CERT DIGITAL – QPS
(QUALIFIED PRESERVATION SERVICE)

PRESERVATION SERVICE POLICY PRACTICE & STATEMENTS (PSPPS)

VERSION 1.0 / 27.08.2025

[LANGUAGE: ENGLISH]

Version History

Date	Revision	Author(s)	Summary
27.08.2025	1.0	Adelin Cusman	Initial version of CERT DIGITAL QPS PSPPS

Created by	Approved by

Any question or request for information regarding the content of this document should be directed to office@certdigital.ro .

Contents

1. Introduction

1.1 Document Title

CERT DIGITAL QPS – Preservation Service Policy & Practice Statement (PSPPS)

1.2 Document Version and Control

- **Version:** 1.0
- **Date:** 27.08.2025
- **Authoring Organization:** Centrul de Calcul S.A.
- **Status (***Draft/Approved***):** Draft
- **Document Control:** This document is subject to version control. All revisions are logged in the Version History .

1.3 Purpose of the Document

The purpose of this Preservation Service Policy & Practice Statement (hereafter referred to as *PSPPS*) is to define the policies and practices applied by **CERT DIGITAL QPS** in the provision of a **Qualified Preservation Service** for electronic signatures and electronic seals, in accordance with:

- **Regulation (EU) No 910/2014 (eIDAS)**, and
- Applicable **ETSI standards**, including but not limited to ETSI EN 319 401, ETSI TS 119 511, ETSI TS 119 512, ETSI TS 119 312, ETSI EN 319 421/422, ETSI TS 119 441/442, and ETSI EN 319 102-1.

This document communicates to regulators, auditors, subscribers, relying parties, and other stakeholders the framework under which CERT DIGITAL QPS operates its preservation service, including:

- The objectives and scope of the service;
- The roles and responsibilities of participants;
- The preservation processes and evidence policies;
- The legal and compliance obligations that apply.

1.4 Scope of the Service

The **CERT DIGITAL QPS** preservation service is designed to ensure the **long-term validity and probative value** of:

- **Qualified Electronic Signatures (QES)**;
- **Qualified Electronic Seals (QSealS)**.

The service provides mechanisms to preserve:

- Digital signatures and seals, including their associated validation data (PDS – Preservation of Digital Signatures);
- Proof of existence for arbitrary digital data (PGD – Proof of Existence of Data), where applicable.

The service supports one or more **preservation storage models** as defined in ETSI TS 119 511:

- **With Storage (WST);**
- **With Temporary Storage (WTS);**
- **Without Storage (WOS).**

1.5 Audience

This document is intended for:

- **Auditors and supervisory bodies** evaluating the conformity of CERT DIGITAL QPS with eIDAS and ETSI standards;
- **Subscribers** (entities using CERT DIGITAL QPS preservation services);
- **Relying parties** who rely on preserved evidences issued by the service;
- **Internal staff** of CERT DIGITAL QPS, to ensure alignment with documented practices and policies.

1.6 Policy Framework

The CERT DIGITAL QPS PSPPS is structured in alignment with ETSI TS 119 511 §4.3 and ETSI EN 319 401. It establishes:

- **Policies** governing preservation activities (cryptographic algorithms, time-stamping, evidence renewal);

- **Practices** applied in service operations, including security, evidence generation, storage, renewal, and retrieval.

This PSPPS is a **publicly available document**, ensuring transparency and trust for all parties interacting with the preservation service.

All public documents related to CERT DIGITAL QPS, including this PSPPS, are published and made available at: **https://certdigital.ro/repository**.

1.7 References

This PSPPS makes reference to the following normative documents:

- Regulation (EU) No 910/2014 (eIDAS)
- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers
- ETSI TS 119 511 – Policy and Security Requirements for Trust Service Providers providing Preservation Services
- ETSI TS 119 512 – Protocols for Trust Service Providers providing Preservation Services
- ETSI EN 319 421 – Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422 – Time-Stamp Protocol and Profiles
- ETSI TS 119 312 – Cryptographic Suites
- ETSI TS 119 441 – Policy and Security Requirements for Trust Service Providers providing Signature Validation Services
- ETSI TS 119 442 – Protocols for Trust Service Providers providing Signature Validation Services
- ETSI EN 319 102-1 – Electronic Signatures and Infrastructures (AdES validation)

1.8 Object Identifiers (OIDs)

CERT DIGITAL QPS has established a dedicated **OID arc** under its enterprise number (1.3.6.1.4.1.47898) for the qualified preservation service.

The following OIDs are reserved and assigned:

1.8.1 CERT DIGITAL QPS Core OIDs

OID	Description
1.3.6.1.4.1.47898.10	CERTDIGITAL Qualified Preservation Service (id-qps)
1.3.6.1.4.1.47898.10.1	CERTDIGITAL QPS Preservation Service Policy & Practice Statement (PSPPS)

1.8.2 CERT DIGITAL QPS Preservation Profiles

OID	Description
1.3.6.1.4.1.47898.10.1.1	CERTDIGITAL QPS – WOS Preservation Profile
1.3.6.1.4.1.47898.10.1.2	CERTDIGITAL QPS – WST Preservation Profile
1.3.6.1.4.1.47898.10.1.3	CERTDIGITAL QPS – WTS Preservation Profile

1.8.3 CERT DIGITAL QPS Extended Policies (reserved for future use)

OID	Description
1.3.6.1.4.1.47898.10.2	CERTDIGITAL QPS Validation Policy
1.3.6.1.4.1.47898.10.2.1	CERTDIGITAL QPS Default Validation Policy (baseline EU rules)
1.3.6.1.4.1.47898.10.3	CERTDIGITAL QPS Cryptographic Policy
1.3.6.1.4.1.47898.10.4	CERTDIGITAL QPS Evidence Format Policy
1.3.6.1.4.1.47898.10.5	CERTDIGITAL QPS API Policy Profile

Each OID is used to uniquely identify **service policies, profiles, and configurations**. These identifiers may appear in:

- Service policies and contracts;
- Preservation objects and evidence containers;
- Validation policies and reports;
- Trusted List entries.

1.9 Definitions and Acronyms

For the purposes of this document, definitions from **eIDAS Regulation** and **ETSI standards** apply. Additional definitions and acronyms are included in Annex A (Glossary).

2. General Principles

2.1 Objectives of the Preservation Service

The main objective of **CERT DIGITAL QPS** is to provide a **Qualified Preservation Service** that ensures the **long-term validity, integrity, and probative value** of:

- **Qualified Electronic Signatures (QES)**;
- **Qualified Electronic Seals (QSealS)**.

The service is designed to:

- Preserve the legal value of signatures and seals beyond the natural cryptographic lifetime of the algorithms originally used;
- Enable relying parties to verify the authenticity and validity of preserved signatures and seals at any point in the future;
- Provide reliable, independently verifiable **preservation evidences** that can be used in legal or administrative proceedings.

The service is operated in full compliance with **Regulation (EU) 910/2014 (eIDAS)**, relevant **ETSI standards**, and recognized best practices for long-term digital preservation.

2.2 Scope of the Service

CERT DIGITAL QPS provides preservation services in the following scope:

- **Preservation of Digital Signatures (PDS):**
  Ensuring that electronic signatures and seals, together with their associated validation data, remain valid and verifiable over extended periods.
    - Profile OIDs:
        - WOS model → **1.3.6.1.4.1.47898.10.1.1**

  - WST model → **1.3.6.1.4.1.47898.10.1.2**
  - WTS model → **1.3.6.1.4.1.47898.10.1.3**

- **Proof of Existence of Data (PGD) [optional]:**
  Providing cryptographic proof that specific digital data existed at a certain point in time, without necessarily validating or preserving signatures.
    - A dedicated OID may be reserved under **1.3.6.1.4.1.47898.10.6** if PGD is formally included in scope.

