certSIGN Time Stamping Authority 2 Policy and Practice Statement

Version 3.6

Date: 22 June 2026

Security Level

Public Document

Important Notice

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Phone: 004-021-31.19.901

Web: www.certsign.ro

Document history

Version	Effective Date (the last day of the month)	Reason	The person who made the change
1.0	January 2017	Releasing the first version	Electronic Services Manager
2.0	March 2017	Second version, after interim audit	Information Security Officer
2.1	April 2017	Minor update for clarification	Information Security Officer
2.2	February 2018	Annual review	Information Security Officer
2.3	November 2018	Update change headquarters	PKI Policies Manager
2.4	January 2019	Annual review	PKI Policies Manager
2.5	March 2019	Minor update for clarification	PKI Policies Manager
2.6	April 2019	Minor update for clarification	PKI Policies Manager
2.7	January 2020	Annual review	PKI Policies Manager
2.8	January 2021	Annual review	PKI Policies Manager
2.9	January 2022	Annual review	PKI Policies Manager
3.0	January 2023	Annual review	PKI Policies Manager
3.0a	April 2023	Update links	PKI Policies Manager
3.1	January 2024	Annual review	PKI Policies Manager
3.2	15 January 2025	Annual review	PKI Policies Manager
3.3	18 July 2025	Add TSU Life-cycle	PKI Policies Manager
3.4	15 January 2026	Annual review	PKI Policies Manager
3.5	31 March 2026	Updates for eIDAS2 conformity	PKI Policies Manager
3.6	22 June 2026	Add SHA512	PKI Policies Manager

This document was created by and is property of:

Owner	Author	Dated created
Information Security Officer	Information Security Officer	December 2016

Distribution list

Destination	Distribution date
Public-Internet	February 2017
Public-Internet	April 2017
Public-Internet	February 2018
Public-Internet	November 2018
Public-Internet	January 2019
Public-Internet	March 2019
Public-Internet	April 2019
Public-Internet	January 2020
Public-Internet	January 2021
Public-Internet	January 2022
Public-Internet	January 2023
Public-Internet	April 2023
Public-Internet	Ianuarie 2024
Public-Internet	January 2025
Public-Internet	July 2025
Public-Internet	January 2026
Public-Internet	March 2026
Public-Internet	June 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	February 2017
2.0	Policies and Procedures Management Body	March 2017
2.1	Policies and Procedures Management Body	April 2017
2.2	Policies and Procedures Management Body	February 2018
2.3	Policies and Procedures Management Body	November 2018
2.4	Policies and Procedures Management Body	January 2019
2.5	Policies and Procedures Management Body	March 2019
2.6	Policies and Procedures Management Body	March 2019
2.7	Policies and Procedures Management Body	January 2020
2.8	Policies and Procedures Management Body	January 2021
2.9	Policies and Procedures Management Body	January 2022
3.0	Policies and Procedures Management Body	January 2023
3.0a	Policies and Procedures Management Body	April 2023
3.1	Policies and Procedures Management Body	January 2024
3.2	Policies and Procedures Management Body	January 2025
3.3	Policies and Procedures Management Body	July 2025
3.4	Policies and Procedures Management Body	January 2026
3.5	Policies and Procedures Management Body	March 2026
3.6	Policies and Procedures Management Body	June 2026

Contents

1 Scope

This document is the certSIGN Time Stamping Authority 2 Policy and Practice Statement (**TSPS**). You must read the **TSPS** before you apply for the certSIGN Time Stamping Authority 2 Service. The purpose of this document is to specify policy and security requirements relating to the operation and management practices of certSIGN as a Time Stamp Authority in accordance with the ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" standard (hereinafter, certSIGN Time Stamping Authority 2 or certSIGN TSA) for issuing qualified electronic time stamps. These can be used in support of electronic signatures or for any application requiring the proof that a datum existed before a specific time.
This version of the TSPS has been approved for use by the certSIGN Policies and Procedures Management Body and is subject to amendment and change in accordance with the policies and guidelines adopted, from time to time, by the certSIGN Policies and Procedures Management Body, conforming to section 6.2.9. The date on which this version of TSPS becomes effective is indicated on this document.

2 References

2.1 Normative references

1. 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
2. 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
3. IETF RFC 3161 "Internet X.509 Public Key Infrastructure Time-stamp Protocol"
4. ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
5. ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"
6. ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
7. Law no.214/2024 on the use of electronic signatures, time-stamping and the provision of trust services based on them.

2.2 Informative references

1. Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
2. IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification"
3. Terms and Conditions for time-stamping customers
4. ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
5. ISO/IEC 15408 (parts 1 to 3): "Information technology – Security techniques – Evaluation criteria for IT security".
6. FIPS PUB 140-3 (2019): "Security Requirements for Cryptographic Modules".

