APROVED
GENERAL MANAGER
DORU VIJIIANU

ZIPPER SERVICES
Qualified Time-Stamping Authority
Policy & Practice Statement

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

.

Edition history			
Edition	**Date and description of the change**	**Prepared**	**Approved**
1	28.02.2022 – First edition	Mirela Ojog	Judit Fekete
2	06.02.2023 – Second Edition	Mirela Ojog	Judit Fekete

ZIPPER

Contents

1. Introduction

This document constitutes ZIPPER's Time-Stamping Authority (TSA) Policy & Practice Statement for Qualified Time Stamping Services. It is intended to describe the rules and operational procedures adopted by ZIPPER TSA for the provision of Qualified Time-Stamping Services according to Regulation (EU) N° 910/2014 (eIDAS Regulation).

ZIPPER's Qualified Time-Stamping Services support assertions of proofs that an electronic record existed before a particular time. These services can be used in support to non-repudiation services, to prove that an electronic signature was generated during the validity period of a public key certificate, to support electronic long term archiving, etc.

The current document specifies general rules used by ZIPPER TSA for the issuance of Time-Stamp Tokens (TST). It defines the parties involved, their responsibilities, rights and the applicability range.

The ZIPPER Time Stamping Services can be reached via http://tsa.ezipper.ro:8777/adss/tsa

This document is publicly available at https://pki.ca.ezipper.ro/repository/policies.php

ZIPPER Qualified Time-Stamping Services are provided according to the eIDAS Regulation, the ETSI EN 319 421 and to EN 319 422 standards and under the authority of ZIPPER acting as Qualified Time-Stamping Authority.

Management may make exceptions to this document on a case-by-case basis to mitigate material, imminent impacts to customers, partners, relying parties, and/or others where practical workarounds do not exist. Any such management exceptions are documented, tracked, and reported as part of the audit process.

2. Policy Administration

Organization Administering this Document:
ZIPPER SERVICES
Time-Stamping Authority
str. Fabricii nr. 93-103
Cluj-Napoca, 400632, Romania

Working Point:
B-dul 1 Decembrie 1918 nr. 1G,
Sector 3, Bucuresti, 032451, Romania

Working Point:
Strada Tăietura Turcului, Nr. 47, Imobilul Novis Plaza, Corp A, Et. 2,
Cluj-Napoca, 400221, Romania
https://ezipper.ro/en/

E-mail: office@ezipper.ro
Telephone +40 21.340.4638 / +40 31.101.1020
Fax: +40 21.340.4636 / +40 31.101.1022
(Mon-Fri 09.00. – 18:00 Eastern European Time)
Contact Person: Policy Administration Team

3. Approval Procedure

Approval of this document and subsequent amendments are made by the persons dedicated by ZIPPER. These persons constitute the Policy Administration Team. Management approves new versions of this document. Amended versions or updates shall be uploaded to the ZIPPER Repository located at https://pki.ca.ezipper.ro/repository/policies.php

Amended versions supersede any conflicting provisions of previous versions of this document. The Policy Administration Team shall determine whether changes to this document require a change in the TSA policy object identifiers of the Certificate policies.

4. References

The following references contain provisions which are relevant to the ZIPPER Qualified Time Stamping Authority Certificate Policy & Certification Practice Statement:

1. Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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

3. ETSI EN 319 421: “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.

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

5. IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

6. ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

7. ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

Appliable Romanian legislation:

8. Government Decision no. 89/2020 on the organization and functioning of the Romanian Digitization Authority

9. ORDER no. 449 of May 30, 2017 regarding the procedure of granting, suspending and withdrawing the status of provider of Qualified reliable services in accordance with Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014

5. Definitions and abbreviations

Term	Meaning
Qualified Trust Service Provider (QTSP)	A trust service provider that provides qualified trust services and is included in the EU trusted list.
Relying party	A Recipient of a time-stamp who relies on that time-stamp.
Subscriber	A Legal or Natural person to whom a time-stamp is issued and who is bound to any

	subscriber obligations.
Time Stamping Authority (TSA)	A Trust Service Provider (TSP) providing time-stamping services
TSA Policy & Practice Statement	Time Stamping Authority Policy and Practice: Statement of the practices that a TSA employs in issuing time stamps.
Time stamp	Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.
Time Stamp Token	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Time-Stamping Unit	Set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.
TSP	Trust Service Provider