[Note: If PGD is not part of the service scope, this subsection will be marked "Not applicable" in the final approved version.]

2.3 Preservation Storage Models

The service supports one or more storage models as defined in **ETSI TS 119 511**, each uniquely identified by a registered **OID**.

- **With Storage (WST):**
    - **OID:** 1.3.6.1.4.1.47898.10.1.2
    - Description: The preservation object (including signatures, validation data, and evidences) is stored by CERT DIGITAL QPS for the full duration of the retention period defined in the service policy.
    - Advantage: Simplifies verification by relying parties.
    - Responsibility: CERT DIGITAL QPS ensures the secure, long-term storage and evidence renewal.
- **With Temporary Storage (WTS):**
    - **OID:** 1.3.6.1.4.1.47898.10.1.3
    - Description: The preservation object is stored by CERT DIGITAL QPS only temporarily, sufficient to complete preservation processing and allow subscribers to retrieve the outputs. After this period, the preservation object is securely deleted, but preservation evidences may be retained.
- **Without Storage (WOS):**
    - **OID:** 1.3.6.1.4.1.47898.10.1.1

- Description: CERT DIGITAL QPS does not store the preservation object. Instead, preservation evidences are returned immediately to the subscriber, who assumes responsibility for long-term storage of both original data and evidences.

2.4 Service Assurance and Compliance

CERT DIGITAL QPS asserts compliance with the following:

- **Regulatory framework:**
  - Regulation (EU) No 910/2014 (eIDAS).
- **Applicable standards:**
  - ETSI TS 119 511 – Policy & Security Requirements for Preservation Services.
  - ETSI TS 119 512 – Protocols for Preservation Services.
  - ETSI EN 319 401 – General Policy Requirements for Trust Service Providers.
  - ETSI TS 119 312 – Cryptographic Suites.
  - ETSI EN 319 421/422 – Requirements and Protocols for Time-Stamping.
  - ETSI TS 119 441/442 – Validation Service Requirements and Protocols.
- **Trust List publication:**
  The service will be listed in the national Trusted List under the service type identifier:
  - **http://uri.etsi.org/TrstSvc/Svctype/PSES/Q** (Qualified Preservation Service). With qualifiers indicating the supported scope:
  - **ForSignatures**
  - **ForSeals**
- **Policy OID Reference:**
  All preservation operations are executed under the **CERT DIGITAL QPS PSPPS OID: 1.3.6.1.4.1.47898.10.1**, which references this document.

2.5 Transparency and Accessibility

The Preservation Service Policy & Practice Statement (PSPPS) is a **public document**. It is made available to:

- Subscribers before entering into a contractual relationship with CERT DIGITAL QPS;
- Relying parties who wish to verify evidences produced by CERT DIGITAL QPS;
- Auditors and supervisory bodies for conformity assessments.

The associated OIDs are published in this document and may also be included in:

- Preservation objects and evidence records;
- Validation reports;
- Publicly accessible documentation (e.g., service website).

The PSPPS and related preservation service policies are available for public download at **https://certdigital.ro/repository**.

2.6 Limitations

The preservation service does not guarantee validity of signatures or seals that were **invalid at the time of ingestion**. Preservation applies only to:

- Signatures and seals that were valid when initially submitted to the service;
- Data submitted in compliance with the technical formats and cryptographic policies defined in Chapter 11 (Technical Specifications).

The service does not extend beyond the preservation of digital signatures, seals, and related evidences. Additional services such as electronic archiving of content, certification authority services, or identity verification are outside the scope of CERT DIGITAL QPS.

3. Service Overview

3.1 Description of the Service

CERT DIGITAL QPS provides a **Qualified Preservation Service (QPS)** for electronic signatures and electronic seals, ensuring their **long-term validity, integrity, and probative value** in accordance with **Regulation (EU) No 910/2014 (eIDAS)** and **ETSI TS 119 511/512**.

The service achieves this by:

- Receiving preservation objects from subscribers;

- Validating digital signatures and seals at the time of ingestion;
- Collecting all associated validation data (certificates, OCSP, CRLs);
- Generating **preservation evidences** using approved formats (ERS / AdES-LTA);
- Renewing preservation evidences before cryptographic algorithms become obsolete;
- Providing secure storage (WST / WTS) or immediate delivery (WOS) of preservation objects;
- Making evidences retrievable and independently verifiable by relying parties.

All preservation operations are carried out under the **CERT DIGITAL QPS PSPPS OID: 1.3.6.1.4.1.47898.10.1**.

3.2 Service Workflows

3.2.1 Ingestion Workflow

1. **Submission:** The subscriber submits a digital signature/seal and, if applicable, the signed data or approved digests.
2. **Validation:** The service validates the signature/seal in accordance with ETSI EN 319 102-1 and the **CERT DIGITAL Default Validation Policy OID: 1.3.6.1.4.1.47898.10.2.1**.
3. **Validation Data Collection:** Certificate chains, CRLs, and/or OCSP responses are gathered.
4. **Evidence Creation:**
    - For ERS profiles: evidence is created using **RFC 4998/6283** and time-stamped (EN 319 422).
    - For AdES-LTA profiles: archival timestamps are embedded into the signature container.
5. **Return/Storage:** Depending on the storage model selected (WOS, WST, WTS), the preservation object is either returned, stored, or stored temporarily.

3.2.2 Renewal Workflow

1. **Monitoring:** CERT DIGITAL QPS continuously monitors algorithm lifetimes against ETSI TS 119 312.

2. **Trigger:** Renewal is initiated when a cryptographic primitive approaches its security end-date.
3. **Renewal Action:** New evidences are generated with stronger algorithms and updated timestamps.
4. **Update:** Renewals are added to the preservation object container (POC) and logged.

3.2.3 Retrieval Workflow

- **Request:** A subscriber or relying party issues a RetrievePO or ValidateEvidence request.
- **Processing:** CERT DIGITAL QPS retrieves the preservation object or validates the evidence.
- **Delivery:** A complete preservation object container (POC), with validation reports and references to its applicable OID profile, is returned.

3.2.4 Deletion Workflow (if applicable)

- WST/WTS models: Objects are securely deleted after contractual retention periods.
- Deletion events are logged and associated with the relevant OID profile.

3.3 Preservation Profiles Supported

CERT DIGITAL QPS supports the following preservation profiles, each identified by a dedicated **OID**:

- **WOS Preservation Profile – OID: 1.3.6.1.4.1.47898.10.1.1**
    - Profile description: Preservation without storage.
    - Service returns evidence immediately to the subscriber.
    - Suitable when the subscriber is responsible for storing data and evidences.
- **WST Preservation Profile – OID: 1.3.6.1.4.1.47898.10.1.2**
    - Profile description: Preservation with storage.
    - CERT DIGITAL QPS stores preservation objects and evidences for the agreed retention period.
- **WTS Preservation Profile – OID: 1.3.6.1.4.1.47898.10.1.3**
    - Profile description: Preservation with temporary storage.

- CERT DIGITAL QPS stores preservation objects only until processing is complete and the subscriber retrieves outputs.

- **Validation Policy Reference – OID: 1.3.6.1.4.1.47898.10.2.1**
  - The default validation policy applied to all signatures/seals prior to preservation.
- **Cryptographic Policy Reference – OID: 1.3.6.1.4.1.47898.10.3**
  - Defines the approved algorithms, key lengths, and renewal rules, in alignment with ETSI TS 119 312.

