APPROVED

PMO GOVERNANCE
DORU VIJIIANU ZIPPER SERVICES SRL Digitally signed by ZIPPER SERVICES SRL Date: 2025.10.14 18:20:08 +03'00'
JUDIT FEKETE FEKETE JUDIT Digitally signed by FEKETE JUDIT Date: 2025.10.14 18:24:43 +03'00'
MIRELA OJOG Mirela Ojog Digitally signed by Mirela Ojog Date: 2025.10.14 20:10:22 +03'00'

-Zipper Services Authority-
Qualified preservation service (QPS)
for qualified electronic signatures/seals (QES)

Policy, Code of Practice and Procedures

THIS DOCUMENT IS THE PROPERTY OF ZIPPER SERVICES S.R.L.
UNAUTHORIZED COPYING IS NOT ALLOWED

History of the edition			
Edition	**Date and description of the change**	**Ready**	**Approved**
1	18.09.2025 – First Edition	Judit Fekete	Mirela Ojog
2	08.10.2025 -Second Edition – minor reviews	Judit Fekete	Mirela Ojog

Annex A. Contents

1. Introduction

The Policy, Code of Practice and Procedures (PCPP) details the policies, practices and procedures that Zipper Services (hereinafter Zipper) applies on Q**ualified preservation service for qualified electronic signatures/seals** (hereinafter **QPS**).

Zipper provides for its users the service for qualified preservation of qualified electronic signatures/seals in compliance with Art. 34 and Art. 40 of Regulation (EU) No. 910/2014 and Regulation (EU) 2024/1183 (eIDAS 2.0) and, it is registered in the trusted list of the European providers of trust services, as well as in the register of the Roumanian trust services providers maintained by Autoritatea pentru Digitalizarea României (ADR).

The content of the **PCPP-QPS** is compliant with the latest versions of the requirements ETSI TS 119 511 and ETSI TS 119 512.

This document is made available to the public at https://pki.ca.ezipper/policies

The technical and security requirements (according to art. 5 of the Technical Norms regarding the accreditation procedure of electronic archive administrators and the approval procedure of electronic archiving systems, integral part of Order 20717/2024) that the electronic archiving system meets are described in the Security Plan specific to the electronic archiving system v1, considered an annex to this document.

Management may make exceptions to this document on a case-by-case basis to mitigate the significant, imminent impact on customers, partners, reliance parties and/or other persons in the absence of practical solutions. Any such handling exceptions are documented, tracked and reported as part of the audit process.

2. Policy and Practice Administration

The electronic archiving service is offered by Zipper Services in the infrastructure of the Zipper Services Data Center, authorized by the ADR for electronic archiving services under the conditions of Law 135/2007 (Decision no. 253 of 23.05.2024).

The organization administering this document:

ZIPPER SERVICES SRL

Str. Rene Jeannel, nr. 8, Imobil Novis Plaza, corp A, et. 2, 400285, Cluj-Napoca, RO

Cluj-Napoca, 400285, Romania

Work point:

1 Decembrie 1918 Blvd. no. 1G,

Sector 3, Bucharest, 032451, Romania

Work point:

Nikola Tesla Street, no. 2, cod 400221, jud. Cluj

Cluj-Napoca, 400285, Romania

https://ezipper.ro/

Email: office@ezipper.ro

Phone +40 21.340.4638 / +40 31.101.1020

Fax: +40 21.340.4636 / +40 31.101.1022

(Monday-Friday 09.00. – 18:00 Eastern European Time)

Contact: pki@ezipper.ro Policy Management Team

3. Approval procedure

The approval of this document and subsequent amendments are made by Zipper's dedicated persons. These individuals make up the policy management team. PMO GOVERNANCE members approves new versions of this document. The amended versions supersede any conflicting provisions of previous versions of this document.

Subscribers who do not accept the new, modified terms and regulations of PCPP shall make a suitable statement within 15 days of the date of the new version of PCPP publication. This will lead to termination of the contract related to the QPS services provided.

4. NAME AND IDENTIFIER OF THE DOCUMENT

The full name of this document is "Qualified preservation service for qualified electronic signatures/seals (QPSES) (Qualified preservation service) Policy, Code of Practice and Procedures (PCPP)" and object identifier (OID):

Name of the document	Object Identifier (OID)
Qualified preservation service (QPS) for qualified electronic signatures/seals (QES) - Policy, Code of Practice and Procedures (PCPP)	**1.3.6.1.4.1.57570.4.3.2** 4=> service classification node 3 => preservation services (subtree for preservation-related policies) 2=> **qualified** preservation variant

According to ETSI EN 319 401 it is mandatory for a TSP to identify the service policies it supports. For preservation services, such identifier is communicated through the documentation provided to the subscribers and relying parties, over specific OID:

- itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2).

Zipper ensures that it does not change the object identifier of this document as well as the object identifiers of policies, practices and other referral documents. If there is an extension/update in policy and practice that will not affect previously issued certificates, Zipper presents a new object identifier that covers the new certificates or extended/updated ones.

5. References

Applicable national legislation:

1. Law no. 135 of 15 May 2007 on the archiving of documents in electronic form
2. ORDER no. 20.717 of May 9, 2024 for the approval of the Technical Norms regarding the procedure for the accreditation of electronic archive administrators and the procedure for the approval of electronic archiving systems and for the repeal of the Order of the Minister of Communications and Information Society no. 493/2009 on the technical and methodological norms for the application of Law no. 135/2007 on the archiving of documents in electronic form
3. MCSI Minister's Order no. 489/15.06.2009 regarding the methodological norms for authorizing data centers
4. Order no. 585 of 9 May 2011 for the completion of the Order of the Minister of Communications and Information Society no. 489/2009 regarding the methodological norms for authorizing data centers
5. Order no. 1167 of 25 November 2011 for the amendment of Annex no. 3 to the Order of the Minister of Communications and Information Society no. 489/2009 on the methodological norms for authorizing data centers.
6. Law no. 455/2001 on the electronic signature, republished, with amendments and completions
7. The National Archives Law no. 16/1996, republished, with subsequent amendments and completions;
8. Law no. 182/2002 on the protection of classified information, with subsequent amendments

and completions;

9. Government Decision no. 89/2020 on the organization and functioning of the Authority for the Digitization of Romania, with subsequent amendments and completions;
10. The technical norms regarding the procedure for the accreditation of the administrators of the electronic archive and the procedure for the approval of the electronic archiving systems, approved by the Order of the Minister of Research, Innovation and Digitalization no. 20.717/2024;

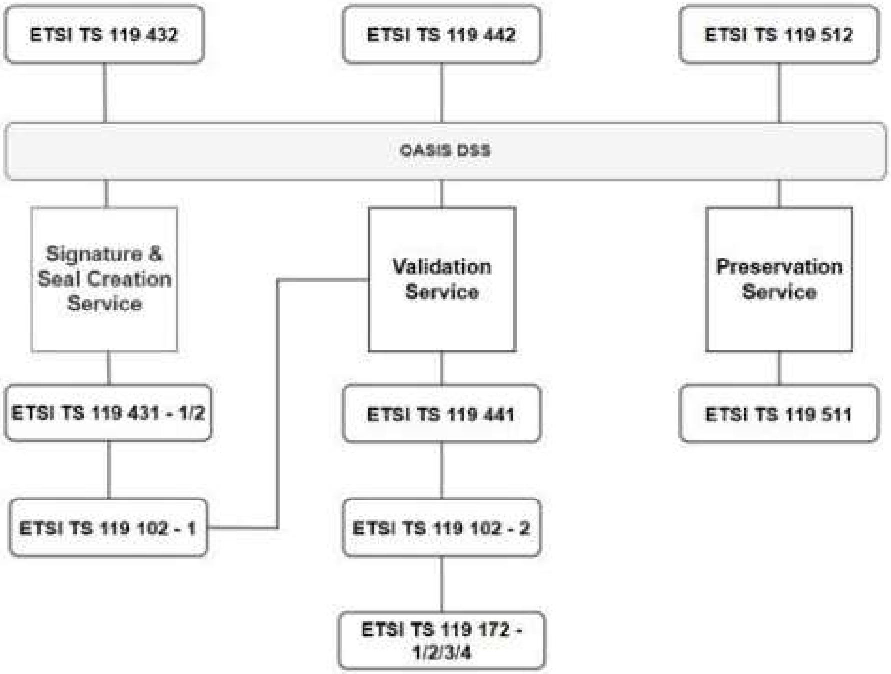
The following references contain provisions that are relevant to the ZIPPER data center policy and the electronic archiving service:

Law no. 190/2018 on measures for the implementation of 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), as amended.

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 [1];

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)

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework



ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services

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 TS 119 132-3 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES

ETSI EN 319 102 On Approval Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;

ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1 : Creation and Validation;

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 TS 119 122-3 Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES;

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 EN 319 162-1 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1 : Building blocks and ASiC Baseline containers;

ETSI EN 319 162-2 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers;

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 EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;

ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;

ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;

ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services;

ISO/IEC 21320-1 Information technology -- Document Container File -- Part 1 : Core;

IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP);

IETF RFC 3986 Uniform Resource Identifier (URI): Generic Syntax;

IETF RFC 4998 Evidence Record Syntax (ERS);

IETF RFC 5280 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

IETF RFC 5816 ESSCertIDv2 Update for RFC 3161;

IETF RFC 6283 Extensible Markup Language Evidence Record Syntax (XMLERS);

IETF RFC 6838 Media Type Specifications and Registration Procedures;

IETF RFC 6960 Online Certificate Status Protocol - OCSP;

W3C Extensible Markup Language (XML) 1.0 (Fifth Edition)", W3C Recommendation;

BSI TR-03125-F Preservation of Evidence of Cryptographically signed Documents, Formats (TR-ESOR-F);

ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;

ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services;

ETSI TS 119 442 Electronic Signatures and Infrastructures (ESI);Protocol profiles for trust service providers providing AdES digital signature validation services.