6. General concepts

6.1 Time-Stamping Services

ZIPPER Qualified Time-Stamping Services consist of the management of the infrastructure for, and the provisioning of Time-Stamp Tokens (TST). These services are provided by the ZIPPER Time-Stamping Authority (TSA) to the Subscribers and are in accordance with the eIDAS Regulation and the ETSI standards.
ZIPPER offers Time-Stamping Services using RFC 3161 Time Stamp Protocol over HTTP transport. Each TST contains a Time-Stamping Policy identifier, unique serial number and a Time-Stamping Unit (TSU) certificate containing ZIPPER TSA identification information.
The Qualified Time-Stamping Services assure the use of a reliable time source and proper management of all system components.

6.2 Time-Stamping Authority

ZIPPER TSA is responsible for provisioning of Qualified Time-Stamping Services as described in this document. It has the responsibility for the operation of the relevant TSUs that are created and signed on behalf of the TSA. The legal entity responsible for the TSA is ZIPPER S.A. acting as a Qualified TSA.
ZIPPER issues Qualified Time Stamps under the following hierarchy:

Root CA
CN = ZIPPER Root CA G1
O = ZIPPER SERVICES SRL
OU = ZIPPER Trust Services
C = RO

Time Stamping Authority CA
CN = ZIPPER TSA G1
O = ZIPPER SERVICES SRL
OU = ZIPPER Time Stamping Services
2.5.4.97 = VATRO-16723187
C=RO

Time Stamping Unit CA
CN = ZIPPER TSU 2023 A
OU = ZIPPER Time Stamping Services
O = ZIPPER SERVICES SRL
2.5.4.97 = VATRO-16723187
C = RO

ZIPPER TSA and TSU certificates are issued according to the following certificate policies:

- **OID 0.4.0.2042.1.2** itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)
- **OID 0.4.0.2023.1.1**: itu-t(0) identifiedorganization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

• OID Tree	
1.3.6.1.4.1.57570	Identification Number (OID) of Zipper Services SRL, registered to IANA
1.3.6.1.4.1.57570.1	Trust Service Provider
1.3.6.1.4.1.57570.1.1	Trust Services Certificate Policy (CP)
1.3.6.1.4.1.57570.1.1.1	Qualified Trust Services Certificate Practice Statement (CPS)
1.3.6.1.4.1.57570.1.1.1.1	Qualified Time Stamping Services

6.3 Subscribers

The Subscriber is the applicant, natural or legal person, to whom the time stamp is provided and who enters into a contractual relationship with ZIPPER.
When the Subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

The Subscriber may be an organization comprising of several end-users or an individual end-user.
When the Subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users, therefore the organization shall duly notify its end-users. In any case, the organization will be held responsible if the obligations are not correctly fulfilled by the end-users.

6.4 Relying Parties

A Relying Party is an individual or entity who receives a digital document that is time-stamped and acts in reliance of a certificate and/or a digital signature issued under the TSA. A Relying Party must evaluate the correctness and validity of the document itself in the contexts where it is used.

6.5 Other Participants

Not applicable.

6.6 Time Stamps Usage

Time stamps issued by ZIPPER, as specified in this document, are qualified within the meaning of the eIDAS Regulation.
Time Stamps shall be used only to the extent the use is consistent with applicable law and within the limits and contexts specified in the present document. Any use outside the limits and contexts specified in this document or for unlawful purposes, or contrary to public interest, or otherwise likely to damage the business or reputation of ZIPPER is prohibited. Indicatively, the use of Time Stamps to time-stamp documents which can lead to unlawful consequences is prohibited.

7. TSA Policy and Practice Statement

7.1 Purpose

This section specifies policy and security requirements relating to the operation and management practices of the ZIPPER as a Time Stamping Authority (TSA) for issuing Qualified Time Stamps. These can be used in support of

electronic signatures or for any application requiring to prove that a datum existed before a specific time.
This document can be used by independent entities as the basis for confirming that ZIPPER TSA is a trusted entity for the issuance of Qualified Time Stamps in accordance with the eIDAS Regulation.
The present document contains specific details of the operating environment, organizational structure, operating procedures, facilities, and computing environment of the ZIPPER TSA. It describes only general rules of issuing and managing TSTs. Detailed description of the infrastructure and related operational procedures are described in additional documents that are not publicly available. These additional documents are only available to authorized ZIPPER personnel and, on a need-to-know basis, to the conformity assessment body auditing the Time-Stamping Services.

