems and products; hosting of technical components; cryptographic techniques or materials; registration and identification procedures; organisational structure or governance; the termination plan; financial resources and liability insurance; elements impacting the national trusted list; and third parties involved in service provision, including contractual terms.

Each notification includes a description of the change, the planned date and time, the reasons for the change with supporting evidence where applicable, and any updated documents.

8.3 Audit and Conformity Assessment Requirements

In order to attain the "qualified" status under Regulation (EU) No. 910/2014, the TSP submits a conformity assessment report confirming the compliance of qualified trust services provided by the TSP with the related requirements of Regulation (EU) No. 910/2014 to the national supervisory body (Bundesnetzagentur). The TSP starts to provide its qualified trust services only after the qualified status has been indicated in the trusted lists referred to in Article 22(1) of Regulation (EU) No. 910/2014. The TSP is audited at its own expense at least every 24 months and when any major change is made to Trust Service operations by a conformity assessment body as provided by Article 3 paragraph 18 of eIDAS and accredited by the German Accreditation Authority (DAkkS; http://www.dakks.de/en, member of EA) for performing conformity assessment (audit) according to eIDAS requirements and according to ETSI EN 319 4xx/5xx. The TSP has chosen a conformity assessment body who is entirely independent from the organization. The resulting conformity assessment report is submitted to the supervisory body within three working days of receipt by the TSP.

The results of the performed internal and external audits are properly archived. The certification document received by the Conformity Assessment Body may be published on the TSP's website.

8.4 Non-Compliance and Corrective Action

Where the TSP fails to fulfil any of the requirements set out by the Regulation (EU) No. 910/2014, it shall provide a required by supervisory body remedy within a set time limit, where applicable.

The TSP aims for full compliance and timely correction of non-conformities.

The management of the TSP is responsible for implementing a corrective action plan.

9 Other Business and Legal Matters

9.1 Fees

The TSP provides a price list for its services on their website www.paperless.io.

The TSP charges fees for issuing certificates according to the respective price list published on their website or made available upon request.

The TSP charges a fee for certificate access according to their pricing policy.

There is no charge for certificate revocation and the provision of certificate status information.

The TSP reserves the right to charge an hourly rate or a fee, depending on the services rendered, additional to the fees mentioned above.

The TSP has established a refund policy.

9.2 Financial Responsibility

The TSP has entered into a contract for an insurance policy for liability claims against the TSP. The insurance coverage is provided by an insurance company authorized to operate in the European Union.

The TSP has the necessary resources and the financial stability to properly operate the trust services.

The insurance policy meets the requirements of eIDAS, German Vertrauensdienstegesetz (VDG), Vertrauensdiensteverordnung (VDV) and Versicherungsvertragsgesetz (VVG)

9.2.1 Insurance or warranty coverage for end-entities

It is in the sole responsibility of Subscribers and Relying Parties to ensure an adequate insurance, to cover risks using certificates, signatures, seals or any other services offered by the TSP, according to eIDAS, VDG and VDV.

9.3 Confidentiality of Business Information

All information and data obtained by the Trust Service Provider (TSP) during the course of its operations is treated as confidential, unless explicitly excluded under this clause. Confidential information encompasses, without limitation, strategic and business plans, sales-related data, trade secrets, organizational identifiers, registration details, and subscriber-related information. Disclosure of such information within the TSP organization or to contracted service providers engaged by the TSP does not constitute a breach of confidentiality.

Information that is already in the public domain, or that is included in issued certificates, does not qualify as confidential. Likewise, data that the TSP is expressly permitted to disclose—whether by written authorization of the concerned party, by legal obligation, or because it forms part of publicly available certificate content—does not fall under confidentiality obligations. In line with RFC 5280, certificate status information, including Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) responses, is not regarded as confidential.

The TSP implements all necessary measures to ensure compliance with the General Data Protection Regulation (GDPR) and applicable national data protection requirements. The TSP processes identification data solely to the extent that it is appropriate, relevant, and not excessive for granting access to its services.

9.4 Privacy of Personal Information

The TSP takes technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data in accordance with Regulation (EU) 2016/679.

The TSP presents its privacy policy (including data protection procedures) at the beginning of the registration process.

The confidentiality and integrity of registration and signature activation data is protected, especially when exchanged with the subscriber/subject or between distributed TSP's system components.

TSP personnel or systems never have access to or store the SD at any point.

To support essential business activities and in order to meet statutory requirements, the TSP securely retains records including user consent and identification information.

When personal data is processed by a third party, if needed by the law, an appropriate agreement with the third party is as processors of personal data is in place in order to ensure that they do comply with the legal requirements, including the implementation of technical, organizational and legal measures to protect the personal data.