5. Definitions and abbreviations

IT audit - the activity of collecting and evaluating evidence to determine whether the system IT complies with the performance and work parameters according to the design requirements, if it ensures the functionalities necessary for business requirements and compliance with the legislation in the field, if it is secure, if it maintains the integrity of the processed and stored data, if it allows the achievement of the entity's strategic objectives and the efficient use of information resources;

IT auditor - the authorized natural person who holds an IT auditor certificate or the legal person with certified personnel who carries out an audit activity of information systems, according to regulations and good practices in the field;

IT audit report - the tool through which the purpose of the audit is communicated, the objectives pursued,the norms/standards applied, the period covered, the nature, procedures, findings and conclusions of the audit, as well as any reservations that the IT auditor has regarding the audited information system;

qualified trust service provider - according to art. 3 point 20 of 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;

backup - the activity of copying files or databases in order to preserve and recover them in case of damage or other unforeseen event;

Data container: a data object containing a set of data objects and additional information describing the data objects contained and, optionally, the content and relationships between them (digital signatures/seals, timestamps, evidence records, validation data, etc.);

Qualified EU Timestamping Authority: a qualified trust service provider issuing qualified electronic timestamps as provided for in Regulation (EU) No 910/2014;

evidence recording: data that can be used to prove the existence of an archived data object or a group of archived data objects at a particular point in time;

QPSES (Preservation Service for Electronic Signatures): a qualified preservation service for qualified electronic signatures/seals;

OCSP: a protocol providing online certificate status information (OCSP or CRL);

ASiCArchiveManifest file: container file whose name matches "*ASiCArchiveManifest*.xml" containing one ASiCManifest element instance

ASiCEvidenceRecordManifest file: container file used in ASiC-E to reference a set of files to which an ER applies whose name matches "META-INF/ASiCEvidenceRecordManifest*.xml" and containing one ASiCManifest element instance

ASiCManifest file: file whose name matches "*ASiCManifest*.xml" containing one ASiCManifest element instance

container: file created according to ZIP holding as internal elements files with related manifest, metadata and associated signature(s), under a folder hierarchy. A data object which contains a set of data objects and additional information describing the contained data objects and optionally its content and its interrelationships (digital signatures/seals, time-stamps, evidence records, validation data, etc.);

Delta preservation object container: a preservation object container describing exclusively the difference between an already existing preservation object container and an updated data object; **digital signature techniques:** techniques based on digital signatures/seals, time-stamps or evidence records;

EU qualified time-stamping authority: a qualified trust service provider issuing qualified electronic time-stamps as laid down in Regulation (EU) No. 91 0/2014;

expected evidence duration: expected duration of the evidence records;

export-import package: information extracted from the preservation service, including content and evidence, that can be imported;

long-term: a long time period in which technological changes, such as obsolescence of cryptographic technology, crypto algorithms, key sizes or hash functions, key compromises or the ability to check the validity status of the certificates may be a concern;

long-term preservation: long-term preservation (with storage), where the extension of the validity status of a digital signature and / or the provision of proofs of existence of data over a long period of time does not depend on the obsolescence of cryptographic technology, crypto algorithms, key sizes or hash functions, key compromises or the ability to check the validity status of the certificates;

notification protocol: a protocol used by the preservation service to notify the preservation client;

preservation client: a preservation client being a component or a piece of software which interacts with a preservation service via the preservation protocol;

preservation evidence: evidence of preservation provided by the preservation service which can be used to prove that one or more preservation goals are met for a given object; **preservation evidence policy:** an evidence preservation policy, including a set of rules specifying

the requirements and the internal process of generating and validating any preservation evidence;

preservation evidence retention period: a preservation period of preservation evidence; **preservation goal:** the preservation goal is the extension (augmentation) of the validity status of digital signatures/seals beyond the technological validity status, provision of proofs of existence of data over long periods of time or a combination of both;

preservation mechanism: preservation mechanism based on digital signature techniques, which is used to preserve preservation objects and to maintain the validity of preservation evidence**;** **preservation interface:** the preservation interface is a component implementing the preservation protocol. Evrotrust elaborates and uses an applied programming interface (API) in compliance with the requirements of ETSI TS 119 512;

preservation manifest: description of a data object in a preservation container referring to the preservation data objects or additional information and metadata in the preservation object container;

preservation object (PO): a preservation object, which is submitted to, processed by or retrieved from a data preservation service;

preservation object container (POC): a container for data object preservation, for example, ASiC-S, ASiC-E or Information Packages OAIS;

preservation object identifier: a unique identifier of a preservation object; **preservation period:** a preservation period has the duration in which the preservation service preserves the submitted preservation objects and any evidence associated there to; **preservation profile:** a preservation profile represents a uniquely identified set of implementation details pertinent to the preservation storage model and the preservation goals which specify how preservation evidence is generated and validated;

preservation protocol: communication protocol between the preservation service and the client;

preservation scheme: a preservation scheme represents a set of procedures and rules pertinent to the preservation storage model and the preservation goals;

preservation service: a preservation service capable of extending the validity status of a digital signature over a long period of time and / or providing proofs of existence data over a long period of time;

preservation service provider: a provider rendering a preservation service;
preservation service policy: a policy for a preservation service;

preservation service practice statement: a practice statement for a preservation service;
preservation storage model: a model of storage (temporary, permanent);

preservation submitter: a legal or natural person (submitter, for example, a bank's client) using the preservation service to submit the data object;

preservation subscriber: a legal or natural person (client) bound by agreement with Zipper (for example, a bank, an insurance company, utility company, etc.);

proof of existence: a proof that a certain data object existed as of specific date / time**; proof of qualified time stamp** – qualified electronic time stamp in accordance with Article 3(3) of 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;

submission data object: an original data object provided by the submitter; **time assertion:** a time-stamp token or an evidence record;

submission data object: an original data object provided by the submitter; time assertion: a time-stamp token or an evidence record;

archival nomenclature - a working tool used in the archival field, which is developed by each creator for the organization and management of his own documents, in accordance with the provisions of the National Archives Law no. 16/1996, republished, with subsequent amendments and completions;

Qualified long-term preservation - qualified service for the preservation of qualified electronic signatures according to art. 34 para. (1) of 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;

qualified certificate – qualified certificate for electronic signature according to Article 3(15) of 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;

audit log - a register in which all actions taken on data and/or documents in electronic form or on the system itself are recorded, including information such as the date and time of the action, the user involved, the type of action (creation, modification, deletion, etc.), as well as any other relevant details;

Electronic Document Retention Policy – establishing rules and procedures for long-term archive retention and management, including defining document retention and disposal periods in accordance with the archive administrator's regulations and policies

preservation services with storage (WST) In this case, the data to be preserved is stored by the preservation service while the evidences and the preserved data are delivered upon request by the preservation service to the preservation client. The preservation service stores the submitted data object(s) (SubDO(s)) and the preservation object(s) (PO(s)) and the associated preservation evidences. The PO(s) are derived from the SubDo(s) by augmentation or by building a Preservation Object Container (POC).

preservation services with temporary storage (WTS) The data to be preserved is stored temporary on the long-term preservation service side. The service temporary stores the submitted SubDO and the generated preservation evidence. Preservation evidence is produced synchronously after the SubDO is received. The preservation service keeps traces of its actions to be able to provide records of its activities.

6. Ancronym

AUG Augmentation goal

CA Certification Authority

CARL Certification Authority Revocation List

CRL Certificate Revocation List

DN Distinguished Name

EUMS European Union Member State

OCSP On-line Certificate Status Protocol

QTSP - Qualified trust service provider;

CSA (Certificate Status Authority) - Trust authority for status check (OCSP)

ER - Evidence Record

PCPP - Policy, Code of Practice and Procedures

PO - Preservation Object

PDO - Preservation Data Object

PDS - Preservation of digital signatures

PGD - Preservation of general data

POC - Preservation Object Container

PRP - Preservation Service Protocol

PRS - Preservation service

PSP - Preservation Service Provider

QC - Qualified certificate

QES - Qualified electronic signature or qualified electronic seal

QPS – Qualified Preservation Service

QVS – Qualified Validation Service

SubDO - Submission data object

SigS - Digital signature creation service

TS - Trust Service

TL - Trusted List

TSA - Time-Stamping Authority

TSP - Trust Service Provider

UTC - Coordinated Universal Time

ValS - Validation Service

Zipper Services SRL - Zipper

WST - preservation service with storage

WTS - preservation services with temporary storage

6. APPLICABILITY OF QUALIFIED PRESERVATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES / SEALS

The service is intended for users who need long-term preservation of their electronic documents or long-term preservation of documents signed with electronic signature. Preservation Service aims to support a qualified preservation service for qualified electronic signatures / seals under Regulation (EU) No 910/2014.

This document deals with two main applications:

1) Long-term preservation using electronic signature techniques, the ability to validate an electronic signature, the ability to maintain its validity status, and the ability to obtain evidence of the existence of associated signature data, as well as during the filing preservation service, even if later the signature key is compromised, the validity of the certificate expires or there is cryptographic attack of the signature algorithm or hash algorithm used in the signature;
2) Provide evidence of the existence of digital objects, using electronic signature techniques (electronic signatures, time stamps, records of evidence).

These evidences provide a proof of existence of the digital signature and the validation data (time-stamps, certification paths, revocation information), and also a proof of existence of the signed data in case the signed data is provided together with the signature.

Based on ETSI 119 511 specifications, the validation data will be included in a validation report and the preservation service will use a signature validation service to create a validation report. ETSI EN 319 102-1 defines different validation statuses (TOTAL_VALID, TOTAL_FAILED, INDETERMINATE). In case all the needed validation data cannot be collected and verified by the validation service, the EN 319 102-1, clause 5 and clause 5.1.3 define how the status “TOTAL-FAILED” and INDETERMINATE to be used and what information must be returned: “the validation process shall output additional information to explain the TOTAL-FAILED/INDETERMINATE indication for each of the validation constraints that have been taken into account and for which a negative result occurred.” If the validation result is INDETERMINATE OR TOTAL_FAILED, it means the validation service has concluded that the signature is definitely invalid. The preservation service cannot accept the signature as valid evidence. In these cases:

- The preservation process will fail for that object
- The preservation service will:
  - Record the failure in its preservation evidence record,
  - Generate a validation report that shows the INDETERMINATE or FAILED result,
  - Stop further evidence generation for that signature/document.

7. Service provision process

7.1 General concepts

The primary task of the **Long-Term Preservation Service** is to ensure the continued validity of qualified electronic signatures and qualified electronic seals affixed to electronic documents.

This document refers to a trust service provided by Zipper pursuant to Art. 34 and Art. 40 of Regulation (EU) No. 91 0/2014 and in compliance with the applicable Romanian legislation. The Policy and Practice describes all requirements related to any used procedures and technologies that could enhance the reliability of the qualified electronic signature/seal outside its technological validity period. Zipper applies the requirements, recommendations or authorizations of the European Commission applicable to a service for qualified long-term preservation with storage (preservation service with storage) for combined preservation of digital signatures and with temporary storage (preservation service with temporary storage) for any type of data objects.

In accordance with Articles 34 and 40 of Regulation (EU) *eIDAS 2.0*, the service guarantees that signatures and seals remain **valid and verifiable** over extended periods, despite technological change, cryptographic evolution, or the potential expiry/revocation of certificates.

The relationship between Zipper and the end-user are governed by the General Terms and Conditions of the Contract for Preservation services, or, where applicable, by a contract for provision of the respective service, the General Terms being an inseparable part thereof.

This PCPP defines the requirements and commitments of the preservation service for maintaining the long-term validity and evidentiary value of signed or sealed electronic documents.

The provider (Zipper) may specify and limit:

- the formats of accepted signatures and seals,
- any additional technical or operational parameters.

Sub-groups of preservation covered by present document:

- [WST] preservation service with storage;
- [PDS] preservation of digital signatures;
- [PGD] preservation of general data;
- [PDS+PGD] combined preservation of digital signatures and general data- the preservation service will extend the validity status of submitted digital signatures and at the same time providing a proof of existence for the other submitted data
- [AUG] augmentation of submitted preservation evidence.

7.2 Participants

7.2.1 Subscribers (beneficiary)

Any natural or legal person who has a contract with Zipper for a qualified preservation service for qualified electronic signatures / seals is a QERDS subscriber. The subscriber/beneficiary is the applicant, the natural or legal person who requests the qualified preservation service for qualified electronic signatures / seals and who enters into a contractual relationship with ZIPPER. The subscriber will be held directly liable if his obligations are not fulfilled correctly.

Where practically feasible, the certification service provided and the products used in the QERDS delivery are also accessible to people with disabilities.