8. TSA Policy

8.1 Overview

The TSAP Policy defines a set of rules used during the issuance of TSTs and regulates the security level for ZIPPER TSA. ZIPPER TSA issues TSTs according to ETSI EN 319 422.
ZIPPER TSU issues qualified electronic time-stamps as per the eIDAS regulation; ZIPPER TSU does not issue non-qualified electronic time-stamps.
TSTs are issued with an accuracy of one (1) second.
Time-stamps are requested by means of Hypertext Transfer Protocol (HTTP), as described by RFC 3161.

8.2 Identification

The object-identifier (OID) of the ZIPPER TSA Policy & Practice Statement is 57570.:

1.3.6.1.4.1.57570	Identification Number (OID) of ZIPPER, registered to IANA
1.3.6.1.4.1.57570.1	Certification Service Provider
1.3.6.1.4.1.57570.1.1	Qualified Certificate Policies
1.3.6.1.4.1.57570.1.1.1	Qualified Time Stamping Services

This OID is referenced in every TST issued by ZIPPER, and the ZIPPER TSA Policy & Practice Statement is available to both Subscribers and Relying Parties.
ZIPPER issues TSTs in accordance with ETSI EN 319 421 best practice for time-stamping policy
(OID 0.4.0.2023.1.1).

8.3 User Community and Applicability

There are no limitations on users' eligibility or applicability of the services delivered. ZIPPER TSA can provide Time-Stamping Services to any user, including closed communities.
ZIPPER does not provide public Time-Stamping Services.

8.4 Conformance

ZIPPER TSA uses the identifier in TSTs as given in section "Identification".
ZIPPER TSA ensures compliance of the provided services with regulations specified in section "Compliance with Legal Requirements" and ensures reliability of control mechanisms described in section "TSA Practices".

9. Obligations and Liability

This chapter includes all the obligations, liabilities, guarantees and responsibilities of the ZIPPER TSA, its Subscribers and TST users (Subscribers and Relying Parties). These obligations and responsibilities are regulated by agreements accepted by all parties.
ZIPPER operates the ZIPPER TSA and assumes responsibility that the requirements of section "TSA Practices" of this document, as well as the provisions of the eIDAS, are implemented.
ZIPPER's agreements with Subscribers and Relying Parties describe mutual obligations and responsibilities,

including financial responsibilities. The ZIPPER TSA Policy & Practice Statement (this document) is an integral part of these agreements.

9.1 TSA Obligations & Guarantees towards Subscribers

ZIPPER guarantees an availability of 99.00 % of the Time-Stamping Services on a 24/7 basis excluding scheduled technical breaks, concerning equipment and system conservation.
ZIPPER undertakes the following obligations towards Subscribers:

- To operate in accordance with this ZIPPER TSA Policy & Practice Statement (this document) and other relevant operational policies and procedures;
- To ensure that TSUs maintain a minimum UTC time accuracy of ± 1 second;
- To maintain a competent and experienced team that can ensure the continuity of the Time-Stamping Services;
- To ensure on a permanent basis the physical and logical security, as well as the integrity of materials, software and databases required for the correct functioning of the Time-Stamping Services;
- To monitor and control the Time-Stamping Services and the whole TSA infrastructure, in order to prevent or limit any disturbance or unavailability of the Time-Stamping Services;
- To undergo internal and external reviews to assure compliance with relevant legislation and internal ZIPPER policies and procedures;
- To provide high availability access to ZIPPER TSA systems except in the case of planned technical interruptions and loss of time synchronization.

9.2 Subscriber Obligations

Subscribers should verify the signatures created by ZIPPER TSA on the TST.
Such verification comprises of:

- Verification whether the TSA signature on the TST is valid.
- Verification of the TSA certificate:
    - Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself)
    - Verification whether the certificate is not expired at the moment of TSA signature
    - Verification whether the certificate was not revoked at the moment of TSA signature.

Subscribers must use secure cryptographic functions for time-stamping requests.
Further Subscriber obligations may also be defined in ZIPPER's Terms and Conditions for Time-Stamping Services.