3.4 Supported Formats and Standards

Signature/Seal formats:

- CAdES (CMS Advanced Electronic Signatures) – ETSI EN 319 122-1
- XAdES (XML Advanced Electronic Signatures) – ETSI EN 319 132-1
- PAdES (PDF Advanced Electronic Signatures) – ETSI EN 319 142-1
- ASiC (Associated Signature Containers) – ETSI EN 319 162-1

Preservation evidences:

- RFC 4998 Evidence Record Syntax (ERS)
- RFC 6283 XMLERS (XML Evidence Record Syntax)
- AdES-LTA augmentation (ETSI EN 319 122-1, 319 132-1, 319 142-1)

Protocols:

- Preservation protocol bindings as per ETSI TS 119 512 (SOAP/XML and REST/JSON).

3.5 Service Limitations

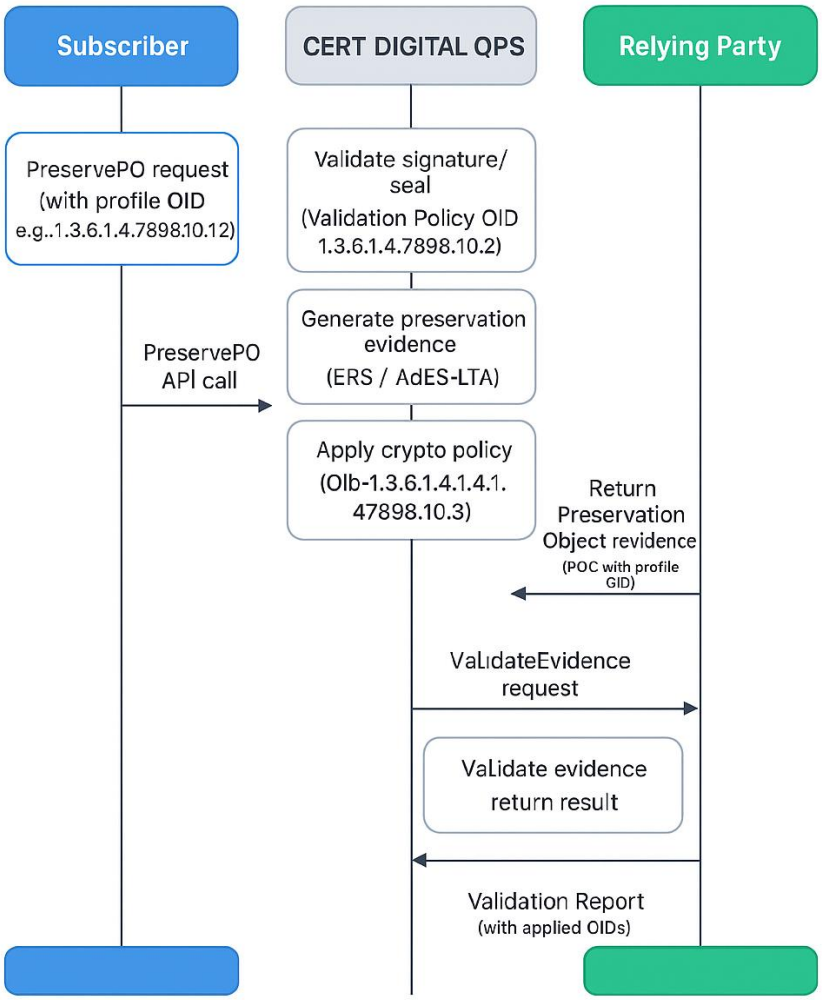
- Only signatures/seals that are **valid at ingestion** can be preserved.
- Preservation objects must comply with **accepted formats** and **crypto policy OID: 1.3.6.1.4.1.47898.10.3**.
- Data size may be limited depending on technical constraints (specified in Chapter 11).
- Renewal is bound to cryptographic policy thresholds (OID 1.3.6.1.4.1.47898.10.3).

3.6 Service Interfaces

CERT DIGITAL QPS exposes the following interfaces (per ETSI TS 119 512):

- PreservePO → Submit preservation object (references applied profile OID).
- RetrievePO / RetrievePOC → Retrieve stored objects (includes OID of the storage model).
- UpdatePOC → Renew evidences (with reference to crypto policy OID).
- ValidateEvidence → Validate evidence and return results with applied validation policy OID.
- DeletePO → Secure deletion (where applicable).
- RetrieveInfo → Retrieve metadata, including supported OIDs.
- RetrieveTrace → Retrieve logs, with OID references for lifecycle traceability.

3.7 High-Level Workflow Diagram



4. Service Environment

4.1 Overview

The **CERT DIGITAL QPS** preservation service operates in a **secure, redundant, and controlled environment** designed to ensure:

- Continuous availability of the preservation service;
- Protection of sensitive cryptographic material;
- Integrity and confidentiality of subscriber data;
- Compliance with the **cryptographic policy OID: 1.3.6.1.4.1.47898.10.3**;
- Alignment with **ETSI EN 319 401**, **TS 119 511**, and applicable data protection regulations (e.g., GDPR).

4.2 Physical Security Controls

- **Data Centers:**
  - Operated in Tier III+ or equivalent facilities within the EU.
  - Redundant power, cooling, and fire suppression systems.
  - Physical access restricted to authorized staff, enforced by multi-factor authentication (badge + biometric).
- **Access Control:**
  - All physical access logged and monitored via CCTV.
  - Dual-control required for entry to critical rooms (e.g., HSM vaults).
  - Visitors and contractors subject to strict escort policies.
- **Environmental Monitoring:**
  - Continuous monitoring of temperature, humidity, and fire risks.
  - Automated alerts and incident procedures in case of deviations.

4.3 Logical and Network Security

- **Network Segmentation:**
  - Separation of internal trust-service networks from public access zones (DMZ).

- Dedicated management VLANs, not accessible from the Internet.

- **Firewalls and IDS/IPS:**
  - Multi-layer firewalls at perimeter and core.
  - Intrusion detection and prevention systems monitoring all ingress/egress.
- **Secure Communications:**
  - All external interactions (e.g., PreservePO, ValidateEvidence) over TLS 1.2+ with strong cipher suites (aligned with crypto policy OID: 1.3.6.1.4.1.47898.10.3).
  - Mutual authentication for subscriber and relying party connections where applicable.
- **System Hardening:**
  - Servers hardened according to CIS/NIST baselines.
  - Security patches applied according to vulnerability management policy.
  - Critical systems protected by SELinux/AppArmor and integrity monitoring.

4.4 Cryptographic Module Environment

- **Hardware Security Modules (HSMs):**
  - All private keys used by CERT DIGITAL QPS (e.g., for signing preservation evidences, issuing service assertions) are stored in **FIPS 140-2 Level 3 or Common Criteria EAL4+ certified HSMs**.
  - HSM operations bound to the **Crypto Policy OID: 1.3.6.1.4.1.47898.10.3**.
- **Key Management:**
  - Dual-control required for activation of signing keys.
  - Key ceremonies performed under documented procedures.
  - Keys subject to lifecycle management (generation, usage, rollover, destruction).
- **Time Synchronization:**
  - All cryptographic operations synchronized with secure, redundant UTC time sources.

- Time-stamps used in preservation evidences are obtained from a **Qualified Time-Stamping Authority (QTSA)** conforming to **EN 319 421/422**.

4.5 Service Redundancy and Continuity

- **Redundancy:**
  - All critical components (application servers, HSMs, databases) deployed in high-availability clusters.
  - Load balancing ensures service continuity during maintenance or node failure.
- **Backup and Recovery:**
  - Daily encrypted backups of preservation objects and evidences (WST/WTS profiles).
  - Off-site replication with geographically separated facilities.
  - Tested disaster recovery plan ensuring recovery point objective (RPO) ≤ 24h and recovery time objective (RTO) ≤ 4h.
- **Business Continuity:**
  - Documented Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
  - Regular failover testing and incident response exercises.