7.2.2 Trusting Parties

Trusting parties (third parties) are natural or legal persons who rely on the evidence provided by the provider in relation to the QERDS. In this case, they are not QERDS users.

7.2.3 Other participants

To provide the service under this document, Zipper does not use external qualified certification service providers.

Zipper reserves the right to enter into contracts with external parties for the provision of certain certification services (e.g. qualified electronic certificate issuers), where necessary.

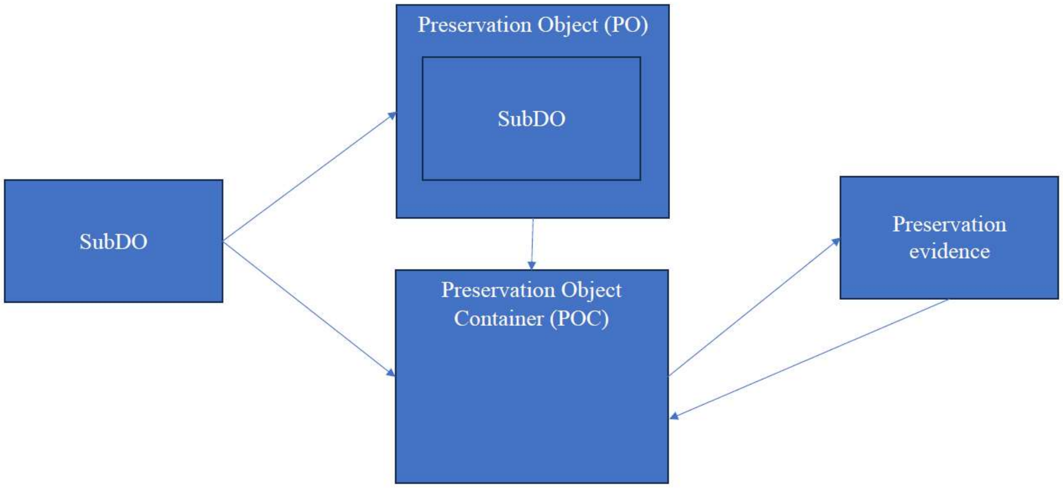
7.3 Preservation period

In the case of a preservation service with storage [WST], the preservation period is the duration during which the preservation service preserves the preservation objects (POs).

The POs may consist of:

- the submitted data objects (SubDO) and POs derived from the submitted data objects by augmentation, or
- by building a POC including the associated evidences.

This preservation period can be defined using a duration period (e.g. in month or years) from the time of the submission, from legally required retention periods, by a criteria, or by a date.



During that period, the preservation service creates and augments preservation evidences as needed to achieve the preservation goal. The way of evidences that are created may change during this period because for example certificates expire or because a cryptographic algorithm is not trustworthy anymore.

The preservation service can use external sources of information to appreciate which cryptographic algorithms, key sizes or hash functions are not likely to be trustworthy anymore, e.g. ETSI TS 119 312 and when necessary issue a new (version of a) preservation profile.

7.4 REQUIREMENTS TO THE QUALIFIED PRESERVATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES/SEALS

The QPSES service provided by Zipper meets all the requirements of ETSI EN 319 401, paragraph 6.1 as *well as the requirements described of the document "Practice of Qualified Certification Services":*

> The preservation profiles that support the preservation service are described in paragraph *"Preservation Profiles"*

> Realization of preservation targets (PDS and PGD) is described in paragraph "FUNCTIONAL MODEL OF A QUALIFIED PRESERVATION SERVICE"

> 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 Zipper when providing a storage service

> The input / output packets, the relevant storage evidence and the additional information required for their validation are accessed by using the service interface or by requesting a specific request for data and / or evidence. They can be provided separately or in an I/O package that is securely protected by encryption. In all cases, they are handed over only to the client or his authorized representative;

> All QPSES provision information is stored for a period of 10 years in accordance with the national legislation. After the end of the period all available data is permanently destroyed, unless otherwise agreed with the Subscriber;

> Zipper ensures authentication of the sender;

> Sending of data objects is secured by evidence stamped with electronic time stamp of Evrotrust 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 Zipper;

7.5 FUNCTIONAL MODEL OF A QUALIFIED PRESERVATION SERVICE

7.5.1 Preservation services with storage [WST]

In this case, the data to be preserved is stored by the preservation service while the evidences and the preserved data are delivered upon request by the preservation service to the preservation client.

The preservation service stores the submitted data object(s) (SubDO(s)) and the preservation object(s) (PO(s)) and the associated preservation evidences.

The PO(s) are derived from the SubDo(s) :

- by augmentation or
- by building a Preservation Object Container (POC).

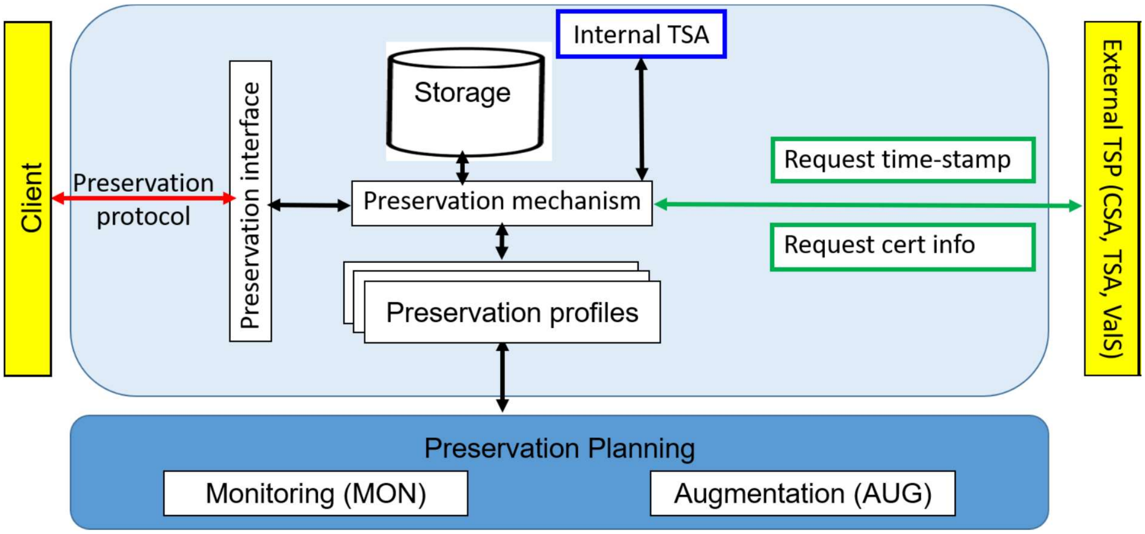


Figure: Long-term preservation service with storage

The submitter (subscriber) provides the system with one or more preservation data objects, and the preservation service sends back a unique identifier of the preservation object. Then, during the preservation period, the submitter may extract upon request one or more preservation evidence and/or preservation objects. The qualified preservation service provides a possibility of deleting any preserved data objects, in concordance with the national law. In case of deletion of preservation evidence, the respective subsystems also delete it but the preservation service preserves the preservation evidence till the end of the preservation period.

7.5.1.1 Practice Statement related to ePreservation (eArchiving) service offered by Zipper

The preservation/archiving flow consists of:

1. Downloading the document and associated metadata from the operational archive to the RepoZip LTa aplication in the agreed way (FTP hot folder, API). Ex. the operational archive application will call, through webservice, the request to upload a document and the associated metadata in the archive.

2. Based on document type, RepoZip make the association to the archival nomenclature of the user company and completing the mandatory metadata (based on Romanian law).

3. The application verify automatically the electronic signature of the document. The signature/seal of the official issuer of the document need to valid and made with a qualified certificate.

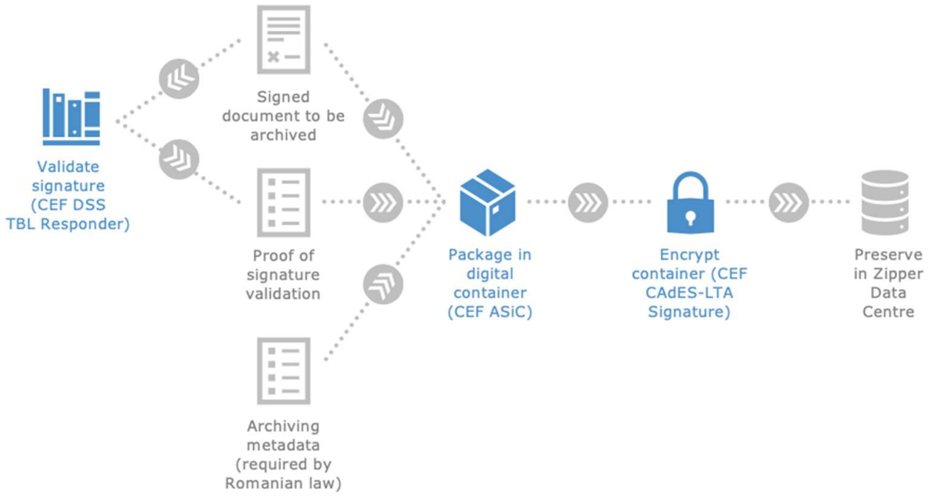
4. Generate a validation report based on ETSI EN 319 102-1, using Zipper `qualified validation service` QVS (checks certificate status, revocation, signature profile, algorithms, etc.). Validation report is signed with a qualified electronic seal (issued for Zipper) and embedded qualified TS.

- QVS returns a Validation Report (VR), digitally signed/sealed by the QVS, asserting the result at that point in time.

5. The validation will result a TOTAL_PASSED, INDETERMINATE OT TOTAL_FAILED status, based on Zipper constrain rules.

6. Only the TOTAL_PASSED and INDETERMINATE (NO-POE) electronic document will be accepted in the archive to be preserve. An ASIC-E container is created and is countersigned/sealed by the archive administrator (Zipper) using a qualified electronic certificate. The signature applied on ASIC will provide Long Term Availability and Integrity of Validation Material (ER).

7. The RepoLTA archiving application will mentain the preservation of the validity status of the digital signature (LTA-level signature) applied on ASIC file. This operation will be done for ASIC files, before the qualified timestamp applied will expire or there are cryptographic security issues.


Validate signature (CEF DSS TBL Responder)
Signed document to be archived
Proof of signature validation
Archiving metadata (required by Romanian law)
Package in digital container (CEF ASiC)
Encrypt container (CEF CAdES-LTA Signature)
Preserve in Zipper Data Centre

In case of a successful IMPORT in the archive:

1. The electronic document will receive a unique ID (IDDoc/POID) for identification within the archive. The automatically created metadata is generated (e.g. archival time, user)

2. The document container `Associated signature container' is created, stored in a ZIP format (extension .asic), according to ETSI TS 102 918 V1.3.1. The container will contain the original pdf received, the received metadata, the validation report, according to ETSI EN 319 102-1

3. It is countersigned with the electronic signature of the administrator of the electronic archive and the qualified time stamp is applied, the CAdES container created will have B-LTA level.

The „electronic file'' attached to each archived document will contain at least the following information:

Received from the Beneficiary:

a) the owner of the document in electronic form.

a) the issuer of the document in electronic form.

b) the holder of the right to dispose of the document.

c) date of issue of the document.

d) type of document in electronic form.

e) the classification level of the document in electronic form.

f) keywords necessary to identify the document in electronic form.

g) the document retention period (can be calculated relative to a metadata/keyword).

h) elements for locating the physical support; - if it's necessary.

