DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

PRESERVATION SERVICE POLICY AND PRACTICE STATEMENTS

VERSION 1.0 – 16/06/2025

[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	Edition n.º	Content
16/06/2025	1.0	Initial draft

RELATED DOCUMENTS

Document Details	Author(s)
Certification Practice Statement	DigitalSign
Signature Validation Service Policy And Practice Statements	DigitalSign

AUTHORIZATIONS

Created by	Approved by
	

LEGAL NOTICE

Any question or request for information regarding the content of this document should be directed to svs@digitalsign.pt.

CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

The present document is entitled "Preservation Service Policy and Practice Statements". The purpose of the Policy and the Practice Statement is to meet the general requirements in order to provide trust and confidence in electronic transactions including, amongst others, the generally applicable requirements from Regulation (EU) No. 910/2014 establishing a legal framework for electronic signature and electronic seal, including their preservation. Therefore, the present document is to define the practices and procedures used to support the preservation rules regarding Qualified Signatures and Qualified Seals in conformity with Regulation (EU) No 910/2014, European Standards – ETSI, Legal acts of Portugal and guarantees that this service:

- Applies operational procedures and security management procedures that exclude any possibility for manipulation of the data and the status of the preserved qualified electronic signatures or qualified electronic seals;
- Capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period, according with the requirements of Articles 34 and 40 of Regulation (EU) No. 910/2014;
- Applies the requirements and recommendations of the European Commission applicable to a service for qualified long-term preservation without storage;
- The data to be preserved is stored on the client side. The preservation service neither stores the electronic document nor the preservation evidences. Evidences are produced synchronously and are included in the response. The preservation service only keeps traces of its actions to be able to provide records of its activities.
- The preservation service without storage neither stores the data to be preserved nor a hash of the data nor evidences.
- The submitter submits one or more electronic document and immediately retrieves a response with one or more preservation evidence(s) for it (synchronous mode).
- Fulfils the technical procedures for the preservation of qualified electronic signatures or qualified electronic seals according with requirements of ETSI TS 119 511, ETSI TS 119 512 and ETSI TS 119 172-4;
- The signature (OID) validation policy is in line with ETSI TS 119 172-4 and unambiguously states that the signature is qualified according to Regulation (EU) No. 910/2014;

Furthermore, the present document has been prepared in accordance with current Portuguese legislation and European legislation and standards for the provision of qualified trust services.

1.1.1. NORMATIVE REFERENCES

- **Regulation (EU) No 910/2014** of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- **ETSI EN 319 401** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- **ETSI SR 019 510** Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures;
- **ETSI TR 119 001** "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations";
- **ETSI TS 119 312** Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- **ETSI TS 119 102-2** "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report";
- **ETSI EN 319 122-1** "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures";
- **ETSI EN 319 122-2** "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures";
- **ETSI EN 319 132-1** "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures";
- **ETSI EN 319 132-2** "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures";
- **ETSI EN 319 142-1** "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures";
- **ETSI EN 319 142-2** "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles";
- **ETSI TS 119 172-1** "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents";
- **ETSI TS 119 172-4** "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted Lists";
- **ETSI TS 119 442** "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services";
- **ETSI EN 319 403** "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers";

- **ETSI TS 119 312** "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites";
- **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- **ETSI EN 319 411-1** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements";
- **ETSI EN 319 411-2** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates";
- **ETSI EN 319 412-4** "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates";
- **ETSI TS 119 172-2** "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies";
- **ETSI TS 119 172-3** "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 3: ASN.1 format for signature policies";
- **IETF RFC 3647** "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

1.1.2. USERS AND FIELDS OF APPLICATION OF THE PRESERVATION SERVICE

Preservation service allows extension of the validity status of a qualified electronic signature or qualified electronic seal over long periods of time in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or the loss of the ability to check the validity status of public key certificates. The Users of the present preservation service provided by DigitalSign can be legal or natural persons. They can be used when an User wishes to delegate the preservation of validity status of the electronic signatures and seals to DigitalSign.

