ZIPPER

APPROVED

PMO GOVERNANCE
DORU VIJIIANU ZIPPER SERVICES SRL Digitally signed by ZIPPER SERVICES SRL Date: 2025.10.14 18:06:46 +03'00'
JUDIT FEKETE FEKETE JUDIT Digitally signed by FEKETE JUDIT Date: 2025.10.14 18:21:01 +03'00'
MIRELA OJOG Mirela Ojog Digitally signed by Mirela Ojog Date: 2025.10.14 16:01:42 +03'00'

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

Disclosure Statement

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

Annex A. Contents

1. Introduction

Zipper Services (hereafter 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).

This document is the **Disclosure Statement** of the Qualified Trust Service Provider (QTSP) Zipper concerning the qualified preservation of qualified electronic signatures/seals. The Disclosure Statement is based on the structure defined in Annex A of the document ETSI TS 319-411-1, and is for informative purposes to the users of the SERVICE. This document does not substitute or replace the Policy, Code of Practice and Procedures (PCPP) for the SERVICE, according to which qualified long-term preservation of qualified electronic signatures and seals is provide.

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

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. Document Administration

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. Management 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 of Disclosure Statement 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

Zipper QPS service is applicable only for electronic documents, based on certificate profiles for electronic signatures under eIDAS (Regulation (EU) No 910/2014).

0.4.0.19511.1.2 is an ETSI Object Identifier (OID) that refers to a Qualified Certificate (QC) under the EU eIDAS Regulation, defined in ETSI EN 319 412-1.

5. Acronyms

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. Classes and levels of signatures/seals

THE COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 has defined the technical specifications and standards referring to the classes and levels of qualified and advanced e- signatures/e-seals, which each Member State of the Union should support and which are accepted by the public authorities of the Member States in view of their cross-border interoperability and the required level of security for specific business purposes:

Type	Current Standard	Latest Version	Title
XAdES Baseline Profile	**ETSI EN 319 132-1**	**V1.3.1 (2024-07)**	*Electronic Signatures and Infrastructures (ESI); XAdES digital*

Type	Current Standard	Latest Version	Title
			signatures; Part 1: Building blocks and baseline signatures
CAdES Baseline Profile	**ETSI EN 319 122-1**	**V1.3.1 (2023-06)**	*Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and baseline signatures*
PAdES Baseline Profile	**ETSI EN 319 142-1**	**V1.2.1 (2024-01)**	*Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and baseline signatures*
ASiC Baseline Profile	**ETSI EN 319 162-1**	**V1.2.1 (2024-04)**	*Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and baseline containers*

The DECISION (art. 1 and 3), in accordance with the Regulation 910/2014, approves the following advanced signatures/seals in CMS, XML, and PDF formats at B, T and LT levels of compliance, that should be recognized among Member States.

The DECISION (Articles 2 and 4) approves the conditions under which the validity of an advanced electronic signature/seal is confirmed:

(1) the certificate that supports the advanced electronic signature was valid at the time of signing, and when the advanced electronic signature is supported by a qualified certificate, the qualified certificate that supports the advanced electronic signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I of Regulation (EU) No 910/2014 and that it was issued by a qualified trust service provider;

(2) the signature validation data corresponds to the data provided to the relying party;

(3) the unique set of data representing the signatory is correctly provided to the relying party;

(4) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(5) when the advanced electronic signature is created by a qualified electronic signature creation device, the use of any such device is clearly indicated to the relying party;

(6) the integrity of the signed data has not been compromised;

(7) the requirements provided for in Article 36 of Regulation (EU) No 910/2014 were met at

the time of signing;

(8) the system used for validating the advanced electronic signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues.

Zipper is a QTSP for validation of electronic signatures/seals and generates 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.

7. Model, mechanism and scheme

7.1 Model

This version of the SERVICE is implemented and provided with an associated own Storage/Archive and follows the WST Model (preservation service with storage) according to the ETSI TS 119 511 specifications.

7.2 Mechanism

The Qualified/Advanced signature/seal with extended class (AdES) and LTA level provides an internal mechanism through which it remains verifiable over a long period. The signature/seal AdES class, B-LTA level is best suited for a long-term preservation container.

The current version of the SERVICE uses preservation container for signed/sealed data object with AdES class and LTA level of signature/seal.

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.

7.3 Scheme

The long-term preservation scheme is determined by the long-term preservation and the evidence record that is applied to achieve a specific purpose or set purposes of electronic document preservation. The current version of the SERVICE provided by the QTSP Zipper implements long-term preservation:

- Preservation Profile F1 - Preservation scheme with storage based on evidence records
- Preservation Profile F3 - Preservation scheme with signature augmentation and with storage

7.4 Validation

Validation within the scope of the SERVICE is a process to check the validity of digital signatures of e-documents and of time stamps before preservation.

The SERVICE shall use an internal validation process or an external qualified validation service to check the validity status of a signature/seal before storing an e-document through the storage container.

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. Zipper QPSES implemented a records evidence is in accordance with IETF RFC 4998. This policy is listed in the preservation profile, which makes it known to users of QPSES and third parties.