Generated automatically in the archiving app (after the moment of electronic archiving):

Generated by Archiver:

i) the unique identifier of the document in electronic form, within the electronic archive.

j) date of archiving (date of entry into the archive).

k) the digital format in which the document is archived in electronic form.

l) the history of the document in electronic form.

m) the size of the archived document

In order to prevent unauthorized user access, access control is carried out through imposed restrictions, through access rules to the documents in the archive. The verification of the integrity of the archived documents is ensured by the fact that they are signed by the holder of the right of disposal and countersigned by the archive administrator. The integrity check is done by the automated agents of the archiving system based on the signature applied to all documents entered in RepoZip.

If a document does not meet the integrity criteria, it is automatically marked and cannot be archived. After correction, it will have to be re-entered into the system and, if it passes the validations successfully, it will be archived.

All operations performed on the electronic archive are logged, the audit records containing the date and time of the event, the type of event, the result (success or failure) of the event.

Access to the RepoZip electronic archiving system is achieved through secure communication lines between the Beneficiary and the Provider (Zipper Services). Access to archived documents is restricted, a user can retrieve an archived document only if he is part of the access group established by the participant to access the document and has the appropriate security level to be able to view the document.

The archiver verification and signature module uses eSignature DSS to first validate the electronic signature of the received document, before the document is approved for archiving.

- Check if the signature is qualified and what type of certificate was used. The beneficiary will be responsible for signing the documents using a qualified certificate provided by a QTSP (qualified trust service provider). If signing is outsourced, it must be done by a QTSP, which offers QTS (qualified trust services) signing. AdES digital certificates are accepted (according to ETSI TR 119 112 V1.1.1 (2019-04) and ETSI EN 391 102-1 [i.6]) of the type:

-> Basic Signature (Ex. CAdES-B, PAdES-B, etc.)

-> Signature with Time (e.g. CAdES-T, PAdES-B-T, etc.)

-> Signatures with Long-Term Validation Material. Ex. CAdES-X, PAdES-B-LT

-> Signatures providing Long Term Availability and Integrity of Validation Material (Ex. CAdES-X-L, PAdES-B-LTA, PADES-E-LTV, etc.)

The verification steps are:

A) the X.509 certificate for the electronic signature applied to the document by the holder of the right of disposition is checked by:

-> hash comparison for document integrity;

-> Public Key Certificates (PKC) used

-> Revocation status information for each Certificate Revocation List (CRL) or Certificate Status (OCSP)

-> `Time assertion' applied to the signature (if any)

- The document to be archived is then packed in a digital container together with proof that the signature has been validated, as well as other metadata detailing the archiving process, according to Romanian law.

- In the next step, the container is encrypted to protect the integrity. Encryption occurs by applying a long-term archiving signature (also called an LTA-level signature) with a qualified timestamp provider.

- The Data Container Creation and Encryption (ASIC) module is also based on the eSignature DSS specifications: the Associated Signature Container (ASiC) base profile for the container and the CMS Advanced Electronic Signature (CAdES) for encryption.

- ASIC: `Associated signature container' according to ETSI TS 102 918 V1.3.1. The container will contain the original pdf received, the verification PDF (point b), the received metadata, signature identification data.

Zipper eArchiving service archive Preservation Object Containers as is described in Zipper eArchiving Policy.

The POC contains:

- Preservation Objects (POs) — the data to be preserved. These could be only signed data
- Evidence, validation and revocation / status data — data needed to validate signatures, time-stamps, certificate revocation / validity paths, and possibly validation reports. These are essential to ensure that in future the validity status (or invalidity) of signatures can be reconstructed.
- Metadata about the POC itself: identifiers (e.g. owner of the document), timestamps, hash values, checksums, etc. This supports integrity, traceability, ability to verify that the container hasn’t been tampered with, and helps reconstruct evidences.

Zipper POC container has the following specifications:

- **Format**: ASiC-E container
- **Contents**: Signed documents + signatures + validation report (signed XML)
- **Signature level**: B-LTA (Baseline with Long-Term validation and Archival timestamps)
- **Signing certificate**: Qualified certificate for electronic seal issued by a QTSP [Provider] from TL, issued to *Zipper Services*
- **Timestamping**: Qualified timestamp (QTS) provided by Zipper QTS (see https://pki.ca.ezipper.ro/repository/certs.php)
- **Validation data included**: Certificates, revocation information (CRLs/OCSP) by a Validation report issued by Zipper QVS.
- **Purpose**: Preservation service ensures the signature and associated objects are verifiable over

the long term, compliant with ETSI TS 119-511 and eIDAS requirements.

Zipper will preserve the POC by extending it over time:

[**Client**] → *Zipper Creates initial POC* (ASiC-E, B-LTA level) → [**Preservation Service** PDS+PGD+WST] -> *Validate via SVS* → *Collect validation data-> Generate Preservation Evidence-> Store extended POC (+ evidence) with* => [**Preservation Service-AUG**] **(A-E, B-LTA level)**

↓

RetrievePO / Audit / Verify

7.6 Preservation Goals

The Long-Term Preservation Service pursues distinct but complementary **goals**, which may be used separately or in combination:

1. **General Data Preservation (PGD)**
    - Provide evidence of the long-term existence of an electronic data object
2. **Digital Signature/Seal Preservation (PDS)**
    - Ensure that electronic signatures and seals remain valid, verifiable, and legally reliable for long periods
    - Maintain proof of existence and the validity status of associated signed or sealed data
    - Keep signatures/seals verifiable and legally reliable even after certificates expire or cryptographic algorithms weaken
3. **Augmentation (AUG)**
    - Perform **periodic re-time-stamping** when algorithms or certificates approach end of life
    - [WST]: During the preservation period, the preservation service shall make sure that the preservation evidence can be used to achieve the corresponding preservation goal

- [WTS]: During the evidence preservation period, the preservation service shall make sure that the preservation evidence can be used to achieve the corresponding preservation goal
- NOTE 1:This can be jeopardized in case a cryptographic algorithm cannot be trusted anymore or revocation information cannot be received anymore
- [WST] [WTS]: The preservation service shall augment the preservation evidences before they cannot be used anymore to achieve the corresponding preservation goal
    - In case of a digital signature, augmentation can be done by incorporating to a digital signature information to maintain the validity of that signature as there are e.g. time stamps, validation data, etc.
    - In case of an evidence record, augmentation can be done by time stamp renewal or hash tree renewal according to IETF RFC 6283
- [AUG] is performed only in combination with PGD or PDS

7.7 EXPORT-IMPORT DATA PACKAGES

Zipper allows users of the preservation services to request export-import packages with stored data, evidence, and all the information needed to validate the evidence. Export-import packages can be used to move stored data from one preservation service to another preservation service. Zipper has used the export-import package format described in ETSI TS 119 512.

The preservation service keep records of all released export-import packages including:

•The date of the event

•The criteria that has been used to select the set of preservation objects to be included in the export-import package.

In case of WST, Zipper export packages with the preservation evidence produced in the described mode are the information included in an archival format of an AdES signature.

In case of archived objects, the export format will be a standardized format (Associated Signature Container Extended (ASiC-E) according to ETSI EN 319 162-1 -clause 4.4).

Export packages are provided only to an authorized legal or natural person.

7.8 PRESERVATION OPERATIONAL PROTOCOLS

The preservation protocol allows the preservation client to interact with the preservation interface. The communication channel between the preservation service user and QPSES is secured, i.e., Zipper ensures the security of user authentication and privacy in accordance with the requirements of ETSI TS 119 512. The protocol used is protected against unauthorized use.

QPSES allows one or more data objects (SubDOs) to be stored under a specific preservation profile by retrieving either a preservation object identifier or a proof of preservation (synchronous mode). The preservation object identifier can later be used to retrieve PO objects and / or to trace or delete POs or to update containers of preservation objects (asynchronous mode) as is defined in ETSI TS 119 512.

The Long-Term Preservation Service allows the retrieval of evidence and / or preservation objects (POs). POs may contain evidence (RetrievePO) as defined in ETSI TS 119 512.

The service allows the deletion of the stored POs. If the evidence is deleted, the SubDO is also deleted. QPSES ensures that stored POs can only be deleted before the end of the preservation period when the deletion request is submitted (along with appropriate justification). Each provided justification is recorded along with information about the request for deletion (DeletePO), as defined in ETSI TS 119 512.

QPSES allows requires a set of object identifiers from data storage, which can be used to retrieve or delete POs.

7.9 PRESERVATION EVIDENCE POLICY

The Evidence Record is a structure that binds hash values of the signed documents or signatures with archive timestamps. Zipper QPSES evidence includes a time-stamp token that conforms to IETF RFC3161 and the updated version RFC 5816. QPSES uses an electronic time stamp that matches the time-stamping protocol used, and the time-stamp token profile, as defined by ETSI EN 319 422.

The **preservation evidence** consists of:

- Archive timestamps - CAdES-(LT)A, XAdES-(LT)A, PAdES-LTA with cryptographic hash indexes (like ats-hash-index-v3 for CAdES)
- **Validation reports** generated when the signature/seal was checked with certificates, CRLs/OCSPs used during validation
    - Zipper QSP, over QVS creates the validation report that is compliant with ETSI EN 319 102-1 as an XML document defined by ETSI TS 119 102-2. The validation report contains the following elements about the validated electronic signature:
        - Signature Validation Report Element, containing the overall signature validation status for the signature as well as additional information on the signature validation performed (clause 4.3).

- Signature Validation Objects Element, that contains the materials collected during the validation procedure, such as CRLs, trust anchors, OCSP responses, etc. and the Proof of Existence at the earliest time of the existence of the object (clause 4.4.)
- Validator Information Element, that identifies the entity validating the signature. (clause 4.5.)
- Validation Report Signature, that contains the validation report signature. (clause 4.6.)

The Qualified Validation Report will be stored associated with the preservation evidence package because and it proves that **at a certain time**, the signature/seal was valid according to eIDAS, contains the full validation context (algorithms, certificate chains, revocation status) and reduces the burden of revalidation in the future — the validation service offered by Zipper QVS timestamp the QVR itself to guarantee its integrity.

Record Evidence

Zipper QPSES implemented a records evidence is in accordance with **IETF RFC 6283 (**MerkleTree**).**

Evidence Record Generation: This record provides cryptographic proof that a set of data objects existed and were unchanged since the timestamp time.

The process to build the Evidence Record involves computing hashes for data objects, building a hash tree and obtaining a timestamp on the root. Also involves repeating renewals/re-timestamping over time as cryptographic strength degrades or certificates expire.

Verification: Given an Evidence Record, the Subscriber can verify that a data object existed at a given time, by tracing through the hash tree, timestamp, and proof chain, checking all cryptographic steps. This proof can be viewed on RepoZip application (MerkleTree proof).