4.6 Monitoring and Logging

- **Service Monitoring:**
  - Continuous monitoring of availability, performance, and latency of APIs (PreservePO, RetrievePO, ValidateEvidence).
  - Alerts raised for anomalies and failures.
- **Security Logging:**
  - Detailed logging of access, API calls, evidence generation, and renewal actions.
  - Logs are tamper-evident and retained for at least 10 years.
- **Traceability:**

- RetrieveTrace API allows subscribers and auditors to obtain lifecycle trace information, including the OIDs of applied profiles and policies.

4.7 Personnel and Organizational Controls

- **Trusted Roles:**
  - Roles defined for system administrators, security officers, and operational staff.
  - Segregation of duties to prevent conflicts of interest.
- **Background Checks:**
  - All trusted staff undergo pre-employment screening and periodic re-validation.
- **Training:**
  - Annual security and compliance training on ETSI/eIDAS requirements, incident response, and secure key management.
- **Access Policies:**
  - Principle of least privilege enforced.
  - Role-based access control implemented across all systems.

5. Service Policy

5.1 Preservation Evidence Policy

The **CERT DIGITAL QPS** preservation service ensures that all preservation evidences generated are:

- **Complete:** Contain all data required to prove validity at the time of preservation (signatures, certificates, revocation data, timestamps).
- **Verifiable:** Independently verifiable by relying parties using standard tools and policies.
- **Immutable:** Once generated, evidences are cryptographically bound to prevent modification.

- **Traceable:** Evidences include references to the specific preservation profile OID applied (e.g., WOS/WST/WTS).

Preservation evidences may be implemented in one of the following forms:

- **Evidence Record Syntax (ERS)** – **RFC 4998/6283**, using hash trees anchored with timestamps.
- **AdES-LTA augmentation** – Adding archival timestamps and validation data inside advanced electronic signatures (PAdES-LTA, XAdES-A, CAdES-A).

The choice of evidence format is governed by the **Evidence Format Policy OID: 1.3.6.1.4.1.47898.10.4**.

5.2 Time Evidence Policy

- **Time-Stamping:**
  - All preservation evidences include **trusted timestamps** conforming to **RFC 3161** and ETSI EN 319 422 profiles.
  - Time-stamps are obtained from a **Qualified Time-Stamping Authority (QTSA)** in accordance with **EN 319 421**.
- **Assurance:**
  - The service guarantees that every evidence chain includes at least one timestamp from a QTSA.
  - Timestamps are renewed periodically to maintain long-term cryptographic strength.
- **Policy Reference:**
  - The time evidence policy is defined under the **PSPPS OID: 1.3.6.1.4.1.47898.10.1** and further referenced in the **Evidence Format Policy OID: 1.3.6.1.4.1.47898.10.4**.

5.3 Cryptographic Policy

CERT DIGITAL QPS enforces a strict cryptographic policy aligned with **ETSI TS 119 312 (Cryptographic Suites)**.

- **Policy Identifier: OID: 1.3.6.1.4.1.47898.10.3**
- **Accepted Hash Functions:**
  - SHA-256 (minimum) – current default
  - SHA-384, SHA-512 – supported for high-assurance use
- **Accepted Signature Algorithms:**
  - RSA ≥ 3072 bits
  - ECDSA with curves P-256, P-384, P-521
  - EdDSA (Ed25519, Ed448) where supported
- **Time-Stamp Signature Algorithms:**
  - Same as above, restricted to algorithms supported by the selected QTSA.
- **Crypto Renewal Thresholds:**
  - Hash algorithms renewed at least 5 years before known collision/weakness date.
  - Signature algorithms renewed at least 3 years before recommended end-of-life.

All cryptographic operations within the service (including evidence signing and HSM operations) reference this **cryptographic policy OID** in audit records and evidence metadata.

5.4 Renewal Policy

The preservation service implements a **proactive renewal strategy** to ensure long-term security of preserved signatures and seals.

- **Monitoring:** Algorithms are monitored continuously against ETSI TS 119 312 updates, NIST recommendations, and ENISA guidelines.
- **Renewal Intervals:**
  - Evidence chains (ERS) are renewed every **X years** [to be defined contractually], or earlier if cryptographic weaknesses are identified.
  - AdES-LTA archival timestamps are renewed periodically to maintain validity.
- **Process:**

1. Evidence chain validity checked.

2. New hash-tree built using updated algorithms.
3. New timestamps obtained from QTSA.
4. Updated evidence appended to Preservation Object Container (POC).

- **Policy Reference:** Each renewal action is recorded with reference to the **Crypto Policy OID (1.3.6.1.4.1.47898.10.3)**.

5.5 Validation Policy

- **Policy Identifier: OID: 1.3.6.1.4.1.47898.10.2.1**
- **Scope:** Applied to all signatures and seals at the time of ingestion.
- **Basis:** Derived from ETSI EN 319 102-1 (validation of AdES signatures) and ETSI TS 119 441/442.
- **Application:** Ensures that only signatures/seals **valid at the time of ingestion** are preserved. Invalid signatures are rejected with a detailed validation report.

5.6 Policy Publication

- The **PSPPS (OID: 1.3.6.1.4.1.47898.10.1)** and all subordinate policy OIDs are published:
  - In this document (publicly available).
  - On the CERT DIGITAL QPS official website.
  - In audit reports, where applicable.
- Policies are updated periodically, with changes recorded in the **Change History (Annex C)**.

The PSPPS and all policy OIDs are published at the CERT DIGITAL QPS repository:
https://certdigital.ro/repository

6. Service Practices

6.1 Overview

The operational practices of **CERT DIGITAL QPS** are designed to ensure that all preservation activities are:

- Performed securely and consistently,
- Traceable and auditable,
- In compliance with the **PSPPS (OID: 1.3.6.1.4.1.47898.10.1)**,
- Executed according to the defined **preservation profiles (WOS/WST/WTS)**.

These practices apply to all operational phases, from ingestion to evidence renewal, retrieval, and eventual deletion.

6.2 Ingestion of Preservation Objects

- **Submission:**
  - Subscribers submit preservation objects (signatures, seals, or data with associated metadata) through the PreservePO interface.
  - Each submission specifies the intended profile OID (e.g., WST → 1.3.6.1.4.1.47898.10.1.2).
- **Validation:**
  - Submitted objects are validated against the **Validation Policy OID: 1.3.6.1.4.1.47898.10.2.1**.
  - Invalid objects are rejected with a detailed validation report.
- **Processing:**
  - If valid, the system collects all necessary validation data (certificates, CRLs, OCSP).
  - Preservation evidence is generated according to the **Evidence Format Policy OID: 1.3.6.1.4.1.47898.10.4**.
- **Acknowledgment:**
  - A Preservation Object Container (POC) is created.

- Returned to the subscriber (WOS/WTS) or stored securely (WST).

6.3 Evidence Generation

- **ERS-based evidence (RFC 4998/6283):**
  - Hash trees are computed from the preservation object and associated validation data.
  - Anchored by qualified timestamps (EN 319 421/422).
- **AdES-LTA augmentation:**
  - Archival timestamps and validation data embedded in the original signature container (e.g., PAdES-LTA).
- **Signature of evidences:**
  - All evidences are cryptographically bound and signed using HSM-protected keys.
  - Operations comply with the **Crypto Policy OID: 1.3.6.1.4.1.47898.10.3**.

6.4 Evidence Renewal

- **Triggering:**
  - Renewal is scheduled proactively before the end-of-life of algorithms, as per **Crypto Policy OID**.
  - Renewal may also be triggered by supervisory alerts (e.g., ENISA crypto updates).
- **Process:**

1. Existing evidence is validated.
2. New hash trees or archival timestamps are generated using updated algorithms.
3. A new qualified timestamp is appended.
4. The renewed evidence is stored in the updated POC.