1.1.3. QTSP IDENTIFICATION

DigitalSign – Certificadora Digital, S.A.
Largo Pe. Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira, Guimarães
Portugal
E-mail: geral@digitalsign.pt
Support Phone: +351 253 560 650

1.1.4. SUPPORTED NAME AND IDENTIFIER OF THE DOCUMENT

The Preservation Service Policy is identified with a registered formal object identifier (OID) 1.3.6.1.4.1.25596.6.1.1.

1.2. DEFINITIONS AND ABBREVIATIONS

1.2.1. DEFINITIONS

- **Container**: data object, which contains a set of data objects and optional additional information, which describes the contained data objects and optionally its content and its interrelationships;
- **Data object**: actual binary/octet data being operated on (e.g. transformed, digested, or signed) by an application and which may be associated with additional information like an identifier, the encoding, size or type;
- **Delta preservation object container**: special preservation object container describing the difference to an already existing preservation object container;
- **Digital signature techniques**: techniques based on digital signatures, time-stamps or evidence records;
- **eIDAS Regulation:** 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.
- **EU qualified time-stamping authority:** a qualified trust service provider issuing qualified electronic time-stamps as laid down in Regulation (EU) No. 910/2014;
- **Evidence record**: unit of data, which can be used to prove the existence of an archived data object or an archived data object group at a certain time;
- **Expected evidence duration**: for a preservation service with temporary storage or without storage, duration during which the preservation service expects that the preservation evidence can be used to achieve the preservation goal;
- **General Data Protection Regulation:** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- **Information Security Management System:** certified Information Security Management System according to ISO/IEC 27001.
- **Long-term**: time period during which technological changes may be a concern;
- **Long-term preservation**: extension of the validity status of a digital signature over long periods of time and/or extension of provision of proofs of existence of data over long periods of time, in spite of obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or of the loss of the ability to check the validity status of public key certificates;
- **Notification protocol**: protocol used by a preservation service to notify the preservation client;

- **OCSP:** a protocol providing online certificate status information (OCSP or CRL);
- **Preservation client**: component or a piece of software which interacts with a preservation service via the preservation protocol;
- **Preservation evidence**: evidence produced by the preservation service which can be used to demonstrate that one or more preservation goals are met for a given preservation object;
- **Preservation evidence augmentation**: addition of data to an existing preservation evidence to extend the validity period of that evidence;
- **Preservation evidence policy**: set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence;
- **Preservation goal**: one of the following objectives achieved during the preservation time frame: extending over long periods of time the validity status of digital signatures, providing proofs of existence of data over long periods of time, or augmenting externally provided preservation evidences;
- **Preservation mechanism**: mechanism used to preserve preservation objects and to maintain the validity of preservation evidences;
- **Preservation interface**: component implementing the preservation protocol on the side of the preservation service;
- **Preservation manifest**: data object in a preservation object container referring to the preservation data objects or additional information and metadata in the preservation object container;
- **Preservation object**: typed data object which is submitted to, processed by or retrieved from a preservation service;
- **Preservation object container**: container which contains a set of data objects and optionally related metadata providing information about the data objects and optionally preservation manifest(s) specifying its content and relationships;
- **Preservation object identifier**: unique identifier of a (set of) preservation object(s) submitted to a preservation service;
- **Preservation period**: for a preservation service with storage, duration during which the preservation service preserves the submitted preservation objects and the associated evidences;
- **Preservation profile**: uniquely identified set of implementation details pertinent to a preservation storage model and one or more preservation goals which specifies how preservation evidences are generated and validated;
- **Preservation protocol**: protocol to communicate between the preservation service and a preservation client;

- **Preservation scheme**: generic set of procedures and rules pertinent to a preservation storage model and one or more preservation goals which outlines how preservation evidences are created and validated;
- **Preservation service**: service capable of extending the validity status of a digital signature over long periods of time and/or of providing proofs of existence of data over long periods of time;
- **Preservation service provider**: trust service provider providing a preservation service;
- **Preservation service policy**: trust service policy for a preservation service preservation service;
- **Practice statement**: trust service practice statement for a preservation service;
- **Preservation storage model**: one of the following ways of implementing a preservation service: with storage, with temporary storage, without storage;
- **Preservation submitter**: legal or natural person using the preservation client to submit the submission data object;
- **Preservation subscriber**: legal or natural person bound by agreement with a preservation trust service provider to any subscriber obligations;
- **Proof of existence**: evidence that proves that an object existed at a specific date/time;
- **Proof of integrity**: evidence that data has not been altered since it was protected;
- **Qualified Preservation Service:** A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.
- **Qualified Trust Service Provider:** An entity which provides one or more Qualified Trust Services and is granted the qualified status by the Supervisory Body**.**
- **Signer**: entity being the creator of a digital signature;
- **Submission data object**: original data object provided by the client;
- **Supervisory Body:** The authority that is designated by a member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS Regulation in the territory of that member state.
- **Time assertion**: time-stamp token or an evidence record;
- **Time-stamp**: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time;
- **Time-stamping authority**: trust service provider which issues time-stamps using one or more time-stamping units;