9.5 Dispute Resolution Procedures

The TSP has a "complaints and appeals" procedure for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters. The terms and conditions inform customers and other relying parties about the procedure.

9.6 Representations and Warranties

9.6.1 Subscriber representations and warranties

Subscribers warrant full compliance with all provisions stated in this TSPS, service-based Policies and Practice statements, related agreements, eIDAS and related regulations and rules.

Subjects and Subscribers are responsible for:

- having a basic understanding of the proper use of public key cryptography and certificates,
- providing only correct information without errors, omissions or misrepresentations,
- substantiating information by providing a properly completed application as specified in Section 4.1,
- supplementing such information with a proof of identity as specified Section 3.2.2,
- verifying the content of a newly issued certificate before its first use and to refrain from using it, if it contains misleading or inaccurate information,
- reading and agreeing to all terms and conditions of this TSPS, other relevant regulations and agreements,
- reading and agreeing to the general terms and conditions of the TSP,
- using certificates exclusively for lawful and authorized purposes,
- ensuring that certificates are exclusively used on behalf of the person or the organization specified as the subject of the certificate,
- notifying the TSP of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate,
- revoking the certificate immediately if any information included in the certificate is misleading or inaccurate, or if any change of circumstances makes the information in the certificate misleading or inaccurate,
- verify that the time-stamp has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification;
- take into account any limitations on the usage of the time-stamp indicated by the present document
- take into account any other precautions prescribed in agreements or elsewhere.

9.6.2 Relying party representations and warranties

Relying parties are recommended to:

- verify the validity, suspension or revocation of the certificate using current revocation status information,
- take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions, and
- take any other precautions prescribed in agreements or elsewhere.

Relying parties are informed that as part of the conditions for a certificate to be relied upon as an EU Qualified Certificate, the trust anchor for the validation of the certificate shall be as identified in a service digital identifier of an appropriate EU trusted list entry for a QTSP (see ETSI TS 119 612). ETSI TS 119 615 provides guidance on how to validate a digital certificate against the EU trusted lists, in order to determine whether it can be considered as an EU qualified certificate and ETSI TS 119 172-4 describes how to validate a digital signature against the EU trusted lists, in order to determine whether it can be considered as an EU qualified electronic signature or seal.

9.7 Accessibility Commitment

In line with European Accessibility Act (EAA) and the German Barrierefreiheitsstärkungsgesetz (BFSG) and with reference to accessibility standards such as ETSI EN 301 549, the Trust Service Provider (TSP) undertakes to ensure that its services are usable by all prospective users, including persons with disabilities, to the greatest extent feasible. E.g. the TSP ensures that its web services comply with the Web Content Accessibility Guidelines (WCAG) 2.1 at level AA and offers several different identification methods to accommodate users with varying needs and capabilities.

9.8 Terms & Conditions

The terms and conditions of the trust service provider are made available to relying parties before using the service and include limitations of the trust service and liability.

Before entering into a contractual relationship, the TSP informs, through a durable means of communication, and in a human readable form, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use. Before entering into a contractual relationship, the subscriber has to agree to the terms and conditions of the TSP electronically. After any changes to the terms and conditions, the subscriber must again accept them prior to next use.

If the subscriber and subject are two separate entities and the subject is a legal person, the agreement is divided in 2 parts:

1. The agreement between the TSP and the subscriber ("Subscriber Agreement for the use of qualified certificates for electronic seals", OID `1.3.6.1.4.1.64134.1.1.7`) includes the following clauses:
    - agreement to the subscriber's obligations,
    - consent to the keeping of a record by the TSP of information used in registration, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation, the identity placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the TSP terminating its services
    - confirmation that the information to be held in the certificate is correct
    - obligations applicable to subjects
2. The agreement between the TSP and the subject, as signed by a legal representative of the subject ("Order Agreement for qualified certificates for electronic seals") includes the following clauses:
    - the agreement by the subject on the obligations applicable to subjects
    - consent to the keeping of a record by the TSP of information used in registration, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation, the identity placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the TSP terminating its services

If the subject and subscriber are the same entity (i.e. a natural person) the "Subscriber Agreement for the use of qualified certificates for electronic signatures", OID `1.3.6.1.4.1.64134.1.1.6` is the sole agreement between both parties and includes all relevant clauses listed above.

Terms & Conditions, Privacy Policy and Subscriber Agreement are governed by German law. The place of jurisdiction is the registered office of the TSP.

Terms & Conditions and Subscriber Agreement contain liability clauses to the extent permitted by the German Vertrauensdienstegesetz (VDG), Vertrauensdiensteverordnung (VDV) and Versicherungsvertragsgesetz (VVG).