- **Auditability:**
  - Each renewal action is logged and linked to the applied OIDs.
  - Renewal trace is available via the RetrieveTrace interface.

6.5 Retrieval of Evidences

- **RetrievePO/RetrievePOC:**
  - Subscribers and relying parties may request retrieval of complete preservation objects or evidence containers.
  - Returned object includes references to profile and policy OIDs.
- **ValidateEvidence:**
  - Allows on-demand verification of evidences.
  - Returns validation status (TOTAL-PASSED, FAILED, INDETERMINATE) in accordance with ETSI EN 319 102-1.
  - Validation reports explicitly reference the applied validation policy OID.

6.6 Deletion of Preservation Objects

- **WST:**
  - Preservation objects deleted only after contractual retention period ends or subscriber request.
  - Deletion is performed securely (multi-pass wipe or cryptographic erasure).
- **WTS:**
  - Objects deleted automatically after successful delivery of evidences.
- **WOS:**
  - No deletion required, as data is never stored by CERT DIGITAL QPS.

All deletions are logged, including references to affected OIDs.

6.7 Logging and Audit Trails

- **Event Logging:**
  - All key events (ingestion, validation, evidence generation, renewal, deletion) are logged.

- Logs include the profile OID and applied policies.

- **Audit Trails:**
  - Logs are protected from modification (WORM storage).
  - Retained for a minimum of 10 years, extendable as required by national law.
- **Access to Logs:**
  - Authorized auditors and supervisory bodies may request lifecycle logs via the RetrieveTrace API.

6.8 Incident Management

- **Detection and Response:**
  - Security monitoring systems detect anomalies in service operation.
  - Incidents classified (minor/major/critical) and escalated accordingly.
- **Reporting:**
  - Incidents with potential impact on preservation evidences are reported to the supervisory body in line with eIDAS obligations.
  - Subscribers are notified if their preservation objects may be affected.
- **Post-Incident Actions:**
  - Root-cause analysis performed.
  - Mitigation measures implemented.
  - Audit log entries retained for independent verification.

6.9 Business Continuity in Operations

- **Disaster Recovery:**
  - Evidence generation services can be restored within 4 hours (RTO).
  - Evidence integrity is guaranteed by off-site replicated storage (WST/WTS).
- **Fallback QTSA:**

- If the primary QTSA is unavailable, a secondary QTSA conforming to EN 319 421/422 is used.

- **Periodic Testing:**
  - Business continuity plans are tested at least annually.
  - Test results are documented and reviewed by management.

7. Roles and Responsibilities

7.1 Overview

The **CERT DIGITAL QPS** preservation service involves multiple roles and stakeholders, each with distinct responsibilities. Clear definition of roles ensures transparency, accountability, and compliance with **eIDAS** and **ETSI TS 119 511**.

The primary roles are:

- **Qualified Trust Service Provider (QTSP): CERT DIGITAL QPS**
- **Subscribers** (entities using the service)
- **Relying Parties** (verifiers of evidences)
- **External Providers** (e.g., Time-Stamping Authorities)

7.2 Qualified Trust Service Provider (QTSP)

The QTSP, operating under the identity **CERT DIGITAL QPS**, is legally responsible for the qualified preservation service.

Responsibilities:

- Operate the preservation service in accordance with:
  - **PSPPS OID: 1.3.6.1.4.1.47898.10.1**
  - Applicable profile OIDs (WOS/WST/WTS)
- Ensure compliance with eIDAS and ETSI standards.

- Maintain physical, logical, and organizational security as described in Chapter 4.
- Manage cryptographic keys in HSMs, following the **Crypto Policy OID: 1.3.6.1.4.1.47898.10.3**.
- Provide access to preservation evidences and validation results via defined APIs.
- Monitor algorithms and trigger timely evidence renewals.
- Retain audit logs and provide lifecycle traceability through the RetrieveTrace API.
- Notify supervisory authorities and affected subscribers in case of incidents affecting evidence integrity.
- Publish all relevant service policies at **https://certdigital.ro/repository**.

7.3 Subscribers

Subscribers are natural or legal persons who submit signatures, seals, or data to the CERT DIGITAL QPS preservation service.

Responsibilities:

- Use the service in compliance with applicable contracts, policies, and standards.
- Submit preservation objects in accepted formats and aligned with the **Crypto Policy OID**.
- Ensure that signatures/seals submitted were **valid at the time of ingestion**.
- Safeguard preservation evidences returned under WOS/WTS profiles.
- Notify the QTSP in case of suspected compromise of their submitted data or related credentials.
- Accept that invalid signatures/seals cannot be “repaired” by preservation.

7.4 Relying Parties

Relying parties are natural or legal persons who rely on preservation evidences provided by CERT DIGITAL QPS to verify the long-term validity of signatures and seals.

Responsibilities:

- Verify evidences using standard validation procedures (ETSI EN 319 102-1).

- Ensure they use up-to-date validation tools capable of interpreting preservation evidence formats.
- Consider the applied **validation policy OID** in their assessments.
- Accept that liability of CERT DIGITAL QPS is limited to the scope defined in Chapter 9 (Liability & Legal).

7.5 External Providers

CERT DIGITAL QPS may rely on external providers for specific trust services, particularly:

- **Qualified Time-Stamping Authorities (QTSA):**
  - Provide qualified timestamps (RFC 3161, EN 319 422).
  - Must be listed in the EU Trusted List.
  - Timestamps form the cornerstone of preservation evidences.
- **Validation Service Providers (optional):**
  - If external validation services are used (ETSI TS 119 441/442 compliant), their outputs are integrated into preservation evidences.

Responsibilities of External Providers:

- Operate in compliance with eIDAS and relevant ETSI standards.
- Guarantee integrity and availability of their services.
- Provide contractual assurances to CERT DIGITAL QPS regarding liability and continuity.

7.6 Supervisory Authority

The supervisory authority is the national body designated under eIDAS to oversee qualified trust service providers.

Responsibilities:

- Evaluate conformity of CERT DIGITAL QPS through regular audits (EN 319 403).
- Ensure CERT DIGITAL QPS is correctly listed in the EU Trusted List as a provider of qualified preservation services.

- Take corrective actions in case of non-compliance.

7.7 Summary of Roles and OID Associations

Role	Key Responsibilities	Relevant OIDs
QTSP (CERT DIGITAL QPS)	Operate service, manage crypto policy, generate and renew evidences, ensure compliance, publish policies	PSPPS OID: 1.3.6.1.4.1.47898.10.1 Crypto Policy OID: 1.3.6.1.4.1.47898.10.3 Evidence Format Policy OID: 1.3.6.1.4.1.47898.10.4
Subscriber	Submit valid signatures/seals, safeguard evidences (WOS/WTS), comply with formats & crypto rules	Preservation Profiles OIDs: .1.1 (WOS), .1.2 (WST), .1.3 (WTS)
Relying Party	Verify evidences, interpret validation policies, accept scope/limitations	Validation Policy OID: 1.3.6.1.4.1.47898.10.2.1
External Providers	Provide QTSA services and optional validation services	Linked indirectly through timestamps (EN 319 421/422)
Supervisory Authority	Audit and oversee compliance	EU Trusted List entry (PSES/Q)

8. Obligations

8.1 Overview

This section defines the obligations of all parties involved in the **CERT DIGITAL QPS** preservation service.
Obligations ensure that the service operates in a trustworthy manner and that responsibilities are clearly distributed among:

- **QTSP (CERT DIGITAL QPS)**
- **Subscribers**
- **Relying Parties**

- **External Providers**

8.2 Obligations of the QTSP (CERT DIGITAL QPS)

The Qualified Trust Service Provider, operating under **CERT DIGITAL QPS**, has the following obligations:

- **Compliance and Operation**
  - Operate the preservation service in accordance with:
    - **PSPPS OID: 1.3.6.1.4.1.47898.10.1**
    - Preservation profile OIDs: WOS (.1.1), WST (.1.2), WTS (.1.3)
    - Crypto Policy OID: 1.3.6.1.4.1.47898.10.3
    - Validation Policy OID: 1.3.6.1.4.1.47898.10.2.1
  - Maintain compliance with eIDAS Regulation and ETSI standards.
- **Security**
  - Protect all sensitive cryptographic material in certified HSMs.
  - Maintain physical, logical, and organizational security as outlined in Chapter 4.
  - Ensure integrity and confidentiality of subscriber data.
- **Service Availability**
  - Provide continuous and reliable access to preservation services (24/7).
  - Maintain high availability through redundancy and continuity measures.
- **Preservation and Renewal**
  - Validate all signatures/seals at ingestion against the declared validation policy.
  - Ensure timely renewal of evidences based on the cryptographic policy.
- **Transparency and Publication**
  - Publish the PSPPS and related service policies at **https://certdigital.ro/repository**.
  - Make public the list of supported OIDs and policies.

- **Notification and Incident Handling**
    - Notify subscribers and supervisory authorities of any incident impacting preservation evidences.
    - Provide mitigation and recovery measures.

8.3 Obligations of Subscribers

Subscribers using the CERT DIGITAL QPS service are obligated to:

- **Correct Usage**
    - Submit preservation objects in supported formats and compliant with the **Crypto Policy OID**.
    - Clearly specify the preservation profile (WOS/WST/WTS) to be applied.
    - Ensure that signatures/seals were **valid at the time of ingestion**.
- **Evidence Management**
    - In WOS and WTS profiles, safeguard preservation evidences and associated data after retrieval.
    - Retain evidence for the duration of the legal or business need.
- **Accuracy and Integrity**
    - Provide correct metadata and information during submission.
    - Refrain from submitting fraudulent, corrupted, or malicious data.
- **Notification**
    - Inform the QTSP promptly if evidence or related credentials are suspected to be compromised.
- **Contractual Compliance**
    - Adhere to contractual terms of service, including liability limitations and technical requirements.

8.4 Obligations of Relying Parties

Relying parties that use preservation evidences generated by CERT DIGITAL QPS are obligated to:

- **Evidence Verification**
  - Validate preservation evidences using tools conformant with ETSI EN 319 102-1.
  - Verify the applied validation policy OID (e.g., 1.3.6.1.4.1.47898.10.2.1).
- **Interpretation**
  - Interpret validation reports in the context of the declared policies and OIDs.
  - Accept that liability of CERT DIGITAL QPS is limited as described in Chapter 9.
- **Limitations**
  - Recognize that the preservation service guarantees long-term validity only for signatures/seals that were valid at ingestion.

8.5 Obligations of External Providers

External providers supporting CERT DIGITAL QPS (e.g., QTSAs, external validation services) are obligated to:

- **Time-Stamping Authority (QTSA):**
  - Provide qualified timestamps in compliance with EN 319 421/422.
  - Ensure continuous availability and reliability of time-stamping services.
  - Maintain their listing in the EU Trusted List.
- **Validation Service Providers (if applicable):**
  - Provide validation results in compliance with ETSI TS 119 441/442.
  - Guarantee the integrity and authenticity of validation responses.
- **Contractual Commitments:**
  - Maintain service-level agreements with CERT DIGITAL QPS covering reliability, security, and liability.

8.6 Summary of Obligations

Role	Obligations	OID References
QTSP (CERT DIGITAL QPS)	Operate service securely, ensure compliance, renew evidences, publish policies, notify incidents	PSPPS OID .10.1, Profile OIDs .10.1.1–.1.3, Crypto Policy OID .10.3, Validation Policy OID .10.2.1
Subscribers	Submit valid signatures, use correct profiles, safeguard evidences (WOS/WTS), notify compromise	Profile OIDs .10.1.1–.1.3, Crypto Policy OID .10.3
Relying Parties	Verify evidences, interpret validation results, accept liability limits	Validation Policy OID .10.2.1
External Providers	Provide qualified timestamps and optional validation results, maintain compliance with ETSI standards	Indirect reference to timestamp policies (EN 319 421/422)

9. Liability and Legal

9.1 Overview

The purpose of this section is to establish the **extent of liability** for the Qualified Trust Service Provider (QTSP), as well as limitations applicable to subscribers, relying parties, and external providers.
The liability framework is aligned with **Regulation (EU) 910/2014 (eIDAS)**, in particular Articles **13, 19, and 34**, and with requirements of **ETSI TS 119 511**.

9.2 Liability of the QTSP (CERT DIGITAL QPS)

As a **Qualified Trust Service Provider**, CERT DIGITAL QPS acknowledges its liability as defined under **eIDAS Article 13**:

- **Preservation Service Obligations:**

- CERT DIGITAL QPS is liable for ensuring that preservation evidences are generated, stored (if applicable), renewed, and delivered in compliance with this PSPPS (OID: 1.3.6.1.4.1.47898.10.1).
- Liability applies only when subscribers have complied with the obligations defined in Chapter 8.

- **Integrity of Evidences:**
  - CERT DIGITAL QPS guarantees that evidences issued under its service profiles (WOS/WST/WTS) are intact and correctly linked to the preserved object.
  - Preservation evidences include explicit references to applied profile OIDs for traceability.
- **Availability:**
  - CERT DIGITAL QPS is liable for providing service availability according to contractual Service Level Agreements (SLAs).
- **Renewal:**
  - CERT DIGITAL QPS is liable for performing timely renewals in accordance with the **Crypto Policy OID: 1.3.6.1.4.1.47898.10.3**.
- **Publication:**
  - CERT DIGITAL QPS ensures that the PSPPS, preservation policies, and service status information are published at **https://certdigital.ro/repository**.

9.3 Limitations of Liability

CERT DIGITAL QPS limits its liability under the following conditions:

- **Invalid Signatures at Ingestion:**
  - Liability does not extend to signatures or seals that were invalid at the time of ingestion, even if later preserved.
- **Improper Use of Evidences:**
  - Liability does not cover misuse of preservation evidences, including misinterpretation by relying parties or modification by subscribers.
- **External Dependencies:**

- Liability is limited for failures caused by external providers (e.g., QTSA downtime), provided that redundant providers were available.

- **Force Majeure:**
  - CERT DIGITAL QPS is not liable for service failures caused by events beyond its reasonable control (e.g., natural disasters, large-scale cyberattacks).
- **WOS Profile Limitations:**
  - Under the **WOS Profile (OID: 1.3.6.1.4.1.47898.10.1.1)**, CERT DIGITAL QPS is not liable for the long-term safekeeping of evidences, since these are delivered to and managed by the subscriber.

9.4 Liability of Subscribers

Subscribers are liable for:

- Submitting only valid signatures/seals at the time of ingestion.
- Safeguarding preservation evidences when using WOS/WTS profiles.
- Providing accurate information during submission.
- Misuse or loss of preservation evidences under their control.

9.5 Liability of Relying Parties

Relying parties are liable for:

- Properly validating evidences according to ETSI EN 319 102-1.
- Correctly interpreting applied OIDs and validation policies.
- Accepting the limitations of the preservation service as defined in this PSPPS.

9.6 Liability of External Providers

External providers (e.g., QTSA, validation service providers) are liable for the integrity and availability of their respective services in accordance with their contractual agreements with CERT DIGITAL QPS.

CERT DIGITAL QPS may transfer certain risks to external providers through legally binding contracts and SLAs.