- **Time-stamping service**: trust service for issuing time-stamps;
- **Time-stamping unit**: set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time;
- **Trusted list**: list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation;
- **User**: application or human being that interacts with the Preservation Service.
- **Validation data**: data that is used to validate an electronic signature;

1.2.2. ABBREVIATIONS

AUG Augmentation goal
CSA Certificate Status Authority
EUMS European Union Member State
OVR Overall
PDS Preservation of Digital Signatures
PGD Preservation of General Data
PO Preservation Object
POC Preservation Object Container
PRP Preservation service Protocol
PSP Preservation Service Provider
QES Qualified Electronic Signature or Qualified Electronic Seal
SigS digital Signature creation Service
SubDO Submission Data Object
TS Trust Service
TSA Time-Stamping Authority
TSP Trust Service Provider
ValS Validation Service
WOS Without Storage
WST With Storage
WTS With Temporary Storage

1.3. POLICIES AND PRACTICES

1.3.1. ORGANIZATION ADMINISTRATING THE QTSP DOCUMENTATION

DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal

1.3.2. CONTACT PERSON

Álvaro Matos
DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: svs@digitalsign.pt
Phone: +351 253560650

1.3.3. QTSP (PUBLIC) DOCUMENTATION APPLICABILITY

DigitalSign's public documentation which is related to the provision of the qualified preservation service has been made available to all Users and is published on the internet on https://pki.digitalsign.pt/.

Present policy and practice statement

The management group of this policy evaluates the compliance and internal applicability of this Preservation Service Practice Statement, submitting it to the approval of DigitalSign's Administration, which is the competent body to determine its suitability to the applicable legislation.

The internal approval of this documentation and following fixes and/or updates are made by DigitalSign's Administration. After internal approval, should be assessed their compliance, as described in the previous paragraph. Corrections and/or updates shall be published in the form of new versions of the Preservation Service Practice statement, replacing any previous version.

Policy OID is referred in section 1.1.4. of this document.

Terms and conditions

DigitalSign has its terms and conditions available on https://pki.digitalsign.pt/.

Risk assessment and Information security policy

DigitalSign has an information security management system based on the standard ISO/IEC 27001, ensuring that facilities, procedures, personnel, equipment and products comply with all regulatory and safety requirements applicable to the exercise of its activity. Thus, it uses reliable systems and products, protected from modification, performs planned security audits and prepares reports of incidents caused by possible security or operation failures, triggering the respective corrective actions in a timely manner.

Ensures that the procedures used to ensure operational safety levels, physical and systems, in accordance with the adopted standards, are documented, implemented and updated, and maintains an inventory of assets with the respective classification, in order to characterize their protection needs.

2. TRUST SERVICE MANAGEMENT AND OPERATION

2.1. INTERNAL ORGANIZATION AND ORGANIZATION RELIABILITY

DigitalSign conducts its operations through certification and registration authorities in line with the adopted policies and practices. The contact information of the certification and registration Authorities is available on the website of DigitalSign. In order to achieve reliability and security in its operations related to the provision of trust services, DigitalSign applies the requirements specified in ETSI EN 319 401, including:

- DigitalSign guarantees high level of security and reliability of its operations;
- DigitalSign offers its Qualified Trust Services under non-discriminatory practices;
- DigitalSign ensures that all requirements defined in ISO/IEC 27001 Statement of Applicability and this Practice Statement are implemented and remain applicable to the Qualified Trust Services provided;
- DigitalSign complies with all legal obligations applicable to the provisioning of its Qualified Trust Services;
- DigitalSign fulfils general security requirements set out in article 19 of the eIDAS Regulation as further developed in ETSI EN 319 401;
- In relation to the validation of Qualified Trust Services, DigitalSign provides validation of (Qualified) Electronic Signatures and Seals in accordance with article 33 of the eIDAS Regulation and relevant sections of ETSI TS 119 102 Electronic Signatures and Infrastructures;
- The provision of Qualified Trust Services is subject to an external audit performed at least every 12 months by a Conformity Assessment Body (CAB) and the qualified status is supervised by GNS (Gabinete Nacional de Segurança), the Portuguese National Supervisory Body;
- Records concerning the operation of the Qualified Trust Services are made available to affected parties upon legitimate request for the purposes of providing evidence of the correct operation of the Trust Services for the purposes of legal proceedings;
- DigitalSign has the necessary financial stability and resources for operation in accordance with this document;
- DigitalSign maintains insurance of its civil liability in accordance with the applicable legislation, to cover obligations arising from its operations and in line with Article 13 of eIDAS Regulation.

2.1.1. SEGREGATION OF DUTIES

DigitalSign has established and maintains a policy of strict control procedures to ensure segregation of duties, based on the responsibilities of each task, and ensuring that multiple Trusted Persons are required to perform sensitive tasks.

2.1.2. DIGITALSIGN'S LIABILITY

In accordance with Article 13 of the eIDAS Regulation, DigitalSign will only be liable in relation to the DigitalSign qualified preservation service for damages caused intentionally or negligently due to a failure to comply with its obligations under the eIDAS Regulation.
Any conflicting obligations and the scopes of responsibility shall be severed in order to minimise any possibility for unlawful or unintentional change or misuse of the TSP's assets.

2.1.3. CONFIDENTIALITY

The DigitalSign preservation service guarantees the confidentiality of a signed document according to applicable European and national laws on privacy and data protection. DigitalSign particularly and immediately erases all copies of a received SD, if any, from its servers after having performed a requested transaction.

2.2. HUMAN RESOURCES

In conformity with our global CPS (Certificate Practice Statement), DigitalSign ensures:

- All members of the personnel staff that involved for the provision of the DigitalSign services are either employees of DigitalSign or authorised and qualified personnel of sub-contracting entities providing sub-contracted certification and/or time stamping component services;
- All members are subject to personnel and management practices that DigitalSign follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and related services;
- DigitalSign requires that staff try to be a Trusted Person, must provide evidence of background, qualifications, experience and clearance necessary to perform their possible liability tasks, competently and satisfactorily.
- DigitalSign acting as QTSP obtains a signed statement from each member of the staff on not having conflicting interests with the QTSP, on the preservation of confidentiality and the protection of personal data;
- DigitalSign ensures that all tasks, roles and responsibilities with respect to the DigitalSign trusted services are described in job descriptions and made available to the concerned personnel. These job descriptions are defined from the view point of segregation of duties and least privileges, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness;
- Personnel shall exercise administrative and management procedures and processes that are in line with the DigitalSign information security management procedures;
- Managerial personnel possess expertise in the field of electronic signature and related services, in risk assessment and information security as well as possess familiarity with security procedures for personnel with security responsibilities;

- Training and awareness-raising actions (internal and external);
- Periodic review of the Trusted Person Statute.

2.3. ASSET MANAGEMENT

DigitalSign ensures implementation and maintains appropriate level of protection to its assets and information systems. For this purpose, DigitalSign maintains an inventory of all information assets (both virtual and physical) and their owners, identifying their threats and assigning a classification for the protection requirements to those assets consistent with the risk analysis.

2.4. ACCESS CONTROL

In accordance with the information security policy, the DigitalSign's system access is limited to authorized individuals. In particular, DigitalSign ensures the following measures, among others:

- DigitalSign's personnel is identified and authenticated before using critical applications related to the service
- Use of firewalls to protect the internal network domains from unauthorized access including access by subscribers and third parties;
- Firewalls are configured to prevent all protocols and accesses not required for the operation of the QTSP;
- Constant monitoring of systems and recording of information security events;
- Existence of Antivirus protection – automated systems of virus detection and elimination;
- Separation of management flows for administrators and operators, according with the segregation of duties rule;
- Sensitive data are protected against being revealed through storage and restriction of access thereto for unauthorized Users.