7.5 Archive/Storage

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:

- ensure the security and integrity of the data, at the level of physical security and access through computer means;
- the availability of the electronic archiving service and the backup of the stored information.

Preserved 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.

7.6 Long-term preservation purposes

The SERVICE supports the following goals for long-term preservation:

- Proof of integrity of an e-document (signature/seal);
- Proof of existence (at a time/in the past) of an e-document (signature/seal);
- Preservation of signed/sealed e-document and maintenance of the validity status of signatures/seals (e-documents) over long periods of time;
- Maintenance of the evidence of validity (status) of e-signatures/seals (e-documents) over long periods of time.

7.7 Evidence regarding the long-term preservation purposes

The SERVICE supports and provides the following evidence regarding the long-term preservation purposes:

- Evidence of integrity of an e-document (signature/seal);
- Evidence of existence (at a time/in the past) of an e-document (signature/seal);
- Evidence of the validity status of signatures/seals (e-documents).

This evidence is based on the implemented long-term preservation scheme, through which evidence material is collected, enhanced and stored together with initially signed/sealed e-documents/files in the Archive of the SERVICE.

7.8 Policy and Practice Statement Administration

The Policy and the Practice Statement of the Provider are subject to administrative management and the approval and subsequent amendments are made by Zipper's dedicated persons. These individuals make up the policy management team.

Changes, modifications and additions are admissible, which do not affect the rights and obligations arising from this document and the standard service agreement between the Provider and Users/Relying parties. The Policy and Practice Statement shall be reviewed at least annually in order to reflect potential requirements and prerequisites for changes in security levels of algorithms, formats and profiles of signatures/seals. Each submitted and approved new version of this document shall be immediately published on the website of the Provider.

The Provider’s Policy and Practice Statement for the SERVICE should be used together with the following documents for qualified services of:

- Zipper QVS for electronic signatures/seals
- Zipper QTSA.

8. Long-Term Preservation SERVICE

The main task of the SERVICE is long-term preservation of the validity of the electronic signature or seal on the electronic document. In this respect and in accordance with the Policy, the SERVICE does not accept preservation of data objects (documents) without signature/seal.

Basic Procedures

8.1 Upload/Preserve

- Upload of electronic document: The SERVICE uploads the document, which have to be archived, only after identification of the Subscriber/Submitter within a secure session/procedure. The secure session ensures the integrity and confidentiality of the uploaded document.
- The Policy and the Practice Statement inform the Subscriber/Submitter about the type of signature/seal on document accepted by the SERVICE, how the electronic signatures and seals are validated and which are the conditions for uploading documents.
- The validity of electronic signature(s) or seal(s) of the document received by the SERVICE is validated through the complete long-term validation material via the qualified validation service Zipper QSVS. The validation may be based on a partial or the complete long-term validation material, attached to an electronic signature or seal. Any information still necessary for the validation and for a long-term evidence material is collected from internal or external sources, and is kept with the document. Zipper QSVS generates 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.
- The validation will result a TOTAL_PASSED, INDETERMINATE OT TOTAL_FAILED status, based on Zipper constrain rules. 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
- 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.

- The SERVICE stores the uploaded preserved container encrypted, on Zipper Data Center Object Storage.
- If the process of compiling the evidence material fails, the Provider (the SERVICE) notifies the Subscriber via error message. Based on the error message, the document and the reason for rejection should be clearly established. If the verification for acceptance of the e-document is not confirmed to the Subscriber within the specified term, it is assumed that the Provider (the SERVICE) has not accepted the electronic document.
- The Provider is responsible for storing the POC and ensuring long-term validity container only after sending a positive confirmation for acceptance of the e-document for preservation.

8.2 Download

The Provider, via the SERVICE, ensures that the Subscriber can download his documents stored in the Archive and the respective materials for long-term validation (evidence material) during the period of the Service Agreement.

1. The Subscriber has access to e-documents and to long-term validation materials (evidence), only through a secure channel

2. The SERVICE ensures that each Subscriber has access only to e-documents and long¬term validation materials, which he is actually authorized to access.

8.3 Display of a preserved document

The SERVICE provides the Subscriber the opportunity to view their containers/documents preserved in the RepoZip LTA application. Subscriber has access only to documents and long¬term validation materials, which he is actually authorized to access.

8.4 Deletion of a preserved e-document

The SERVICE provides at the request of the Subscriber selective deletion of documents and all corresponding long-term validation materials (evidence) preserved in the RepoZip Archive. Deletion means physical erasure of a preserved e-document in a way it cannot be restored later (or only with unreasonably high financial costs). The deletion is performed on the entire system of the Provider by deleting any saved copy of the e-document.

9. Termination of the Service Agreement

Upon termination of the Agreement for the SERVICE, the Provider shall provide the documents and long-term validation materials, which the Subscriber has ordered to be preserved, to be downloaded by the Subscriber or by another authorized person. After termination the Provider shall delete the documents and the long-term validation material of the Subscriber. 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.