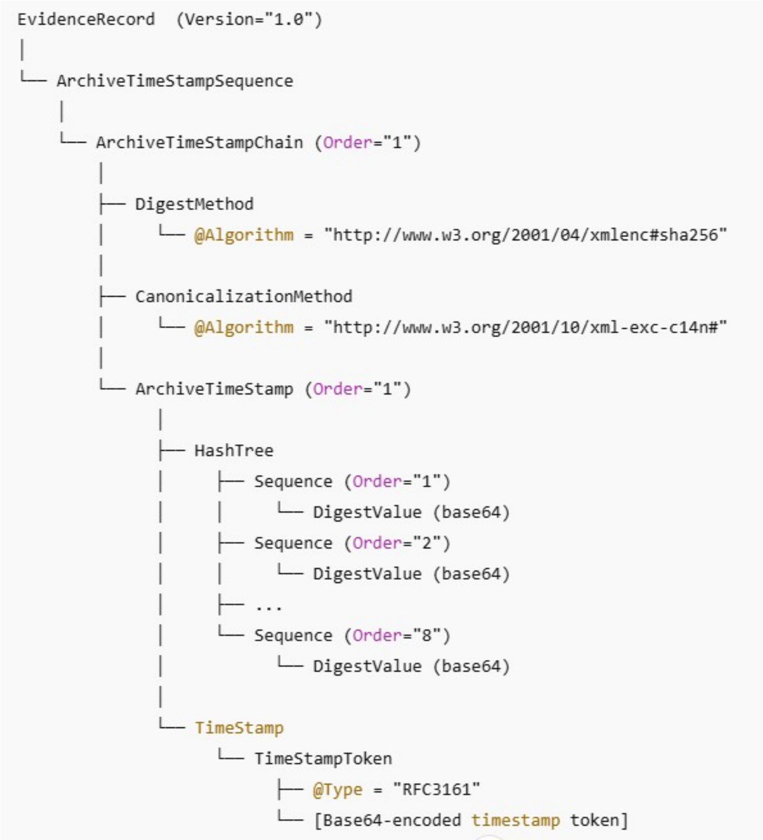
Verification involves:

- Recomputing the hash tree for the original data.
- Verifying the RFC 3161 timestamp using the TSA's certificate chain
- Checking that each renewal step (if any) is valid and consistent with the previous evidence

The format/canonicalization of evidence record is XML (with TimeStamp) :

The **XMLERS** structure hierarchy looks like

(the XML namespace RFC 6283=> urn:ietf:params:xml:ns:ers):



```
EvidenceRecord  (Version="1.0")
|
└── ArchiveTimeStampSequence
    |
    └── ArchiveTimeStampChain (Order="1")
        |
        ├── DigestMethod
        |     └── @Algorithm = "http://www.w3.org/2001/04/xmlenc#sha256"
        |
        ├── CanonicalizationMethod
        |     └── @Algorithm = "http://www.w3.org/2001/10/xml-exc-c14n#"
        |
        └── ArchiveTimeStamp (Order="1")
              |
              ├── HashTree
              |     ├── Sequence (Order="1")
              |     |     └── DigestValue (base64)
              |     ├── Sequence (Order="2")
              |     |     └── DigestValue (base64)
              |     ├── ...
              |     └── Sequence (Order="8")
              |           └── DigestValue (base64)
              |
              └── TimeStamp
                    └── TimeStampToken
                          ├── @Type = "RFC3161"
                          └── [Base64-encoded timestamp token]
```

Storage: The Evidence Record is stored separately from the data object and is correlated to ObjectId (PreservationObjectId).

This policy is listed in the preservation profile, which makes it known to users of QPSES and third parties.

7.9.1 Expected evidence duration applies for a preservation service

Based on ETSI EN 319 401, paragraph 4.4 the expected evidence duration is a duration during which or a date until which, the preservation service expects that a preservation evidence can be used to achieve the preservation goal. This means that the preservation evidence can still be verified and provides cryptographical protection. For several preservation evidence formats, e.g. evidence records or archival AdES signatures, it is sufficient to be able to **successfully validate the latest time-stamp of the whole preservation evidence**.

For preservation evidences generated using digital signature techniques, several durations need to be considered:

1) the private key validity period, i.e. the pre-determined time period during which the private key can be used to generate evidences, unless the associated certificate has been revoked for any reason;

2) the certificate validity period;

3) the duration during which the certificate revocation requests are managed, i.e. a certificate can be revoked;

4) the duration during which the revocation information remains available;

5) the duration during which the hash functions are resistant to collision attacks; and

6) the duration during which the public key is resistant to cryptographic attacks. For public key certificates conformant to IETF RFC 5280, the certificate can only be revoked during the certificate validity period. For public key certificates conformant to IETF RFC 5280, the revocation information is available at least until the end of the validity period of the certificate. However, a CA can provide revocation information also after the expiration of a certificate. EXAMPLE: For qualified certificates, as defined by the Regulation (EU) No 910/2014, the revocation information is provided beyond the validity period of the certificate, see article 24 point 4 of Regulation (EU) No 910/2014.

An evidence generated using time assertions (time-stamps or evidence records) needs to be validated by building a certification path up to a trust anchor.

A preservation evidence can be validated as long as:

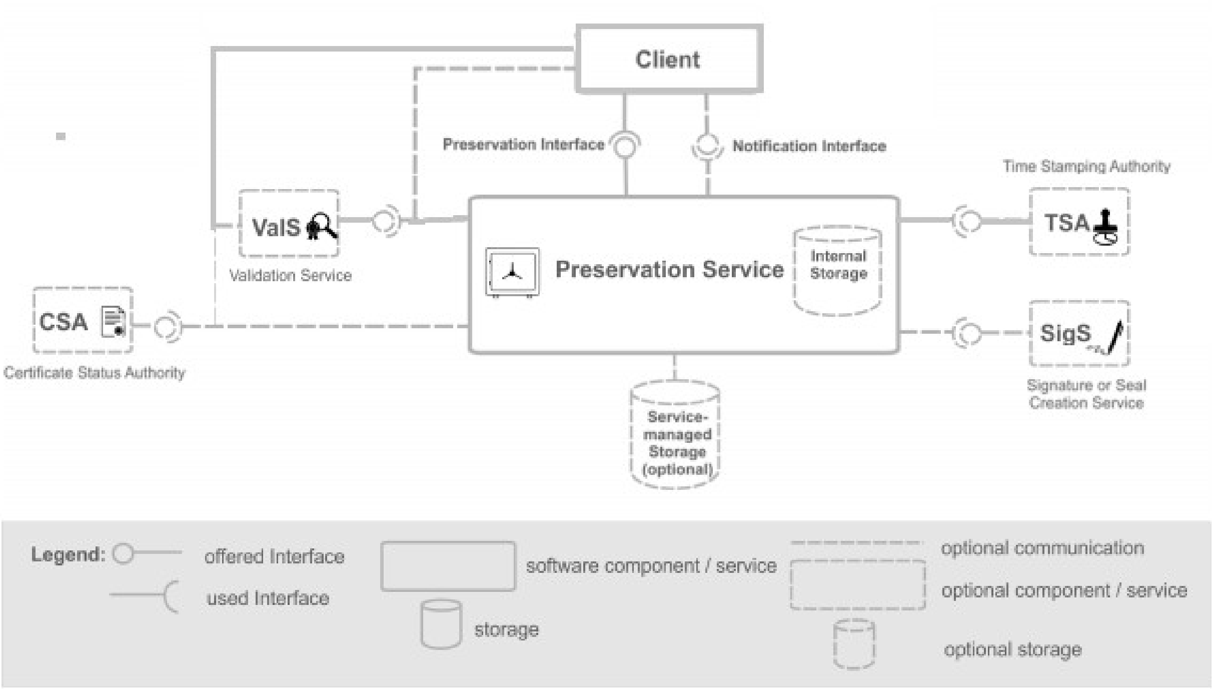
1) none of the certificates from the certification path has been revoked for the reason 'key compromise';

2) no public key present in the validation data is subject to cryptographic attacks; and

3) none of the hash functions used in the validation data is subject to collision attacks.

Point 1) can be verified as long as revocation information is available. If the private key and all backup copies of it are effectively destroyed at the end of the private key validity period, then the only way to compromise the private key will be to perform a successful cryptographic attack on the corresponding public key or on one of the hash functions being used. The expected evidence duration reflects an estimation of a date for the resistance of both the digital signature algorithms and the hash functions used in the validation data for the last preservation evidence. The technological validity period corresponds to a time period during which a signature or evidence can be successful validated and trusted. It depends on until when the certification path can be verified and until when the cryptographic algorithms hashing and signature can be trusted. The technological validity period of signature is similar to the expected evidence duration of preservation evidence based on digital signature techniques.

7.10 SYSTEM ARCHITECTURE



The qualified preservation service defined in the present document provides the preservation interface as specified in clause 5 and use Zipper Time-Stamping Authority (TSA), which issues qualified time-stamps according to ETSI EN 319 422. The service use a qualified Validation Service (QValS) (see ETSI TS 119 441 and ETSI TS 119 442) to collect certification path information and revocation information or directly collect certification path information and gather certificate status information issued by a Certificate Status Authority (CSA).

The qualified preservation service elaborated by Zipper provides interfaces for access to the system resources or external services. The qualified long-term preservation service uses its own storage under the control of Zipper. The service has the goal to preserve general data and ensure evidence of the data object submittal.

The period in which the qualified preservation service preserves the submitted data objects and any preservation evidence related to them by validation and enhancing of the qualified electronic signature reliability beyond the technological validity status or affixing a time stamp, is 10 (ten) years and then they are permanently deleted by the system.

In that period the qualified preservation service generates and extends the preservation evidence necessary for achieving the preservation goal. The method of creating evidence may change in that period in reasons, for example, the certificates expire or because the cryptographic algorithm is not reliable any more.

Zipper keeps itself permanently informed by the ETSI standards (particularly TS 119 312) published on the European Commission's website in order to assess which cryptographic algorithms, key sizes or hash functions are probably not reliable any more, and if necessary, it issues a new preservation profile.

7.11 Preservation Schema

Preservation Schema details the procedural and rule-based framework used for creating and validating preservation evidences and describes the general approaches and methods used to maintain data integrity and access over time.

A Preservation Service in the scope of this document may support multiple Preservation Schemes. The Preservation Scheme defines the general conceptual approach for long-term preservation.

- Each scheme must support at least one Preservation Goal
- Each scheme operates within exactly one Storage Model

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;

Generation and validation of preservation evidences

The present preservation scheme augments the signature corresponding to the signature format, which are announced in the Profile/EvidenceFormat element with the following URIs:

- http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3 according to ETSI EN 319 122-1
- http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp according to ETSI EN 319 132
- http://uri.etsi.org/ades/PAdES/document-time-stamp according to ETSI EN 319 142

Note: ETSI EN 319 122-1 defines id-aa-ets-archiveTimeStampV3(explicitly record which elements are timestamped). In case of CadES signatures, to support long-term archiving, the info will appewar inside

SignerInfo.unsignedAttrs with the digestAlgorithm and ats-hash-index-v3 attribute and the actual timeStampToken (a RFC 3161-compliant TST).

The preservation service verifies that all the validation data needed to validate the signature is available, adds this to the signature and protects it with a time-stamp corresponding to the specific signature format.

The preservation service chooses a hash algorithm to protect the validation data, the signature and the signed data corresponding to the state of the art.