9.3 Relying Party Obligations

Relying parties should verify the signatures created by ZIPPER TSA on the TST.
Such verification comprises of:

- Verification whether the TSA signature on the TST is valid.
- Verification of the TSA certificate:
    - Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself)
    - Verification whether the certificate is not expired at the moment of TSA signature
    - Verification whether the certificate was not revoked at the moment of TSA signature.

Relying Parties should take into account any limitations on the usage of the time stamp indicated by the ZIPPER TSA Policy & Practice Statement. If the verification takes place after the end of the validity period of the Certificate, Relying Parties should follow the guidance denoted in Annex D of ETSI EN 319 421.
Relying parties are expected to use a Trusted List to establish whether the TSU and the Time Stamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time stamps issued by this TSU can be considered as qualified. The qcStatement "esi4-

qtstStatement-1" as defined in clause 9.1 ETSI EN 319 422, is used as an indication that the Time Stamp is qualified.

9.4 Liability

The liability of ZIPPER acting as a TSA and of Subscribers and Relying Parties connected with the Time-Stamping services is specified in the relevant agreement or is as foreseen in the applicable legislation.
ZIPPER is responsible for possible damages directly determined, intentionally or by negligence, to any natural or legal person, as a result of failure to comply with the obligations set out in this document and the Eidas Regulation.
ZIPPER Terms and Conditions for Time-Stamping Services limit ZIPPER's liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include a liability cap regarding the combined aggregate liability of ZIPPER to any and all persons concerning Time-Stamping Services, which is limited to an amount not exceeding that of the respective contract for the Time-Stamping Service, and a total maximum of 500.000EUR, regardless of the nature of the liability and the type, amount or extent of any damages suffered. The liability limitations shall be the same irrespective to the number of Time Stamps or claims related to such Time Stamp or Time-Stamping Service.
ZIPPER TSA is in no way liable for the use of the TSTs it delivers and signs.

10. TSA Practice Statement

This section establishes the general rules concerning the technical, organizational, and procedural requirements of the ZIPPER TSA operation. ZIPPER TSA implements controls that meet ETSI EN 319 421 and ETSI EN 319 422 requirements.
Time-Stamping Certificates are valid for five (5) years but require re-keying every year. Therefore, logs and records for Time-Stamping are retained for one (1) year after the expiration of the TSU Certificate.
A risk assessment is regularly carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures that have been taken.
The ZIPPER Terms and Conditions for the use of Time-Stamping Services are disclosed and made available to all Subscribers and Relying Parties as specified in the present document.
ZIPPER Policy Administration Team has responsibility for maintaining, updating and reviewing all policies, practices and procedures according to the terms of section "Policy Administration" of this document. Management has responsibility to ensure that these policies, practices and procedures are approved and properly implemented.

10.1 Key Management Life Cycle

10.1.1 TSA Key Generation

Personnel in trusted roles under dual control perform the generation of the TSU signing keys in a physically secured environment. The personnel authorized to carry out this function are limited to those required to do so under the TSA practices.

The generation of the TSU signing keys is carried out within secure cryptographic devices, which meets the requirements identified in FIPS 140-2 level 3.

Key Pairs are generated using secure algorithms and parameters based on current research and industry standards following the recommendations of ETSI TS 319 312.
The activities performed in each key generation are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by ZIPPER Management.

10.2 TSU Private Key Protection

ZIPPER takes specific steps to ensure that TSU private keys remain confidential and maintain their integrity.

TSU private keys are stored in a secure Hardware Security Module to perform key signing operations, which comply

with at least FIPS 140-2 level 3 or equivalent EAL 4+ or higher in accordance to ISO/IEC 15408 specifications. Special controls are in place to ensure that the hardware has not been tampered and is functioning correctly.
TSU private keys cannot be extracted in any form and are not accessible outside the Hardware Security Module.
ZIPPER creates backup copies of TSU private keys, for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules. Cryptographic modules used for private key storage meet the requirements of this CPS. Private keys are copied to backup hardware cryptographic modules. Restoring of TSU backup keys require dual control in a physically secured environment.

10.1.3 TSU Public Key Distribution

ZIPPER TSU Public Keys are made available in a Digital Certificate.
ZIPPER TSU Certificates are available for secure download via the ZIPPER Repository website https://pki.ca.ezipper.ro/repository/certs.php They can also be found in the EU Trusted List.