10. Applicability

See Section 6 and section 7 of this document.

11. Rights and Obligations of Users and Relying Parties

12. User Responsibility

The responsibility of the User when using the SERVICE is set by the Service Agreement and the Policy and Practice Statement of the Provider.

13. User Obligations

The obligation of the User is to act in accordance with the contractual terms and the Policy and Practice Statement of the Provider while using the SERVICE.

The obligations of the User are determined by the terms and procedures of the Practice Statement for this qualified SERVICE, the service agreement and its standard conditions that are an integral part of the common Policy of the Provider.

14. User Rights

Users have the right to use the SERVICE in accordance with the Policy and Practice Statement of the Provider for the Qualified Long-Term Preservation Service.

15. Relying Party Responsibility

The Relying Parties decide based on their discretion and/or their policies about the way of accepting and using the preserved signatures and seals. During the verification of the validity for keeping the security level guaranteed by the SERVICE it is necessary for the Relying Party to act with caution, so it is recommended to:

- Assess the conformity with the Policy and Practice Statement of the Provider for the SERVICE;
- use reliable IT environment and applications;

- verify the current CRL or OCSP response;

- take into consideration every restriction in relation to the usage of the signature seal that is included in the Policy and Practice Statement for the SERVICE.

16. Limited Warranty and Disclaimer/Limitation of Liability in providing the SERVICE

Zipper as a QTSP declares and guarantees the following:

- the requirements and the operational procedures of the SERVICE are in compliance with the respective Provider's Policy and Practice Statement;
- only the specified formats/profiles of signatures/seals are preserved;
- the evidence validation material issued by the SERVICE correspond to the status of the signature/seal at the time of validation and not at the time of applying/use for a particular business purpose
- compliance with the requirements for confidentiality of information in a signed/sealed document/file;
- 24x7 service availability;

Zipper shall not take responsibility for:

- SERVICE unavailability due to natural disasters, war, telecommunications/energy disturbance, etc.;
- Illegal applicability of technically validated by the SERVICE signatures/seals for specific business purposes (applications) Illegal applicability of technically validated by the SERVICE signatures/seals for specific business purposes (applications).

17. Applicable Agreements, CPS, CP

The document Qualified preservation service (QPS) for qualified electronic signatures/seals (QES) Policy, Code of Practice and Procedures can be found in the ZIPPER repository of documents at https://pki.ca.ezipper.ro/repository/policies.php

Accordingly, Trusted Services Subscriber Agreement, Terms and Conditions concerning Holders/Relying parties of the SERVICE can be found on the above web address.

18. Privacy Policy/Statement

Commitment to respecting confidentiality explains all aspects regarding the processing of personal data and ensures compliance with all the principles related to processing established by the legislation in force, especially by the Regulation (EU) 679/2016 (GDPR), activities carried out by the company in the capacity of Authorized Person of the Operator (for the period execution of contracts with its clients.

ZIPPER processes personal data in accordance to the applicable data protection legislation in force.

For further details, please refer to ZIPPER Privacy Statement

https://pki.ca.ezipper.ro/repository/compliance.php

All information that has become known while providing services and that is not intended for disclosure is confidential. The Subscriber has the right to obtain information from ZIPPER about the processing of their personal data pursuant to applicable law.

ZIPPER has the right to disclose information about the Subscriber to a third party who pursuant to relevant law or a court decision, is entitled to receive such information. 10.5 ZIPPER may publish non-personalized statistical data about its services.

19. Refund Policy

ZIPPER strives to provide the highest level of quality of the trusted services it offers and provides. ZIPPER makes efforts to secure the highest level of quality of its services. However, Subscriber has the right to withdraw from the purchase contract for any reason in case the purchase of the Validation Service is effected via the internet or a telephone the Subscriber.

The exercise of this right shall be made in writing by the Subscriber to ZIPPER, by sending an email to suport.pki@ezipper.ro within 14 days from the date of purchase.

Subject to previous section, ZIPPER may handle refunds on a case-by-case basis.

20. Applicable Law, Complaints and Dispute Resolution

Any disputes related to the trust services provided under these terms shall be governed in all respects by and construed in accordance with the laws of Romania.

To the extent permitted by law, the parties shall initially seek to solve any dispute amicably and if the dispute is not resolved within thirty (30) days after the initial claim, then the Courts of Bucharest, Romania shall have exclusive jurisdiction to hear and resolving it.

Any dispute requests or claims should be sent to the contact information provided in these Terms and Conditions.

21. Conformity assessments, trust marks/logos, and audit

Audits to verify the conformity with procedural and legal provisions, particularly the conformity the document Qualified preservation service (QPS) for qualified electronic signatures/seals (QES) Policy, Code of Practice and Procedure PROVIDED BY ZIPPER SERVICES are performed every 24 months by an Authority for Conformity Assessment, based on Art. 20 of REGULATION 910/2014 EU (eIDAS).

22. Registration and identity verification points

ZIPPER register and conclude Trusted Services Agreements. More information about Trust Services Agreements can be found at the web address: https://pki.ca.ezipper.ro/