The applied signature level (for PadES, CadES, XadES) will be B-LTA level, wich provides requirements for the incorporation of time-stamp tokens that allow validation of the signature long time after its generation. This level aims to tackle the long term availability and integrity of the validation material. This level is appropriate where the technical validity of signature needs to be preserved for a period of time after signature creation where certificate expiration, revocation and/or algorithm obsolescence is of concern. B-LTA level targets long term availability and integrity of the validation material of digital signatures. The B-LTA level can help to validate the signature beyond many events that limit its validity (for instance, the weakness of used cryptographic algorithms, or expiration of validation data). The use of B-LTA level is considered an appropriate preservation and transmission technique for signed data.

The evidence is included in the signature. The signature format specific standard specifies how to validate the corresponding evidence.

Note: The applied preservation evidence creation policy and a preservation evidence validation policy is announced in the applicable Profile/Policy element with Type equal to the following URI: http://uri.etsi.org/19512/policy/preservation-evidence

7.12 Preservation Profile

A Preservation Profile is the concrete, technical implementation of a Preservation Scheme. Preservation profiles detail the implementation aspects of preservation and specify how preservation evidences are generated, managed, and validated according to the scheme they follow.

The Profile element describes the technical aspects of a Preservation Profile that allow a client to use the Preservation Interface to communicate with the QPresS.

- A preservation profile shall be uniquely identified
- If the preservation target is PDS the Preservation Profile refers to policy-related information that addresses aspects of evidence of creation and validation and signature validation.
- If the preservation target is PGD, the data received from the client will be signed by the

QPresS and then the elements defined in the equivalent preservation profiles defined for the PDS preservation target will be applied.

Preservation Schema/Goal	Focus	Storage Model	Preservation Records
PGD+AUG	Focus is on *existence and integrity*, not on signatures **Evidence record based on Time-Stamps** (e.g., ERS – Evidence Record Syntax, RFC 6283)	WST	**Document Time-Stamp** applied over the data object or a **container evidence record**
PDS+AUG	Ensures not only existence, but also proof of validity at signing time	WST	**PAdES/XAdES/CAdES archival forms with LTV + document time-stamps** (signature validity proof) applied over the entire signed document or archive timestamp chains.

The requirements specified in ETSI EN 319 401, clause 7.5 is applied.

In addition, the following particular requirements apply for the management of the keys used to generate and to validate the evidences:

- The PSP shall insure that the time-stamps used in preservation process come from a TSA that follows state-ofthe-art practices for policy and security requirements for trust service providers issuing time-stamps. In particular the TSA should conform to ETSI EN 319 421 and in the EU context, the preservation profiles may use Qualified TSAs.
- The PSP should only use in preservation process time-stamps that are verifiable using CRLs or OCSP responses which include a 'reason code' in case of the revocation of a public key certificate.
- When PSP signs (part of) a preservation evidence, the PSP should select a signing certificate

issued by a trustworthy CA that implements ETSI EN 319 411-1 or ETSI EN 319 411-2.

- When PSP signs (part of) a preservation evidence, the PSP private signing key shall be held and used within a cryptographic module which is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408, or equivalent national or internationally recognized evaluation criteria for IT security.
- When PSP signs (part of) a preservation evidence, the secure cryptographic device required

Long term validity of ASiC-E

Based on ETSI EN 319 162-1, and ETSI TS 102 918 V1.3.1 long term validity of ASiC-E is achieved for the different container types as follows:

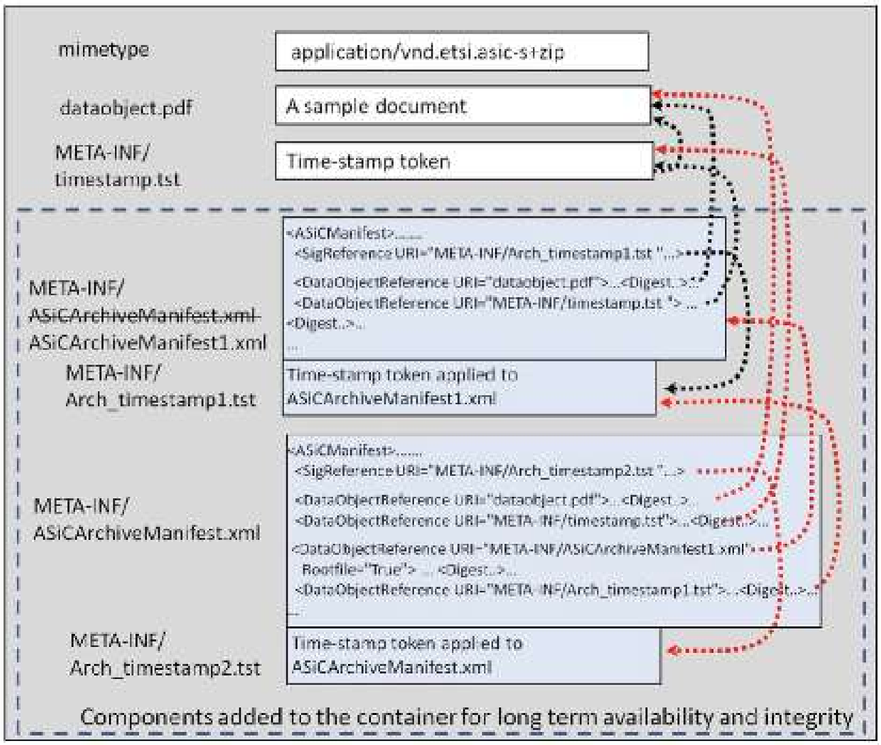
1) For an ASiC-E containers with XAdES signatures, the mechanisms specified in XAdES signatures baseline and extended standards ETSI EN 319 132-1 and ETSI EN 319 132-2 or the evidence record specification IETF RFC 4998 and IETF RFC 6283 will be used for achieving long term validity. This shall apply to all the signatures present in the containers.

2) For ASiC-E containers with CAdES - time assertions either:

a) one or more ASiCArchiveManifest files and related time-stamp token will be added to the container following the rules specified in clause A.7; or

b) one or more ASiCEvidenceRecordManifest files shall apply to all the signed and/or time-asserted data and/or signature and/or time-stamp token files requiring long term validation support.

3) For ASiC-E containers with EvidenceRecord, the internal mechanism of IETF RFC 4998 and IETF RFC 6283 will be used.


mimetype
application/vnd.etsi.asic-s+zip
dataobject.pdf
A sample document
META-INF/
timestamp.tst
Time-stamp token
META-INF/
~~ASiCArchiveManifest.xml~~
ASiCArchiveManifest1.xml
<ASiCManifest>......
<SigReference URI="META-INF/Arch_timestamp1.tst "...>
<DataObjectReference URI="dataobject.pdf">...<Digest..>...
<DataObjectReference URI="META-INF/timestamp.tst "> ...
<Digest..>...
...
META-INF/
Arch_timestamp1.tst
Time-stamp token applied to
ASiCArchiveManifest1.xml
META-INF/
ASiCArchiveManifest.xml
<ASiCManifest>......
<SigReference URI="META-INF/Arch_timestamp2.tst "...>
<DataObjectReference URI="dataobject.pdf">...<Digest..>
<DataObjectReference URI="META-INF/timestamp.tst">...<Digest..>...
<DataObjectReference URI="META-INF/ASiCArchiveManifest1.xml"
Rootfile="True"> ... <Digest..>...
<DataObjectReference URI="META-INF/Arch_timestamp1.tst">...<Digest..>...
...
META-INF/
Arch_timestamp2.tst
Time-stamp token applied to
ASiCArchiveManifest.xml
Components added to the container for long term availability and integrity

7.12.1 Preservation Profile F1 - Preservation scheme with storage based on evidence records

1. F.1.1 SchemeIdentifier

The preservation scheme with storage and evidence records is identified by the following URI:

- http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers

The service profile F1 is published on http://pki.ezipper.ro/PreservationProfileF1
Description:

[PDS] extending over long periods of time the validity status of digital signatures + [PGD] providing proofs of existence of data over long periods of time + [AUG] augmentation of submitted evidences with Storage

2. F.1.2 Preservation goal(s)

The present preservation scheme supports the following three preservation goals:

- 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
- providing proofs of existence of data over long periods of time, which is indicated by the URI:
  - http://uri.etsi.org/19512/goal/pgd
- the augmentation of submitted evidences, which is indicated by the URI:
  - http://uri.etsi.org/19512/goal/aug

3. F.1.3 Preservation storage model

The present preservation scheme supports the preservation storage model "with storage" which corresponds to the value ***WithStorage*** within the PreservationStorageModel element

4. F.1.4 Supported operations

The preservation profile supports the following operations:

- PreservePO according to clause 5.3.3.
- RetrievePO according to clause 5.3.4.
- DeletePO according to clause 5.3.5. (in concordance also with national regulations)

5. F.1.5 Generation and validation of preservation evidences

The present preservation scheme generates preservation evidences in form of evidence records according to IETF RFC 6283, which are announced in the Profile/EvidenceFormat element as:

- **urn:ietf:rfc:6283**

The official XML namespace URI assigned by IANA to identify elements belonging to XMLERS **urn:ietf:params:xml:ns:ers**

For this purpose, the PreservePO function of the present preservation scheme distinguishes two types of SubDO:

- SubDO with one or more digital signatures (SubDOwithDS); and
- SubDO without digital signatures (SubDOwoDS).

For SubDOwithDS, the preservation service will perform a signature validation according to a suitable signature validation policy and collect and store the necessary validation material at a suitable place within a ***validation report embedded within a preservation object container***.

As soon as all SubDO have been prepared accordingly, they are hashed with a suitable hash algorithm, inserted in a Merkle hash-tree as specified in IETF RFC 6283 and protected by an initial archive time-stamp, using Zipper qualified time-stamping authority according to the specified policy.

The validation of the produced evidence records can be performed using a suitable validation policy, which in particular specifies the set of trust anchors and further validation constraints.

The applied preservation evidence creation policy and a recommended preservation evidence validation policy may be announced in the applicable Profile/Policy element with Type equal to the following URI:

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

6. F.1.6 Augmentation of preservation evidences

Based on monitoring the suitability of the cryptographic algorithms based on a suitable cryptographic policy, the preservation service will perform time-stamp-renewals as specified in IETF RFC 4998 and IETF RFC 6283.

7. F.1.7 Requirements for preservation profiles

a. The service supports formats of **preservation evidence**:

- CAdES Archive Time Stamp V3 according to ETSI EN 319 122;

b. No additional output formats are supported

c. Value specifying the time which the profile is deemed active from:

  - ValidFrom=01.12.2025,

d. The evidence preservation period

  - **10 years**, unless the agreement with the client states otherwise or there is another period determined by a normative act (national or EU level).

e. Applicable technical policies:

  - PreservationEvidenceCreationPolicy: urn: oid: 1.3.6.1.4.1.57570.4.3.2
  - ValidationPolicy: urn: oid: 1.3.6.1.4.1.57570.4.2.2.2

7.12.2 Preservation Profile F3 - Preservation scheme with signature augmentation and with storage

The qualified preservation service profile F3.1 complies with scheme F3 described above:

2. F3.1 SchemeIdentifier:

• http://uri.etsi.org/19512/scheme/pds+wst+aug

The service profile F3 is published on http://pki.ezipper.ro/PreservationProfileF3

Description:
[**PDS] extending over long periods of time the validity status of digital signatures +**
+ [AUG] augmentation of submitted evidences with Storage

3. F3.2 Preservation goal (electronically signed data):

The present preservation scheme supports the following preservation goals:

• 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

• the augmentation of submitted evidences, which is indicated by the URI:

- http://uri.etsi.org/19512/goal/aug

4. F3.3 Preservation model (with storage):file

- ***WithStorage***

5. F3.4 List of operations supported by the preservation protocol:

- PreservePO;
- RetrievePO;

- DeletePO (in concordance also with national regulations)

6. **F3.5 The service supports formats for input:**

- http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3 CAdES digital signature according to ETSI EN 319 122;
- http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp XAdES digital signature according to ETSI EN 319 132;
- http://uri.etsi.org/ades/PAdES/document-time-stamp PAdES digital signature according to ETSI EN 319 142;

7. **F3.6 Augmentation of preservation evidences**

Based on monitoring the suitability of the cryptographic algorithms based on a suitable cryptographic policy, the preservation service performs an augmentation of the signature according to the specific evidence format.