2.5. CRYPTOGRAPHIC CONTROLS

DigitalSign applies the requirements for cryptographic controls specified in clause 7.5 of ETSI EN 319 401. In addition, DigitalSign also applies the following particular requirements:

- Time-stamps used in preservation process come from a TSA that follows state-of-the-art practices for policy and security requirements for trust service providers issuing time-stamps, according with Timestamp Policy and TSA Practice Statement, available at: https://pki.digitalsign.pt/.

2.6. PHYSICAL AND ENVIRONMENTAL SECURITY

DigitalSign applies the requirements of clause 7.6 of ETSI EN 319 401 concerning the physical and environmental security. Physical access to DigitalSign offices & data centre facilities is appropriately restricted to authorized personnel, in conformity to our global CPS (Certification Practice Statement). Safeguard measures are in place to protect critical assets and ensure continuity.

- Elaboration and maintenance of a list of persons authorized to access the facilities where the servers and system equipment are located;
- Monitoring of entrances - all existing doors and installations have access control with an anti-passback system, not being allowed to leave a specific room without registration;
- Organization of the facilities structure in four security levels;
- Reinforcement of access control through the use of an identification proximity card and, in some cases, an additional need for biometric authentication (fingerprint reader) and application of the Two Men Rule. In particular, areas used to create and store cryptographic material enforce dual control, each through the use of two-factor authentication including biometrics;
- Existence of a CCTV system and armoured security doors;
- Existence of glass break detectors, movement and open/closed door sensors;
- Location of critic assets at level 4 of security equipment;
- Personnel without escort, including non-accredited staff or visitors are not allowed in such security areas;
- Realization of periodic inspections and updates.

2.7. OPERATION SECURITY

DigitalSign applies the requirements specified in clause 7.7 of ETSI EN 319 401 in order to ensure security of its operations, as per information security policy. DigitalSign uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

- DigitalSign employs a layered security approach for protection against malware;
- The integrity of the systems and information of DigitalSign are protected against viruses, malicious and unauthorised software;
- Backup copies are ensured for all DigitalSign online products and services provided for clients;
- Realization of event logging, protection of log information, administrator and operator logs, clock synchronization, as well as control of operational software, via the installation of software on operational systems;
- 24/7 monitoring on the infrastructure, network and security components;

Detailed descriptions of implemented operation security controls are available as internal document(s).

2.8. NETWORK SECURITY

DigitalSign ensures that network security controls (including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc.) are implemented in compliance with the standard ETSI EN 319 401, specifically with 7.8 clause.
Detailed descriptions of implemented network security controls are available as internal document(s).

2.9. INCIDENT MANAGEMENT

The management of security incidents and improvements is integrated within the overall operations model and the standard incident management procedures there. Incidents are logged into an internal tool and assigned based on their classification. Security and privacy incidents are also forwarded to the CISO or DPO respectively, to keep him/her informed, and take immediate appropriate action.
Detailed descriptions of implemented incident management controls are available as internal document(s).

2.10. COLLECTION OF EVIDENCE

DigitalSign applies the requirements specified in clause 7.10 of ETSI EN 319 401 with respect to collection of evidence.
In addition, the following particular requirements are applied:

- DigitalSign implements event logs, marked with the time of the event, to capture information needed for later proofs, including type of the event, the event success or failure and an identifier of the person and/or component at the origin for such an event;
- Any signature preservation is logged. As a standard, DigitalSign does not log the identity of the User;
- The archived data are stored for a period of 7 years. After expiration of this period the archived data are destroyed;

As above mentioned, DigitalSign maintains records concerning the operation of the services in scope for the purposes of providing evidence of the correct operation of these services. These records will only be disclosed to law enforcement authorities under court order and to persons with right to access to them upon legitimate request. Such information is managed in line with DigitalSign Personal Data Protection Policy.

2.11. BUSINESS CONTINUITY MANAGEMENT

DigitalSign applies the requirements specified in clause 7.11 of ETSI EN 319 401 with respect to business continuity management.
DigitalSign establishes the necessary measures to ensure full and highly automated recovery of the DigitalSign certification and time stamping services in case of a disaster, corrupted servers, software or data.

A Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

2.12. QTSP TERMINATION AND TERMINATION PLANS

DigitalSign has up-to-date termination plan in accordance with clause 7.12 of ETSI EN 319 401.
DigitalSign has created a termination plan that deals with termination notification, subcontractor's management, information maintenance, private key destruction, termination phasing and updating of the termination plan procedure. DigitalSign has taken measure to ensure that the execution of the termination plan is executed in case of bankruptcy.

2.13. COMPLIANCE

DigitalSign applies the requirements specified in clause 7.13 of ETSI EN 319 401 in order to ensure compliance with the legal requirements.
In particular,

- DigitalSign guarantees that it operates in a legal and trustworthy manner and it provides evidence on how it meets the applicable legal requirements;
- The CPS and provision of DigitalSign PKI Services are compliant to relevant and applicable European and national laws;
- DigitalSign employs personnel with the required legal skills and has that fulfil the required roles in order to guard the correct implementation of legal requirements;
- DigitalSign ensures that appropriate technical and organisational measures are undertaken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data, guaranteeing that personal data are processed in accordance with Regulation (EU) No. 2016/679 (commonly, GDPR).
- DigitalSign ensures the review of the present document whenever changes occur to the preservation service.

3. PRESERVATION SERVICE DESIGN

3.1. PRESERVATION SERVICE PROCESS REQUIREMENTS

The Preservation Service process complies with ETSI EN 319 401, ETSI TS 119 511 and ETSI TS 119 512.

Therefore, DigitalSign complies with the following requirements:

- DigitalSign supports a Preservation Service Policy and Practice Statements and the dedicated Terms and Conditions;
- DigitalSign supports service policy with OID 1.3.6.1.4.1.25596.6.1.1.
- The preservation profile that support the preservation service is described in section 3.2.2.;
- The availability of SubDOs and related evidence is achieved through physical, informational and organizational security controls as described in this document;
- External organizations are not involved in the operation of DigitalSign when providing a storage service;
- The process of requesting incoming/outgoing packets includes receiving a written request from a User of the service or another person, which describes exactly which data is the subject of the request. DigitalSign processes the request, reserving the right to reject it without giving any reasons. If DigitalSign approves the request, the User receives the requested data in a securely protected electronic form;
- DigitalSign ensures authentication of the sender;
- Sending of data objects is secured by cryptographic protocols of DigitalSign in a way that excludes any possibility of unnoticed change in the data object;
- The availability, integrity and confidentiality of data objects is guaranteed by DigitalSign;
- The integrity of the data objects is protected when exchanged between the sender and DigitalSign;
- The Preservation Service uses Qualified Time Stamps;
- In order to provide the Preservation Service, DigitalSign does not use external qualified certification service providers.
- The Preservation Service uses a Qualified Electronic Signature Validation Service – provided by DigitalSign, available at: https://verify.digitalsign.pt/signaturesValidator/validator - to guarantee the validation of the qualified electronic signatures and/or qualified electronic seals.

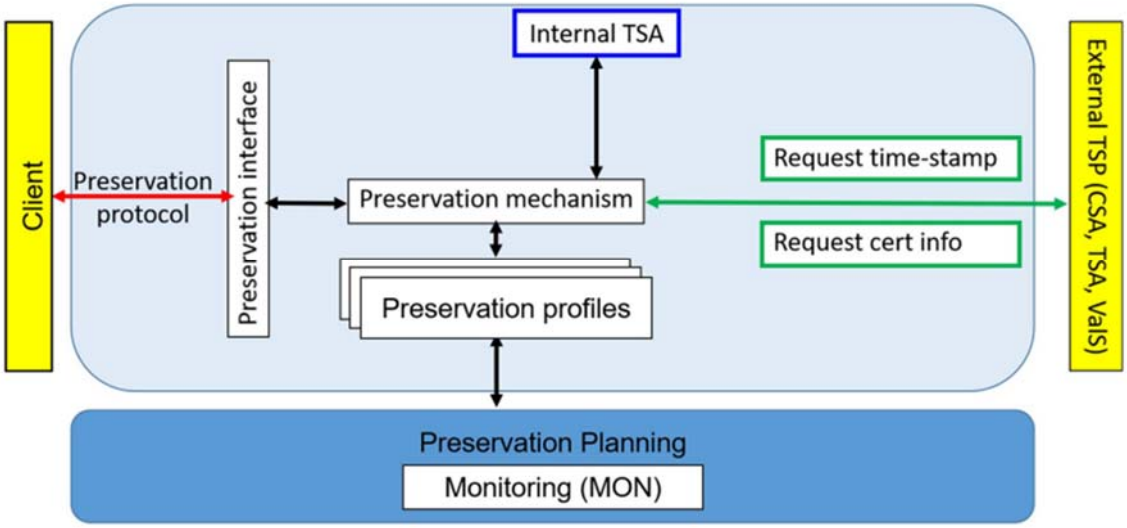
3.1.1. FUNCTIONAL MODEL/WORKFLOW OF THE PRESERVATION SERVICE