9.7 Dispute Resolution

- **Procedure:**
  - Disputes between CERT DIGITAL QPS and subscribers or relying parties are to be resolved in good faith negotiations.
  - If unresolved, disputes shall be subject to arbitration or mediation as defined in contractual agreements.
- **Escalation:**
  - In case of regulatory disputes, the supervisory authority may intervene in accordance with national law implementing eIDAS.

9.8 Applicable Law and Jurisdiction

- This PSPPS and all contractual agreements governed by it shall be subject to the laws of **Romania**, as the country of establishment of CERT DIGITAL QPS.
- The competent courts of **Bucharest, Romania**, shall have jurisdiction over disputes, unless otherwise mandated by EU law.
- Cross-border recognition follows **eIDAS mutual recognition** of qualified trust services across EU Member States.

9.9 Liability Summary Matrix

Party	Liability Coverage	Exclusions	OID References
QTSP (CERT DIGITAL QPS)	Integrity of evidences, correct generation, renewal, publication	Invalid signatures at ingestion, misuse by subscriber, force majeure	PSPPS OID .10.1, Profiles OIDs .10.1.1–.1.3, Crypto Policy OID .10.3

Party	Liability Coverage	Exclusions	OID References
Subscriber	Valid input submission, safeguarding evidences	Invalid input, loss/misuse of evidences	Profile OIDs .10.1.1–.1.3
Relying Party	Correct validation of evidences	Misinterpretation, ignoring policy OIDs	Validation Policy OID .10.2.1
External Providers	Accuracy of timestamps, validation outputs	Service downtime beyond SLA	Linked to EN 319 421/422, 441/442

10. Audit & Compliance

10.1 Overview

The **CERT DIGITAL QPS** service is subject to periodic **conformity assessments** to demonstrate compliance with:

- **Regulation (EU) No 910/2014 (eIDAS)**
- **ETSI EN 319 401** (General Policy Requirements)
- **ETSI TS 119 511** (Preservation Policy & Security Requirements)
- **ETSI TS 119 512** (Preservation Protocols)
- **ETSI TS 119 312** (Cryptographic Suites)
- **ETSI EN 319 421/422** (Qualified Time-Stamping)
- **ETSI TS 119 441/442** (Validation Services)

Compliance is independently assessed by a **Conformity Assessment Body (CAB)** in line with **ETSI EN 319 403-1**.

10.2 Conformity Assessment Process

- **Frequency:**
    - Full conformity assessments are performed at least every **24 months**, in line with eIDAS requirements.

- Interim surveillance audits may be conducted annually or as mandated by the supervisory authority.

- **Scope:**
  - Verification of compliance with PSPPS OID **1.3.6.1.4.1.47898.10.1**.
  - Evaluation of operational practices (Chapters 6–8).
  - Inspection of cryptographic controls against Crypto Policy OID **1.3.6.1.4.1.47898.10.3**.
  - Confirmation of use of qualified time-stamping services (EN 319 421/422).
  - Verification of OID references in evidences, reports, and logs.
- **Deliverables:**
  - A formal **Conformity Assessment Report (CAR)** issued by the CAB.
  - Submission of the CAR to the supervisory authority.

10.3 Supervisory Authority Oversight

- The national supervisory authority designated under eIDAS oversees CERT DIGITAL QPS.
- The supervisory authority:
  - Reviews conformity assessment reports.
  - Maintains CERT DIGITAL QPS listing in the **EU Trusted List (TL)** as a **Qualified Preservation Service**.
  - May conduct **extraordinary audits** in case of incidents, complaints, or regulatory changes.
- **Trusted List Entry:**
  - Service type identifier: **http://uri.etsi.org/TrstSvc/Svctype/PSES/Q**
  - Qualifiers:
    - **ForSignatures**
    - **ForSeals**

10.4 Internal Compliance Monitoring

CERT DIGITAL QPS maintains an internal compliance program that includes:

- **Regular Internal Audits:**
  - At least annually, covering operational security, preservation workflows, and evidence renewal.
- **Vulnerability Management:**
  - Continuous monitoring of cryptographic algorithm status (per ETSI TS 119 312).
  - Prompt updates to the **Crypto Policy OID: 1.3.6.1.4.1.47898.10.3** when changes are required.
- **Policy Management:**
  - All updates to PSPPS and subordinate policies tracked in version history (Annex).
  - Revised policies published at **https://certdigital.ro/repository**.
- **Training & Awareness:**
  - All trusted roles receive annual compliance and security training.

10.5 Incident Reporting Compliance

- **eIDAS Obligations:**
  - CERT DIGITAL QPS complies with eIDAS **Article 19(2)** requiring notification of incidents to supervisory authorities without undue delay.
- **Subscriber Notification:**
  - Subscribers are notified of any incident that may affect the validity or availability of their evidences.
- **Relying Party Communication:**
  - Public statements may be published in the repository URL in case of incidents with systemic impact.

10.6 Continuous Improvement

- CERT DIGITAL QPS adopts a **risk-based approach** to compliance.
- Lessons learned from incidents, audits, and supervisory feedback are used to improve:
  - Security controls
  - Operational practices
  - Policies and procedures

10.7 Compliance Summary

Audit / Oversight Actor	Scope	Frequency	Reference
Conformity Assessment Body (CAB)	External conformity audit vs. ETSI/eIDAS	Every 24 months	ETSI EN 319 403-1
Supervisory Authority	Trusted List inclusion, regulatory oversight, extraordinary audits	Continuous + as needed	eIDAS Art. 17, 19, 20
Internal Compliance Team	Security audits, operational reviews, crypto updates, training	Annual + continuous monitoring	PSPPS OID .10.1, Crypto Policy OID .10.3

11. Technical Specifications

11.1 Overview

This section describes the technical specifications applied by **CERT DIGITAL QPS** in providing its qualified preservation service. It includes:

- Supported signature and seal formats,
- Supported evidence formats,

- Supported cryptographic algorithms,
- Preservation object container formats,
- Service protocol bindings,
- Use of OIDs in technical workflows.

11.2 Supported Signature and Seal Formats

CERT DIGITAL QPS supports preservation of the following advanced electronic signature (AdES) formats, as defined by ETSI standards:

- **CAdES (CMS Advanced Electronic Signatures)** – ETSI EN 319 122-1
- **XAdES (XML Advanced Electronic Signatures)** – ETSI EN 319 132-1
- **PAdES (PDF Advanced Electronic Signatures)** – ETSI EN 319 142-1
- **ASiC (Associated Signature Containers)** – ETSI EN 319 162-1

Preservation applies to both **signatures** and **seals** created in compliance with eIDAS requirements.

11.3 Supported Evidence Formats

Preservation evidences generated by CERT DIGITAL QPS comply with:

- **Evidence Record Syntax (ERS)** – RFC 4998
- **XMLERS (XML Evidence Record Syntax)** – RFC 6283
- **AdES-LTA Augmentation:**
    - PAdES-LTA (PDF)
    - XAdES-A (XML)
    - CAdES-A (CMS)

The choice of evidence format is governed by the **Evidence Format Policy OID: 1.3.6.1.4.1.47898.10.4**.

11.4 Cryptographic Algorithms and Key Lengths

All cryptographic primitives comply with **ETSI TS 119 312 (Cryptographic Suites)**.

- **Policy Identifier: Crypto Policy OID: 1.3.6.1.4.1.47898.10.3**
- **Accepted Hash Functions:**
  - SHA-256 (default)
  - SHA-384
  - SHA-512
- **Accepted Digital Signature Algorithms:**
  - RSA ≥ 2048 bits
  - ECDSA (P-256, P-384, P-521)
  - EdDSA (Ed25519, Ed448)
- **Accepted Symmetric Algorithms (internal use):**
  - AES-256 (encryption at rest, TLS cipher suites)
- **Time-Stamp Signature Algorithms:**
  - RSA/ECDSA/EdDSA per accepted hash functions
- **Crypto Renewal:**
  - Evidence renewed at least 3 years before algorithm end-of-life.