8. **General informations**

a. F3.7 The service supports 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.

b. No additional output formats are supported

c. Value specifying the time which the profile is deemed active from:

  - ValidFrom=01.12.2025,

d. The evidence preservation period

  - **10 years**, unless the agreement with the client states otherwise or there is another period determined by a normative act (national or EU level).

e. Applicable technical policies:

  - PreservationEvidenceCreationPolicy: urn: oid: 1.3.6.1.4.1.57570.4.3.2
  - ValidationPolicy: urn: oid: 1.3.6.1.4.1.57570.4.2.2.2

8. PROTECTION OF STORAGE DATA AGAINST THE RISK OF LOSS, THEFT, DAMAGES OR UNAUTHORIZED AMENDMENTS

Data consisting of software, data archives or audit information are safely preserved in a special infrastructure in Zipper Data Center with implemented control of access.

Data centers meet the following conditions:

(a) ensure the security and integrity of the data, at the level of physical security and access through computer means;

b) the availability of the electronic archiving service and the backup of the stored information.

Data availability is ensured by using dedicated storage devices in two different locations in a high-availability configuration, using a clustered backend that provides mirrored copies of all documents and associated metadata.

9. THE AUTHORITY FOR THE ISSUANCE OF QUALIFIED ELECTRONIC TIMESTAMP

Zipper provides a qualified TSS time verification service. Zipper TSA accepts queries for the issuance of qualified electronic time stamps to verify accurate time in the generated evidence.

A detailed description is provided in the document `Time-Stamping Authority (TSA) Policy & Practice Statement`, on https://pki.ca.ezipper.ro/repository/TSAPDS-EN.pdf

10. Certificate Status Authority (QSVP)

Zipper is a qualified signature validation service provider (QSVP), and should perform the validation of the digital signature/seal and the outcome of this procedure is a signature validation report.

A detailed description is provided in the document “Policy and Practice for Qualified Validation Service of Qualified Electronic Signatures/Seals" (Policy and Practice for Signature Validation Service).

11. General rules regarding ZIPPER's technical, organisational and procedural requirements

This section sets out the general rules regarding ZIPPER's technical, organisational and procedural requirements. Zipper Services SRL has a data center, consisting of 2 containers, on a redundant architecture, high performance and availability of services, in a distributed structure.

The following are described the policies and procedures for ensuring the confidentiality of the data, the integrity and the availability of the documents archived in electronic form, throughout the legal period of their retention.

The RepoZip LTA application provides the archiving application for Subscribers, and includes the validation module and the preservation module. Electronic data and electronic documents submitted to the electronic archiving service contain qualified electronic signatures/seals and the service use the preservation and validation procedures and technologies capable of extending their trustworthiness for the preservation period of such data. In order to create preservation evidence where electronic signatures, electronic seals or electronic timestamps are used, qualified trust services will be used.

In the internal RepoZip LTA application located in the data center infrastructure, the following will be ensured:

Confidentiality - ensuring access to documents (associated metadata) through a secure channel, only by authenticating the person, in accordance with the permissions resulting from the group and role setting (based on the Nomenclature in force sent to the Zipper archiver). The solution allows:

- Multi-factor authentication (MFA)
- Granular access control: Permissions are dynamically managed based on the groups and roles defined in the Archival Nomenclature. Access can be restricted at the level of allowed action (e.g. read, download).
- End-to-end encryption: The communication channels between the user and the archive are encrypted with TLS 1.3 protocols, and the archived objects are stored encrypted (AES-256).

Integrity - the prohibition of modification by unauthorized deletion or addition of documents (associated metadata), by making the imprint of the document and signing with the extended electronic signature of the Archivist

- Fingerprint generation (hash): Each document is associated with a unique hash (e.g. SHA-512) calculated before import
- Qualified electronic signature with time stamp included: Applied by the archivist on the archived object at the time of import into the system, the signature guarantees its integrity and subsequent non-alteration
- Audit trail and logging: Any operation on the document is recorded in a log

Availability - ensuring the necessary conditions for easy retrieval and use, whenever needed, in strict compliance with the conditions of confidentiality and integrity of documents (associated metadata):

- Redundancy and replication: The archive is stored in two geographical locations (geo-redundancy) to prevent data loss
- Periodic and automatic backup: Performed daily, with strict restore policies

- Quick Retrieval Interface: Provides search functionality based on associated metadata

Authenticity - ensuring the possibility of verifying the identity of the person/entity, who signed/sealed the document with a qualified certificate, as the holder with the right to dispose of the document. This verification is done through the qualified signature/seal validation service (Zipper Services accreditation):

- eIDAS qualified certificates: Only signatures/seals based on qualified certificates, issued by accredited suppliers, are accepted and the verification report, signature
- Automatic validation: The system integrates validation services (OCSP, CRL) provided by Zipper Services to verify the validity of the signatures and seals of the holders of the right of disposal.
- Marking of the identity of the signatory: Metadata with the data of the signatory and the issuing authority of the certificate is preserved

Non-repudiation - a measure by which it is ensured that after importing into RepoZip LTA that document existed at that time of time. This proof is provided by the procedurally applied measures, the archivist also applying a qualified time stamp to subsequently demonstrate its existence.

- Registered import with qualified timestamp: At the time of import, a timestamp according to the eIDAS Regulation is applied to the archived object, certified by the QTSP supplier Zipper
- Chain of trust: Each archived object is accompanied by a qualified seal of the Archiver and a timestamp embedded in the signature, forming a cryptographic chain that can be verified in court

11.1 THE OWNER OF THE DOCUMENT IN ELECTRONIC FORM

The owner of the document in electronic form is defined at the application level under the name of Client and will define the types of documents, metadata, groups and users belonging to this Client.

The holder of the right to dispose of the document is the owner or, as the case may be, the issuer of the document, who has the right to establish and modify the regime of access to the document, according to the legislation in force.

11.2 DOCUMENT METADATA

Within the application, descriptive preservation information is created for the archived information, respectively keywords necessary to identify the document in electronic form.

Keywords, hereinafter referred to as metadata, will allow user groups to discover and identify the document of interest.

11.3 SOURCE VALIDATION

The application has a process in place to ensure that the accepted document comes from a known and acceptable source.

The archive can demonstrate that it has access to the tools and resources necessary to establish the technical context of the digital objects it contains. The archive records the representation information (including the format) received in the archive. The Archive has mechanisms in place to monitor and notify when representation information (including format) is approaching when it becomes outdated or no longer valid.

11.4 DOCUMENT ACCESS POLICY

The solution has appropriate mechanisms in place to detect data corruption or loss. There is an internal procedure for reporting all incidents of corruption or loss of data and the steps taken to restore or remove corrupted or lost data.

The solution has appropriate mechanisms in place to ensure the integrity of the archived documents. Integrity is defined as the absence of unintentional changes to the content of the archive, the necessary descriptive metadata remaining properly associated, the verification of the number of copies, the synchronization of the copies, the verification of the completeness of the archiving agreements, the validation of the audit traces for all accesses.

The solution has appropriate mechanisms in place to ensure the confidentiality and privacy of the stored information. All stored information will be obtained, stored and processed in accordance with the laws in force, in particular with the Romanian Law on the protection of personal data. There is a statement of Personal Data Protection Policy, which will be annexed to this document.

Access to the data will be consistent with the classification of the data, the group and the user's role. The regime of access to a document in electronic form, the modification and the term of its retention shall be established exclusively by the holder of the right to dispose of the documents.

The rights of each user are set at the customer, group and role level (access level), thus ensuring user access only to the documents and data of the customer to which the group belongs has access.

All users' passwords are kept encrypted in the RepoZip LTA system. A user account that has not been used for a period of time (can be defined for each subscriber, based on contractual security requirements) is deactivated, requiring a reactivation request from the Beneficiary.

The Beneficiary is obliged to take all possible actions in order to protect the identification name and password necessary for the use of the services provided. The Beneficiary is responsible for any event or facts that occurred through the use of its identification name and access password, unless the event or action occurred for reasons that can be attributed to the Archivist.

11.5 POLICY ON CRYPTOGRAPHIC DEVICES USED

The holder of a cryptographic device must perform his duties and obligations responsibly in every possible situation.

The following elements are taken into account when developing the policy on cryptographic controls:

- how management approaches the use of cryptographic controls, including the general principles underlying the protection of business information;

- Key management approach, including methods for recovering encrypted information in case of loss, compromise or destruction of keys;

- roles and responsibilities for:

- implementation of the policy;
- key management;

A cryptographic device holder must notify its issuer in the event of theft, loss, unauthorized disclosure, or security compromise immediately after the incident.

A cryptographic device holder is not responsible for the failure to perform his/her duties/obligations due to reasons that are impossible for him to control.

The cryptographic device holder is responsible for neglecting its obligations to notify the issuer of the disclosure or breach of security as a result of its mistakes, negligence or irresponsibility.

11.6 POLICY ON MEANS OF CONTROL AND SECURITY OF DOCUMENTS AND DATABASE

The RepoZip LTA application ensures the control and security of access to the application by limiting access to:

- internal mesh Zipper
- the Beneficiary's network/IPs

Control and security of access to documents:

-It is secured, by indicating a username and password.

- The regime of access to a document in electronic form, the modification and the term of its retention are established exclusively by the holder of the right to dispose of the documents. The provider is obliged to comply with the regime of access to electronic documents.

-The rights of each user are set at the customer, group and role level (access level), thus ensuring user access only to the documents and data of the customer to which the group belongs has access.

- All users' passwords are kept encrypted in the RepoZip LTA system.

- A user account not used for a period of 1 year is deactivated, requiring a reactivation request from the Beneficiary.

- The Beneficiary is obliged to take all possible actions in order to protect the identification name and password necessary for the use of the services provided. The Beneficiary is responsible for any event or facts that occurred through the use of its identification name and access password, unless the event or action occurred for reasons that can be attributed to the Provider.

11.7 Control and security of access to the database

-At the request of the Beneficiary, there is also the possibility of using a separate virtual server exclusively for the client's application (a clone of the application and a database containing exclusively the client's data are used) for an increased level of security.

- Any access to the Beneficiary's database is recorded in an access file (called a log to automatic processing). Information regarding the addition, modification or deletion of the Beneficiary's business data is saved

11.8 User authentication

Any activity that can lead to actions on sensitive business data (e.g. download)

The log of a Log event will contain the following data: user id, timestamp and Operation type

The log will be available for consultation by users with rights in this regard.