The definition of Preservation Service by ETSI TS 119 511 foresees three preservation storage models: preservation service with storage (WST), preservation service with temporary storage (WTS), and preservation service without storage (WOS).
DigitalSign provides a Preservation Service with a functional model of a preservation service without storage [WOS]:

- The User submits an electronic document on the preservation service when preservation event occurs. Preservation is executed if a new electronic document/container preservation should be started, or if already preserving electronic document/container should be re-augmented, since expected evidences (used within qualified electronic signatures contained in the preserved electronic document/container) duration is going to expire. The management of the preservation events is performed by the User, not by the preservation service.
- Preservation service receives an electronic document/container containing at least one qualified electronic signature or qualified electronic seal.
- Preservation service validates the qualified electronic signatures and/or the qualified electronic seals within it.
- Preservation service checks the qualified electronic signatures and/or the qualified electronic seals to be preserved.
- Preservation service checks whether every qualified electronic signature and/or qualified electronic seal to be preserved already reached LTA level.
- Preservation service performs augmentation of the qualified electronic signatures and/or qualified electronic seals. After this augmentation, all qualified electronic signatures and/or qualified electronic seals reaches LTA level.
- Preservation service performs the augmentation by adding new archival data to extend their validity status. Preservation evidences are included into the qualified electronic signatures and/or qualified electronic seals presented in the electronic document/container.
- Preservation service prepares a response to the User. Preservation service calculates new expected evidence duration and augmentation period. On success, the response contains upgraded electronic document/container with preservation evidences included within the qualified electronic signatures and/or qualified electronic seals. Otherwise, the rejection or failure reason is returned.
- The User receives updated electronic document/container from the preservation service.
- The User must store the updated electronic document/container in its own storage. The User should update next augmentation time (and expected evidence duration) for the updated electronic document/container to be able to raise the next preservation event on time.

The preservation service uses DigitalSign services, including the Certification Authority for the Issuance of Qualified Electronic Time Stamps, the Operations Certifying Authority and the Qualified Validation Authority. The preservation service uses a reliable time source (UTC) while creating preservation evidence, according with Timestamp Policy and TSA Practice Statement, available at: https://pki.digitalsign.pt/. The preservation service provided by DigitalSign to its Users works with secure and reliable cryptographic algorithms in the process of generation and extension of the reliability of any digital objects in the preserved evidence beyond their technological validity status.

3.1.2. ARCHITECTURE: PRESERVATION SERVICE WITHOUT STORAGE (WOS)



3.1.3. PRESERVATION OPERATIONAL PROTOCOL

The communication channel between the User and the preservation service is secured. DigitalSign ensures the security of User authentication and privacy. In this sense, DigitalSign uses a protocol in accordance with the requirements of ETSI TS 119 512. The protocol used is protected against unauthorized use. The preservation service allows to obtain traces of all operations associated with a particular preservation object identifier.

3.1.4. OPERATIONAL NOTIFICATION PROTOCOLS

The preservation service does not define and does not provide a notification protocol.

3.1.5. PRESERVATION EVIDENCES

The evidences produced by the preservation service, includes a time-stamp token, according with Timestamp Policy and TSA Practice Statement, available at: https://pki.digitalsign.pt/.
If necessary, preservation evidence may be validated by using a qualified validation service in the meaning of Regulation (EU) 910/2014, if that is applicable to the respective evidence format. In this since, DigitalSign recommends using DS Verify, available at: https://verify.digitalsign.pt/signaturesValidator/validator.

Once the preservation evidence has been generated, no data is retained or stored thereafter.