10.1.4 Rekeying TSU's Key

The operation period for TSU key pairs is defined by setting a private key usage period within the TSU's public key certificate.
ZIPPER TSTs are signed with ZIPPER TSU certificates of five (5) years validity. ZIPPER TSU certificates of five (5) years validity are only used to sign TSTs during a usage period of one (1) year.
ZIPPER TSU rekey procedure is executed upon expiry of the usage period (1 year) of the TSU certificate. Public keys are archived for a period of at least ten (10) years from the expiration date of the certificate.

10.1.5 End of TSU Key Life Cycle

ZIPPER TSA ensures that TSU private signing keys are not used beyond the end of their life cycle. In particular, operational and technical procedures are in place to ensure that a new key is put in place before a TSU's key usage period expires, and that TSU private keys or any part, including any copies are destroyed such that the private key cannot be retrieved.
TST generation system shall reject any attempt to issue a TST if the signing private key is expired or if the signing private key usage period is expired.

10.1.6 Life Cycle Management of the Cryptographic Module used to Sign Time-stamps

ZIPPER TSA ensures the security of the HSM throughout its lifecycle.
ZIPPER has in place procedures to ensure that:

- Hardware Security Modules are not tampered with in shipment or storage.
- Acceptance testing is performed to verify that cryptographic hardware is performing correctly.
- Installation, activation and duplication of TSU's signing keys in HSMs is done only by personnel in trusted roles, in a physically secure environment.
- TSU private signing keys stored on HSM are erased upon device retirement in according with the manufacturer's instructions.

10.2 Time-Stamping

10.2.1 Time-Stamp Token

ZIPPER has in place technical procedures to ensure that TSTs are issued securely and include the correct time.
Each TST includes:

- a representation of the datum being time-stamped as provided by the applicant
- a unique serial number to identify specific TST
- a unique identifier of the policy as described in the present document
- an electronic signature generated using a key used exclusively for Time-Stamping
- an identifier for the TSA and the TSU.
- date and time value traceable to the real UTC time value
- signature algorithm used in the TST.

ZIPPER TSUs maintain audit logs for all calibrations against the UTC references.

10.2.2 Clock Synchronization with UTC

ZIPPER TSA ensures that its time is synchronized with UTC within the declared accuracy with multiple independent time sources. ZIPPER TSA incorporates the time in the TST with the accuracy described in section 8.1 of this document.
Audit and calibration records of the synchronization are maintained by ZIPPER. ZIPPER TSA ensures that:

- if the time indicated in a TST drifts or jumps out of synchronization with UTC, this will be detected.
- if the TSU time drifts outside the declared accuracy, and recalibration fails, the TSA will not issue time-stamps until correct time is restored.

ZIPPER implements security controls preventing unauthorized operation, aimed at calibration of TSA time.

10.2.3 Leap Second handling procedure

A leap second is an adjustment to UTC by skipping or adding an extra second on the last second of a UTC month. First preference is given to the end of December and June, and second preference is given to the end of March and September.
ZIPPER monitors that synchronization is maintained when a leap second occurs.

10.3 TSA Management and Operation

10.3.1 Security Management

ZIPPER TSA ensures that administrative and management procedures are applied which are adequate and correspond to recognized best practices.
ZIPPER performs all TSA functions using trustworthy systems that meet the requirements of ZIPPER ISMS.

10.3.2 Asset Classification and Management

ZIPPER maintains an inventory of all assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

10.3.3 Personnel Security

ZIPPER maintains appropriate personnel controls fulfilling security best practice and the requirements of relevant standards.
Managerial and operational personnel possess the appropriate skills and knowledge of Time-Stamping, digital signatures and Trust Services as well as security procedures for personnel with security responsibilities, information security and risk assessment.
ZIPPER implements the Trusted Roles Policy for all those employees that have access to or control cryptographic operations. Trusted Persons and Roles include, but are not limited to:

- Cryptographic business operations personnel,
- Security personnel,
- System administration personnel,
- Designated engineering personnel, and
- Executives that are designated to manage infrastructural trustworthiness.

Prior to commencement of employment in a Trusted Role, ZIPPER conducts background checks which may include indicatively the following:

- Verification of identity
- Check of previous employment and professional reference;
- Confirmation of the highest or most relevant educational degree obtained;

- Verification that there is no criminal conviction;
- Check of financial records.