A TSA Disclosure Statement

The TSA disclosure statement is included in the present document. The relevant sections are outlined below.

A.1 TSA Contact Info

The TSA can be contacted as described in Section 1.5.

A.2 Electronic Time-Stamp Types and Usage

Only a single type of timestamp (as described in Section 7.3) is issued, as described in Section 6.8.

A.3 Reliance Limits

The claimed accuracy is included in the timestamp as described in Section 7.3.

TSA event logs are retained for at least 15 years.

A.4 Obligations of Subscribers

Subscriber obligations are given in Section 9.6.1.

A.5 Obligations of Relying Parties

Relying party obligations – including requirements to check certificates for revocation – are given in Section 9.6.2.

A.6 Limited warranty and disclaimer/limitation of liability

A.7 Applicable Agreements and Practice Statements

The present document (specifically Section 6.8) describes the TSP's timestamping practices.

A.8 Privacy policy

See Section 9.4 for information on privacy of personal information. The full privacy policy is available as described in Section 2.

A.9 Refund policy

See Section 9.1.

A.10 Applicable law, complaints and dispute resolution

A.11 TSA and repository licenses, trust marks, and audit

B PKI Disclosure Statement

The PKI disclosure statement is included in the present document. The relevant sections are outlined below.

B.1 TSP Contact Info

The TSP can be contacted as described in Section 1.5.

The process to request revocations is described in Section 4.9.

B.2 Certificate Type, Validation Procedures and Usage

Certificates (as described in Section 7.1) are issued to the general public as described in Section 4.

The specific CP for each trust service, including the relevant Object Identifier (OID) is given in Section 1.1.1.

Limitations on the use of issued certificates are outlined in Section 1.4.

B.3 Reliance Limits

Limitations on the use of issued certificates are outlined in Section 1.4.

Registration information and TSP event logs are retained for at least 15 years.

B.4 Obligations of Subscribers

Subscriber obligations are given in Section 9.6.1.

B.5 Obligations of Relying Parties

Relying party obligations – including requirements to check certificates for revocation – are given in Section 9.6.2.

B.6 Limited warranty and disclaimer/limitation of liability

B.7 Applicable Agreements, CPS, CP

The applicable documents for each trust service are described in Section 1, specifically Section 1.1.1.

B.8 Privacy Policy

See Section 9.4 for information on privacy of personal information. The full privacy policy is available as described in Section 2.

B.9 Refund Policy

See Section 9.1.

B.10 Applicable law, complaints and dispute resolution

B.11 TSP and repository licenses, trust marks and audit

Bibliography

[1] "RFC3647: Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework." [Online]. Available: https://www.rfc-editor.org/rfc/rfc3647

[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] "ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps." [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.02.01_60/en_319421v010201p.pdf

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

[5] "RFC6960: X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP." [Online]. Available: https://www.rfc-editor.org/rfc/rfc6960

[6] "ETSI EN 319 401: Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers." [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/319401/03.01.01_60/en_319401v030101p.pdf

[7] "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

[8] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

[9] *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*. [Online]. Available: http://data.europa.eu/eli/reg/2024/1183/oj

[10] "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

[11] "ETSI TS 119 431-2: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation." [Online]. Available: https://www.etsi.org/deliver/etsi_ts/119400_119499/11943102/01.02.01_60/ts_11943102v010201p.pdf

[12] "ETSI TS 119 312: Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites." [Online]. Available: https://www.etsi.org/deliver/etsi_TS/119300_119399/119312/01.03.01_60/ts_119312v010301p.pdf

[13] "European Cybersecurity Certification Group Sub-group on Cryptography: Agreed Cryptographic Mechanisms." [Online]. Available: https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

[14] "ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles." [Online]. Available: https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.00_30/en_319422v010100v.pdf

[15] "RFC5905: Network Time Protocol Version 4: Protocol and Algorithms Specification." [Online]. Available: https://www.rfc-editor.org/rfc/rfc5905

[16] "RFC8915: Network Time Security for the Network Time Protocol." [Online]. Available: https://www.rfc-editor.org/rfc/rfc8915.html

[17] "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

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

[19] "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

[20] "RFC5652: Cryptographic Message Syntax (CMS)." [Online]. Available: https://www.rfc-editor.org/rfc/rfc5652

[21] "ETSI EN 319 122-1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures." [Online]. Available: https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.02.01_60/en_31912201v010201p.pdf

[22] "RFC3161: Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)." [Online]. Available: https://www.rfc-editor.org/rfc/rfc3161

Revision History

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