11.5 Preservation Object and Container Format

CERT DIGITAL QPS implements preservation object containers (POC) in compliance with **ETSI TS 119 511 Annex G**.

Each POC contains:

- The preserved data object (or approved digests in WOS profiles),
- Validation data (certificates, CRLs, OCSP responses),
- Preservation evidences (ERS or AdES-LTA),
- Metadata referencing the applied policy and profile OIDs.

OID References in POCs:

- **PSPPS OID:** 1.3.6.1.4.1.47898.10.1
- **Profile OID:** one of 1.3.6.1.4.1.47898.10.1.1 (WOS), .1.2 (WST), .1.3 (WTS)
- **Validation Policy OID:** 1.3.6.1.4.1.47898.10.2.1
- **Crypto Policy OID:** 1.3.6.1.4.1.47898.10.3
- **Evidence Format Policy OID:** 1.3.6.1.4.1.47898.10.4

11.6 Service Protocols

Service interfaces comply with **ETSI TS 119 512 (Preservation Service Protocols)**.

- **Bindings Supported:**
  - SOAP/XML (for legacy systems)
  - REST/JSON (for modern integrations)
- **Core API Operations:**
  - RetrieveInfo → Returns service metadata, supported profiles, and OIDs
  - PreservePO → Submit object for preservation (includes profile OID reference)
  - RetrievePO / RetrievePOC → Retrieve preserved object/evidence container
  - UpdatePOC → Trigger evidence renewal
  - ValidateEvidence → Validate preservation evidence (returns report with applied validation policy OID)
  - DeletePO → Secure deletion of objects (WST/WTS only)
  - RetrieveTrace → Retrieve traceability logs

11.7 Use of OIDs in Technical Workflows

OIDs are embedded in all relevant technical flows for traceability:

- **Ingestion:** Subscriber specifies preservation profile OID (.1.1 / .1.2 / .1.3).
- **Validation:** Results reference Validation Policy OID (1.3.6.1.4.1.47898.10.2.1).

- **Evidence Creation:** Metadata references Evidence Format Policy OID (1.3.6.1.4.1.47898.10.4).
- **Crypto Enforcement:** HSM and signing operations reference Crypto Policy OID (1.3.6.1.4.1.47898.10.3).
- **Publication:** All policy OIDs are documented at **https://certdigital.ro/repository**.

11.8 Data Size and Performance Constraints

- **Maximum preservation object size (WST/WTS):** [to be defined; e.g., 500 MB]
- **Maximum WOS approved digest size:** Up to 512 bytes per hash value.
- **Latency Targets:**
  - PreservePO → Evidence returned within ≤ 5 seconds (95% of cases).
  - ValidateEvidence → Report returned within ≤ 3 seconds (95% of cases).

11.9 Interoperability and Standards Compliance

- Preservation evidences and POCs can be validated with standard tools conforming to ETSI EN 319 102-1.
- All timestamps are issued by qualified TSAs listed in the EU Trusted List.
- Preservation objects are exportable for migration between systems.

11.10 Technical Specifications Summary

Area	Standard / Reference	OID Mapping
Signature Formats	CAdES, XAdES, PAdES, ASiC	–
Evidence Formats	RFC 4998 (ERS), RFC 6283 (XMLERS), AdES-LTA	Evidence Format Policy OID .10.4
Cryptography	ETSI TS 119 312	Crypto Policy OID .10.3
Validation	EN 319 102-1, TS 119 441/442	Validation Policy OID .10.2.1

Area	Standard / Reference	OID Mapping
Protocols	ETSI TS 119 512	–
Preservation Profiles	TS 119 511 (WOS/WST/WTS)	Profile OIDs .10.1.1–.1.3
PSPPS Reference	TS 119 511 §4.3	PSPPS OID .10.1

12. Appendices

12.1 Glossary

AdES (Advanced Electronic Signature): A type of electronic signature that complies with the requirements of EU Regulation 910/2014 (eIDAS) and ETSI standards, ensuring authenticity and integrity.

ASiC (Associated Signature Container): A format for bundling signed data and associated digital signatures into a single container.

CAdES (CMS Advanced Electronic Signatures): An AdES standard for signatures based on CMS (Cryptographic Message Syntax).

CERT DIGITAL QPS: The Qualified Trust Service Provider (QTSP) operating the Qualified Preservation Service described in this PSPPS.

Crypto Policy OID: An object identifier referencing the set of cryptographic algorithms and key lengths supported by the service.

eIDAS: Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

ERS (Evidence Record Syntax): A format defined in RFC 4998 for preserving digital signatures through cryptographic evidence records.

LTA (Long-Term Archival): A profile of AdES that incorporates timestamps and validation data to ensure long-term validity.

OID (Object Identifier): A globally unique identifier used to reference policies, profiles, and technical specifications.

PAdES (PDF Advanced Electronic Signatures): An AdES standard for signatures based on PDF.

PO (Preservation Object): The original data object, signature, or seal submitted for preservation.

POC (Preservation Object Container): The structure that encapsulates the preserved object, evidences, and metadata, including references to OIDs.

PGD (Proof of Existence of Data): An optional preservation profile proving that a given data object existed at a point in time.

PSPPS (Preservation Service Policy & Practice Statement): The present document defining policies and practices of the CERT DIGITAL QPS.

QTSA (Qualified Time-Stamping Authority): A trust service provider issuing qualified electronic timestamps under eIDAS.

QES (Qualified Electronic Signature): An advanced electronic signature created by a qualified signature creation device and based on a qualified certificate.

QSealS (Qualified Electronic Seal): An advanced electronic seal created by a qualified seal creation device and based on a qualified certificate.

TSL (Trusted List): The official list maintained by each EU Member State, containing information about recognized QTSPs and their services.

WOS/WST/WTS: ETSI-defined preservation storage models: Without Storage, With Storage, With Temporary Storage.

12.2 References

Primary Legislation:

- Regulation (EU) No 910/2014 (eIDAS Regulation)

ETSI Standards:

- ETSI EN 319 401 – General Policy Requirements for Trust Service Providers
- ETSI EN 319 403-1 – Conformity Assessment Requirements
- ETSI TS 119 511 – Policy & Security Requirements for Preservation Services
- ETSI TS 119 512 – Protocols for Preservation Services
- ETSI TS 119 312 – Cryptographic Suites

- ETSI EN 319 421 – Policy & Security Requirements for Time-Stamping Authorities
- ETSI EN 319 422 – Time-Stamp Protocols and Profiles
- ETSI TS 119 441 – Policy & Security Requirements for Signature Validation Services
- ETSI TS 119 442 – Protocols for Signature Validation Services
- ETSI EN 319 102-1 – Procedures for AdES Signature Validation

RFCs:

- RFC 4998 – Evidence Record Syntax (ERS)
- RFC 6283 – XML Evidence Record Syntax (XMLERS)
- RFC 3161 – Time-Stamp Protocol

Additional Guidance:

- ENISA Cryptographic Guidelines
- NIST SP 800-131A – Cryptographic Key Management Guidance

12.3 Contact Information

Organization:	Centrul de Calcul S.A.
Legal Form:	Qualified Trust Service Provider under Regulation (EU) 910/2014
Address:	Tudor Vladimirescu street, No 17, Târgu Jiu, Gorj România
Repository URL:	https://certdigital.ro/repository
Email:	office@certdigital.ro
	sediu@centruldecalcul.ro
Phone:	+40 31 94 66
	+40 253 214 767

All inquiries regarding this PSPPS should be directed to the compliance team at the above contact details.