APPROVED

PMO GOVERNANCE

DORU VIJIIANU ZIPPER SERVICES SRL Digitally signed by ZIPPER SERVICES SRL Date: 2025.10.14 18:32:20 +03'00'

JUDIT FEKETE FEKETE JUDIT Digitally signed by FEKETE JUDIT Date: 2025.10.14 18:35:02 +03'00'

MIRELA OJOG Mirela Ojog Digitally signed by Mirela Ojog Date: 2025.10.14 15:26:58 +03'00'

-Zipper Services Authority-
Qualified archiving service (QAS)

Disclosure Statement

History of the edition			
Edition	**Date and description of the change**	**Ready**	**Approved**
1	01.10.2025 – First Edition	Judit Fekete	Mirela Ojog

ZIPPER

Annex A. Contents

1. Introduction

Zipper QTSP offers 'Electronic archiving' service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period.

This document is the **Disclosure Statement** of the Qualified Trust Service Provider (QTSP) Zipper concerning the qualified archiving service. 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 archiving SERVICE, according to which qualified long-term archiving service is provided.

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 archiving (QAS) - Policy, Code of Practice and Procedures (PCPP)	**1.3.6.1.4.1.57570.4.4.2** 4=> service classification node 4 => archiving services (subtree of preservation-related policies) 2=> **qualified** archiving variant

Zipper QAS 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.

The QAS is intended for Subscribers who need long-term archiving of their electronic documents signed with advanced/qualified electronic signature. The registration of documents in electronic form by the electronic archiving system certifies the official existence of those documents. The registration number uniquely identifies the document within the system. Once registered, the document cannot undergo any changes in content. At the same time as the registration, the electronic file of the document shall be completed, under the conditions of art. 8 para. (2) and (3) of Romanian Law no.

135/2007, republished.

5. Acronyms

CA Certification Authority
CRL Certificate Revocation List
OCSP On-line Certificate Status Protocol
QTSP Qualified trust service provider
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
PSP - Preservation Service Provider
RepoZip - Zipper Archiving application, registered in the Romanian Register of electronic archiving systems https://www.adr.gov.ro/arhivare-electronica/
QC - Qualified certificate
QES - Qualified electronic signature or qualified electronic seal
QPS – Qualified Preservation Service
QVS – Qualified Validation Service
QAS – Qualified Archiving Service
SubDO - Submission data object
QTSP – Qualified Trust Service Provider
TSA - Time-Stamping Authority
Zipper Services SRL - Zipper
WST - preservation service with 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 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*

Type	Current Standard	Latest Version	Title
			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.

7. Description of the Archiving Service (Scope & Lifecycle)

7.1 Mechanism

Zipper QAS use the following services:

- Zipper QPS: 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, based on QPS PCPP;
- Zipper QVS for validation of electronic signatures/seals according to ETSI TS 119 441 and ETSI TS 119 442 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.
- Zipper QTS issues qualified time-stamps according to ETSI EN 319 422

The archived objects uses preservation container for signed/sealed data object with AdES class and LTA level of signature/seal.

7.2 Information packages — Information Package Format

The Information Package is defined in a formal data definition language (XML), and is sent to the Subscriber, based on metadata list defined by the Romanian law.

The IP differentiate between mandatory and optional data elements in the definition and description of the data structure.

Optional elements in the format maybe defined as mandatory due to conditional logic (e.g. an element is optional, but if it exists the otherwise following optional requirement is mandatory).

Retention period is defined in the Subscriber`s Nomenclator (in month), but calculation of date could be relative to date of issue of the document or other date (defined in another metadata – e.g. document closing date)

7.3 Transfer submission

Zipper QTSP is responsible for the integrity and confidentiality of the transfer of the submission provided by the Subscriber and will verify if the the procedures and protocols for the transfer has been followed by the subscriber.

The exchange of information between the Subscriber and Zipper QTSP is carried out based on a signed agreement (contract), which includes the means, requirements and responsibilities related to

information security. Each agreement will contain a documented procedure for handling transfer between Zipper QTSP and Subscriber and also, the possible failures between the subscriber and Zipper EATSP.

Different communication security protocols can be applied (at data link, network, transport and application level) such as: tunneling protocols (IPSec/SSL VPN), sFTP, FTPs, HTTPS, which will be established in the signed agreement.

7.4 Information Package Verification and Preservation (POC creation)

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). The preservation of Object Container based on Qualified Preservation Service, Preservation scheme with signature/seal augmentation and with storage (F3 – comply with ETSI ES 119 512 Appendix F) will apply the following verifications:

- 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
- 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.
- 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). Receive submission is provided.
- Augmentation of POC: 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.

In case of a successful IMPORT in the electronic archive:

1. The electronic document will receive a unique ID (IDDoc/POID) for identification within the

archive. The automatically created metadata is generated. The „electronic file'' attached to each archived document will contain at least the metadata list specifie in Romanian Law 135/2007.

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 (B-LTA level)

7.5 Access

Access to 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.

7.6 Retention and Deletion

In accordance with the National Law and the regulations on document management, digital data destruction is carried out only after the legal retention period has been completed and in the presence of strictly controlled and audited processes.

Proof of deletion need to be adapted to legal compliance (e.g., GDPR, Romanian National Archives Law no. 16/1996 updated in 2025) and internal auditing procedures.

When a document reaches the retention period, our system:

- Records a possible deletion request in the audit log, mentioning the date, time, operator and reason for deletion
- Performs a final check of the list of documents before deletion, and needs operator approval
- Keeps all deletion records in logs, so that they are available for audit and legal verification, according to the Romanian and European legal framework
- If there is a requirement to extend the preservation of a document, it must be documented and approved by Romanian National Archives.

This procedure ensures compliance with national legislation, transparency of the process and the possibility of demonstrating, at any time, that the documents have been deleted legally and securely

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.

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.

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 archived/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. Rights and Obligations of Users and Relying Parties

1. 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.

2. 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.

3. 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.

4. 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.

11. 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).

12. Applicable Agreements, CPS, CP

The document Qualified archiving service (QPS) 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.

13. 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.

14. 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.

15. 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.

16. 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).

17. 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/