12. Obligations and liability

This chapter includes all obligations, liabilities, warranties and liabilities of ZIPPER LTA, its subscribers and users (subscribers and relied parties). These obligations and responsibilities are governed by agreements accepted by all parties.

ZIPPER assumes responsibility for implementing the requirements of the "LTA Practices" section of this document, as well as the provisions of national law.

ZIPPER's agreements with subscribers and the parties they rely on describe each other's obligations and responsibilities, including financial responsibilities. The ZIPPER Policy and Practice Statement (this document) forms an integral part of these agreements.

12.1 Zipper obligations and warranties towards subscribers

ZIPPER guarantees the availability of 99.5% of the 24/7 electronic archiving infrastructure and application, with the exception of scheduled technical breaks, in terms of equipment and system maintenance.

ZIPPER assumes the following obligations towards Subscribers:

- Operate in accordance with this ZIPPER LTA Policy and Practice Statement (this document) and other relevant operational policies and procedures;
- Ensure that the TSO maintains a minimum UTC time accuracy of ± 1 second;
- Maintaining a competent and experienced team that can ensure the continuity of the Infrastructure Services;
- Permanently ensuring the physical and logical security, as well as the integrity of the servers, software and databases necessary for the proper functioning of the electronic archiving services
- Monitors the entire LTA infrastructure to prevent or limit any disruption or unavailability of services
- Undergoes internal and external reviews/audits to ensure compliance with relevant legislation and ZIPPER's internal policies and procedures;
- Provides high-availability access to ZIPPER LTA systems, except for planned technical outages and loss of time synchronization.

12.2 Subscribers' rights

The beneficiary subscribers have the following rights:

a) establishing the regime of access to the archived document, as well as its modification, under the conditions of art. 14 of Law no. 135/2007;

b) the attestation of the original or copy value of the archived document;

c) online access to the electronic register of the electronic archive;

d) online access to the electronic file attached to each document entered into the electronic archive, according to the established access regime;

e) Online access to archived documents that do not have public access and to their electronic files is considered ensured when the persons who have the right of access to documents and to

Their electronic files can be consulted through a private network (which is not connected to the Internet). The written consent of the beneficiary regarding the use of that network is required.

Subscribers should verify the data package POC archived by ZIPPER LTA.

This check includes:

- Check that the data package contains the original archived document, the electronic record of the document and the signature validation report, countersigned by the archivist
- Verification of the archivist's certificate:
    - Verification of the trust path up to the trusted root certificate and for each of the certificates in the chain (including the certificate with which it is signed)
    - Verify that the certificate is not expired at the time of signing
    - Check that the certificate has not been revoked at the time of signing

Other obligations of the Subscriber may also be defined in the ZIPPER Terms and Conditions for Electronic Archiving Services.

12.3 Zipper's liability

The liability of ZIPPER acting as administrator of the archive for its subscribers is specified in the agreement between the parties or is that provided for in applicable law.

ZIPPER is liable for any damages caused directly, intentionally or negligently, to any person or entity, as a result of the failure to comply with the obligations set forth herein.

ZIPPER's terms and conditions for electronic archiving services limit ZIPPER's liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include a liability ceiling on ZIPPER's combined aggregate liability to any and all persons in respect of electronic archiving services, which is limited to an amount not exceeding that of that contract for the timestamping service and a total maximum of €300,000, regardless of the nature and type of liability, the value or extent of any damage suffered.

ZIPPER LTA is in no way responsible for the fraudulent use of the service.

13. Statement of good practice

13.1 Infrastructure management and operation

13.1.1 Security Management

ZIPPER ensures that appropriate administrative and management procedures are in place that correspond to recognised best practices.

ZIPPER performs all EE functions using reliable systems that meet the requirements of ZIPPER ISMS.

13.1.2 Asset classification and management

ZIPPER maintains an inventory of all assets and assigns a classification of protection requirements to those assets in accordance with risk analysis.

13.1.3 Staff security

ZIPPER maintains adequate personnel controls that meet the best security practices and requirements of the relevant standards.

Management and operational staff have the appropriate skills and knowledge on timestamping, digital signatures and trust services, as well as security procedures for staff with security responsibilities, information security and risk assessment.

ZIPPER implements the Trust Roles Policy for all those employees who have access to or control cryptographic operations. Trusted people and roles include, but are not limited to:

- Crypto Business Operations Staff,
- Security personnel,
- system administration staff;
- Designated engineering personnel and
- Directors who are assigned to manage the credibility of the infrastructure.

Prior to entering a trust role, ZIPPER conducts background checks which may include, as a guideline, the following:

- Identity verification
- Verification of previous employment and professional reference;
- Confirmation of the highest or most relevant educational degree obtained;
- Verification that there is no criminal conviction;
- Verification of financial records.

ZIPPER requires that personnel wishing to become trusted persons provide evidence of the training, qualifications and experience necessary to competently perform their future job responsibilities as specified in the employment contract and job description, before performing any operational or security functions.

Employment contracts signed by employees include confidentiality provisions for information brought to their attention during their performance.

ZIPPER ensures that staff have achieved trust status and that departmental approval has been granted before these staff have been:

- Issued access devices and granted access to the necessary facilities;
- Issued electronic credentials to access and perform specific functions on ZIPPER LTA or other IT systems.

User accounts are created for personnel with specific roles that require access to the system in question. All users must log in with a dedicated account, and administrative commands are only available with explicit permission. File system permissions and other features available in the operating system security model are used to prevent any further use. User accounts are locked out as soon as possible when the role change dictates.

13.1.4 Physical and environmental security

ZIPPER implements the Physical Security Policy, which supports the security requirements of this LTA policy and practice statement.

ZIPPER LTA operations are conducted in a physically protected environment that discourages, prevents, and detects the unauthorized use, access to, or disclosure of sensitive information and systems.

ZIPPER also maintains disaster recovery facilities for its electronic archiving service operations. ZIPPER's disaster recovery facilities are protected by several levels of physical security comparable to those of the primary ZIPPER installation.

The physical security system includes layers for key management security, which serves to protect the online and offline storage of the cryptographic signing unit (OSC) and keying materials.

The areas used for the creation and storage of cryptographic materials require access control. Access to CSOs and key materials is restricted in accordance with segregation of duties requirements. The opening and closing of cabinets or containers on these levels is recorded for audit purposes.

ZIPPER's operations are protected through physical access controls, making them accessible only to duly authorized individuals. Access to secure areas of buildings requires the use of an 'access' card and/or biometrics. The use of the access card is recorded by the building's security system.

Access card logs are reviewed regularly.

Secure zipper facilities are equipped with primary and backup:

- Power supply systems to ensure continuous and uninterrupted access to electricity and
- Heating/ventilation/air conditioning systems for controlling temperature and relative humidity.

ZIPPER has taken reasonable precautions to minimize the impact of water exposure to its facilities, as well as to prevent and extinguish fires or other harmful exposures to flame or smoke.

All media containing production and data software, audit, archive or backup information is stored in zipper facilities or secure off-site storage facilities with appropriate physical and logical access controls designed to limit access by authorized personnel and protect these media from accidental damage.

ZIPPER securely stores all removable media and paper containing sensitive information related to its operations in secure containers. Sensitive documents and materials are shredded before disposal. The media used to collect or transmit sensitive information becomes unreadable before disposal. Cryptographic devices are physically destroyed before removal.

13.1.5 Operations management

ZIPPER LTA ensures that procedures, processes and infrastructure must comply with operational management, security procedural requirements, system access management, reliable system deployment and maintenance, business continuity management and incident management as defined in ETSI EN 319 421.

The operations management procedures for the ZIPPER LTA are incorporated into the general procedures for managing ZIPPER's internal operations.

13.1.6 Compromise of Zipper trusted services

Zipper has developed procedures to manage the continuity of its operations. In case of service interruptions, it strives to minimize these interruptions so as not to affect the activity of the client/client. Zipper has created and maintains a disaster continuity plan. In the event of a disaster, including the compromise of a private signing key, operations are resumed within the deadline set out in the continuity plan. The causes of the disaster are taken into account and reasonable measures are determined to eliminate the cause of the interruption of the process, as well as measures to prevent such disasters in the future.

The company has created, documented, implemented and maintained plans, procedures and control mechanisms in accordance with the international standard ISO 22301 to ensure the necessary level of business continuity and continuity of information security in adverse cases.

Zipper provides:

a) an appropriate management structure available to prepare, mitigate and respond to a destructive event, using staff with the necessary authorities, experience and competence;

b) developing and approving response and recovery plans and procedures that describe in detail how the company will handle a destructive event and maintain continuity of information security;

c) information security control mechanisms within procedures and systems and tools to maintain disaster continuity and recovery;

d) compensatory mechanisms for controlling information security control mechanisms that cannot be maintained in an adverse event.

The continuity plan includes the backup of critical systems. The backup is stored in the two locations, which are 300 km away geographically. The special conditions comply with the applicable standards, recommendations and regulations in the field of information security. The Company verifies any mechanisms created to control the continuity of information security at regular intervals, so that it can ensure their effect and effectiveness in unfavorable cases. Zipper regularly backs up important information and software and guarantees that all basic information and software can be recovered after a disaster or in the event of loss of archive. The recovery mechanisms are checked regularly, so that it can be guaranteed that they meet the requirements of the work continuity plan.

Storage for business recovery in the event of an incident or disaster is maintained and stored in safe and secure locations. Zipper has the obligation to inform subscribers and any third parties about incidents occurring in the service provision activity.

13.1.7 Termination of the trusted service

The Trusted Service ends:

- with a decision of the Board of Directors of ZIPPER;
- by a decision of the authority exercising the supervision of trusted services;
- with a court decision;
- upon the liquidation or cessation of ZIPPER operations.

ZIPPER ensures that potential disruption to subscribers and parties is minimised as a result of the termination of ZIPPER's services and, in particular, ensures that the information necessary to verify the correctness of the services is continuously maintained.

If it is necessary for ZIPPER to cease operation, ZIPPER shall use commercially reasonable efforts to notify Subscribers and reliant parties of such termination prior to termination of the Service.

13.2 Preservation of evidence of the service

- ✓ The retention period of the collected samples is in accordance with national legislation and is in accordance with the recommendations of ETSI TS 119 312;
- ✓ The confidentiality and integrity of current and archived records of the operation of the Service are maintained and archived in accordance with Zipper's business practice;
- ✓ The time used to record events, as required in the log log, is synchronized with UTC at least once a day;
- ✓ Events are recorded in a way that cannot be easily deleted or destroyed;
- ✓ The same preservation profile applies throughout the sample preservation period;
- ✓ The validity period of the samples is extended by using secure and reliable cryptographic algorithms;
- ✓ The evidence format in this policy complies with the requirements of IETF RFC 6283, as well as CAdES ETSI EN 319 122, XAdES ETSI EN 319 132, and PAdES ETSI EN 319 142.

If necessary, Zipper extends the validity of the evidence to the archive. During the archiving period, the archiving service checks whether the evidence can be used to achieve the appropriate preservation purpose. This can be threatened if the cryptographic algorithm can no longer be trusted or the archive administrator's certificate is revoked. In such cases, Zipper expands the evidence before it can be used to achieve the purpose of archiving.

13.3 Organizational reliability

ZIPPER LTA ensures that its organization is reliable in accordance with ETSI EN 319 421. ZIPPER has the financial stability and resources to operate in accordance with this Policy and Practice Statement.