ZIPPER requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently, as specified in the employment contract and job description, before they perform any operational or security functions.
Employment contracts signed by the employees include confidentiality provisions for information that comes to their knowledge in the course of their performance.
ZIPPER ensures that personnel have achieved trusted status and departmental approval has been given before such personnel are:

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

User accounts are created for personnel in specific roles that need 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 other use. User accounts are locked as soon as possible when the role change dictates.

10.3.4 Physical and Environmental Security

ZIPPER implements the Physical Security Policy, which supports the security requirements of this TSA Policy & Practice Statement.
ZIPPER TSA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.
ZIPPER also maintains Disaster Recovery facilities for its Time-Stamping Services operations. ZIPPER's Disaster Recovery facilities are protected by multiple tiers of physical security comparable to those of ZIPPER's primary facility.
The physical security system includes tiers for key management security which serves to protect both online and offline storage of Cryptographic Signing Unit (CSUs) and keying material. Areas used to create and store cryptographic material enforce access control. Access to CSUs and keying material is restricted in accordance with segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.
ZIPPER operations are protected using physical access controls making them accessible only to appropriately authorized individuals. Access to secure areas of buildings requires the use of an "access" card and/or and biometrics. Access card use is logged by the building security system.
Access card logs are reviewed on a regular basis.
ZIPPER's secure facilities are equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control 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 damaging exposure to flame or smoke.
All media containing production software and data, audit, archive, or backup information is stored within ZIPPER facilities or in secure off-site storage facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such 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. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed prior to disposal.

10.3.5 Operations Management

ZIPPER TSA ensures that the procedures, processes and infrastructure to comply with the operational

management, procedural security requirements, system access management, trustworthy systems deployment and maintenance, business continuity management and incident handling as defined in ETSI EN 319 421.
The operations management procedures for the ZIPPER TSA are incorporated within the overall ZIPPER internal operations management procedures.

10.3.6 Compromise of TSA Services

In the event of compromise of a TSU signing key, ZIPPER will revoke the relevant Certificate and add it to the ZIPPER CRL. The TSU will not issue time-stamps if its private key is not valid.
In the event of a loss of clock calibration, ZIPPER will not issue time-stamps until steps are taken to restore calibration of time.

10.3.7 TSA Termination

The TSA is terminated:

- with a decision of ZIPPER's Board of Directors;
- with a decision of the authority exercising supervision over the Time-Stamping Services;
- with a judicial decision;
- upon the liquidation or termination of ZIPPER's operations.

ZIPPER ensures that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation of ZIPPER's services, and in particular, it ensures the continued maintenance of information required to verify the correctness of the services.
In the event that it is necessary for ZIPPER TSA, to cease operation, ZIPPER shall make a commercially reasonable effort to notify Subscribers and Relying Parties of such termination in advance of the TSA termination.
ZIPPER TSA shall revoke the TSU certificates upon termination of its services.

10.3.8 Compliance with Legal Requirements

ZIPPER ensures compliance with legal and regulatory applicable requirements, i.e. the following:

- 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 (eIDAS Regulation);
- Personal Data legislation (including Regulations (EU) No 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);
- European Standards:
    - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
    - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and Security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
    - ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates;
    - 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

ZIPPER acting as a Qualified Trust Service Provider is subject to compliance audits for its TSA and Time-Stamping Services to ensure they meet the requirements of the eIDAS Regulation.

10.3.9 Record Concerning Time-Stamping Services

ZIPPER TSA ensures that all relevant information concerning the operations of the ZIPPER Time Stamping Services is recorded for a defined period, in particular for providing evidence for the purposes of legal proceedings. The following records are maintained:

- Synchronization of clocks used in time-stamping
- Detection of loss of synchronization
- Time-stamp requests and created time-stamps
- Events relating to the lifecycle of TSU keys and Certificates

ZIPPER maintains records of all relevant information concerning the operation of the ZIPPER TSA for the time period specified in Section 10.1.4.

10.3.10 Organizational reliability

ZIPPER TSA ensures that its organization is reliable as required in ETSI EN 319 421. ZIPPER has the financial stability and resources required to operate in conformity with this TSA Policy & Practice Statement.