3.1.6. PRESERVATION OF DIGITAL SIGNATURES

The preservation service will verify the submitted data object according to the signature validation policy supported by the preservation profile. To extend the ability to validate a digital signature and to maintain its validity status, the preservation service shall, at the minimum, provide a proof of existence of the signature and of the validation data needed to validate the signature using digital signature techniques.

To extend the ability to validate a digital signature and to maintain its validity status, the preservation service, on one side, provide a proof of existence of the signature and of the validation data needed to validate the signature and on the other side a proof of existence of the signed data.

Thus, in this case, the preservation of digital signatures is achieved by timely digital signature augmentation. This is performed through 3 stages:

Validation data collection: It is performed at the time of submission, if not yet present in the qualified electronic signature or qualified electronic seal.

LTA level assurance: It is performed immediately after grace-period elapsed (or at the time of submission, if grace-period is already elapsed), if validation data or part of it is missing, or all covering qualified time stamp is not presented within digital signature (LTA level is not reached). This assures, that all required validation data is collect at the time it is still available and still suitable for validation. New archival time stamp, which covers all digital signature data, validation data and actually signed data, is obtained and included into the digital signature. This provides the proof of existence for validation data, previously added time stamps and also for actually signed data. Supported preservation object formats assures, that archival time stamp directly covers the signed data even if detached signatures are used.

LTA level preservation assurance: It is performed when preservation event is raised by the maintenance process. New archival time stamp is obtained and included into the digital signature. This provides the new proof of existence for previously added time stamps, validation data, signed data and protection against certificate expiration and possible future obsolescence of the used cryptographic algorithms.

Digital signature augmentation (and validation) is based on the standard ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation [EN 319 102-1] and is performed according Signature validation policy of DigitalSign, available at: https://pki.digitalsign.pt/.

3.2. PRESERVATION SCHEME

3.2.1. PRESERVATION SCHEME WITH SIGNATURE AUGMENTATION AND WITHOUT STORAGE

- **Unique Identifier**

The preservation scheme with signature augmentation and without storage is identified by the following URI: http://uri.etsi.org/19512/scheme/pds+wos+aug.

- **Preservation goal(s)**

Extending over long periods of time the validity status of digital signatures, which is indicated by the URI: http://uri.etsi.org/19512/goal/pds.

- **Preservation storage model**

The present preservation scheme supports the preservation storage model "without storage" according to clause 4.3.3 of ETSI TS 119 512.

- **Supported operations**

PreservePO according to clause 5.3.3. of ETSI TS 119 512.

- **Generation and Validation of Preservation Evidences**

Supported formats for input: **CAdES digital signature** according to ETSI EN 319 122; **XAdES digital signature** according to ETSI EN 319 132; **PAdES digital signature** according to ETSI EN 319 142.
Supported formats of preservation evidence: **CAdES Archive Time Stamp V3** according to ETSI EN 319 122; **XAdES Archive Time Stamp** according to ETSI EN 319 132; **PAdES Document Time-Stamp** according to ETSI EN 319 142.

- **Augmentation of preservation evidences**

Based on monitoring the suitability of the cryptographic algorithms based on a suitable cryptographic policy, such as ETSI TS 119 312, the preservation service shall perform an augmentation of the signature according to the specific evidence format.

3.2.2. PRESERVATION PROFILE

DigitalSign supports the following preservation profile:

- ProfileIdentifier

  urn:oid:1.3.6.1.4.1.25596.6.2.1;

- Operation

PreservePO;

- Policy

http://uri.etsi.org/19512/policy/preservation-evidence;
http://uri.etsi.org/19512/policy/signature-validation

- ProfileValidityPeriod

ValidFrom= Not applicable.

- PreservationStorageModel

  WithoutStorage;

- PreservationGoal

PDS - extending over long periods of time the validity status of digital signatures;

- EvidenceFormat

Shall be present and indicate the supported evidence formats, whereas the following URIs may appear: CAdES, XAdES e PAdES:

http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3
http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp
http://uri.etsi.org/ades/PAdES/document-time-stamp

- Description

PDS with signature augmentation; Preservation Service Without Storage.

- SchemeIdentifier

http://uri.etsi.org/19512/scheme/pgd+wos+aug

- ExpectedEvidenceDuration

The evidence preservation period is defined by agreement with the client or there is another period determined by a normative act.