3 Definitions and abbreviations

3.1 Definitions

- **Coordinated Universal Time (UTC)**: Time scale based on the second as defined in Recommendation ITU-R TF.460-6. For all practical purposes, UTC is equivalent to the solar time average in the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and the solar time derived from the irregular Earth rotation. The UTC is the principal standard of the hour by which the world regulates clocks and the time.
- **NTP**: "Network Time Protocol (NTP) is a networking protocol for clock synchronization of computer systems over network packet routing with variable latency. The standard for reference is the IETF RFC 1305 (Network Time Protocol (NTP v3)).
- **Ministry of Communications and Information Society**: for legal purposes declared as National Standard of this unit, as well as maintenance and official dissemination of the scale "Coordinated Universal Time"
- **Relying party**: The recipient of a time-stamp who relies on that time-stamp.
- **Stamping Authority (TSA)**: It is the TSP providing time-stamping services using one or more time-stamping units.
- **Subscriber**: Legal or natural person to whom a time-stamp is issued.
- **Time-stamp**: Data in electronic form which binds other electronic data to a time, providing evidence that these data existed at such time.
- **Time-stamp policy**: A set of rules that indicate the applicability of a time-stamp to a community and/or class of application of the common security requirements. This is a specific type of trust service policy as defined in ETSI EN 319 421.
- **Time-stamping service:** trust service for issuing time-stamps.
- **Time-Stamping Unit (TSU)**: The set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.
- **Trust Service Provider (TSP)**: entity which provides one or more trust services.
- **TSA Disclosure statement**: set of statements about the policies and practices of a TSA which particularly require emphasis in the disclosure to subscribers and relying parties, for example to meet regulatory requirements.
- **TSA practice statement**: statement of the practices that a TSA employs in issuing time-stamps.
- **TSA system**: Set of IT products and components employed to provide support to the provision of time-stamping services.
- **UTC (k)**: time scale given by the laboratory "k" and which has a close relation to the UTC, with the goal to reach ±100 ns.
- **certSIGN TSA:** represents "certSIGN Time Stamping Authority 2" that is the certSIGN Time Stamping Authority functioning in accordance with the ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"

3.2 Abbreviations

For the purposes of the present document, the abbreviations are as follow:

BIPM Bureau International des Poids et Mesures
CA Certification Authority
IT Information Technology
PPMB Policies and Procedures Management Body
TAI International Atomic Time
TSA Time-Stamping
TSP Trust Service Provider
TST Time Stamp Token
TSU Time-Stamping Unit
UTC Coordinated Universal Time

4 General Concepts

4.1 Concepts and general requirements

TSPS is a detailed description of the terms and conditions regarding the provision of the services, of managerial and operational practices that the certSIGN Time Stamping Authority 2 applies in the provision of timestamping services.

4.2 Time-stamping services

The provision of time-stamping services is broken down, in the present document, into the following component services for the purposes of classifying requirements:

- **Time-stamping provision**: This service component generates TSTs.
- **Time-stamping management**: the service component that monitors and controls the operation of time-stamping services to ensure that the service provided is as specified in the CPS and TSA CPS.

certSIGN TSA adheres to the standards and regulations established in section 2 of this document to keep trustworthiness of the time-stamping services for subscribers and relying parties.

4.3 Time-stamping services parties

4.3.1 Time-stamping authority (TSA)

A Trust Service Provider (TSP) providing time-stamping services to the public, is called the Time-Stamping Authority (TSA). The TSA has the overall responsibility for the provision of the time-stamping services identified in clause 4.2. The TSA has responsibility for the operation of one or more TSUs which create and sign on behalf of the TSA. The TSA responsible for issuing a time-stamp is identifiable.
certSIGN TSA hereby confirms, that the TSA is audited at least every 24 months by a conformity assessment body. The assessment report is submitted to the national supervisory body. If the supervisory body requires the TSA to remedy any failure to fulfil requirements, certSIGN as TSA shall act accordingly and in a timely manner.

The supervisory body shall be informed of any change in the provision of the TSA.
certSIGN TSA may make use of other parties to provide parts of the time-stamping services. However, the TSA always maintains overall responsibility (as per clause 6.5) and ensures that the policy requirements identified in the present document are met.
certSIGN TSA may operate several identifiable time-stamping units.
certSIGN TSA is a qualified trust service provider as described in eIDAS which issues qualified time-stamps. certSIGN TSA is identified in the TSU certificate used for signing the TST.

Contact Information:

certSIGN SA
Address: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania
Phone: 004-021-31.19.901
Web: www.certsign.ro

4.3.2 Subscriber

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations

are not correctly fulfilled.
When the subscriber is an organization, it comprises several end-users or an individual end user and some of the obligations that apply to that organization must apply to the end- users as well. In any case, the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such organization is expected to suitably inform its end users.

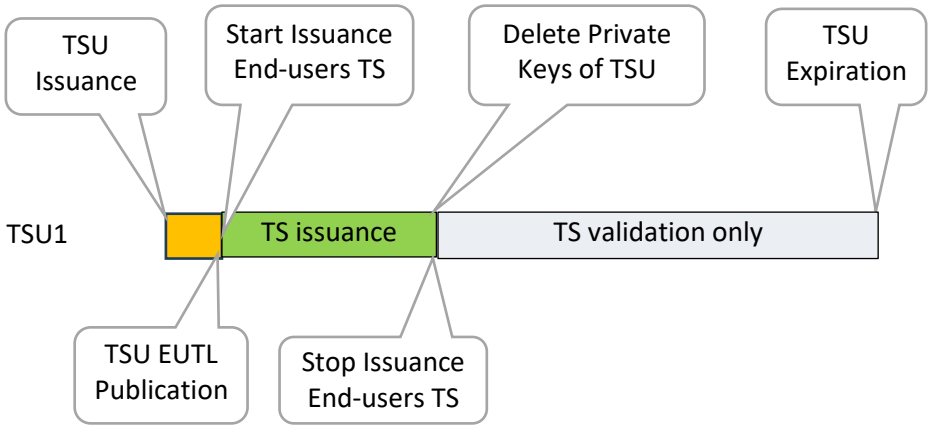
4.3.3 TSA relying party

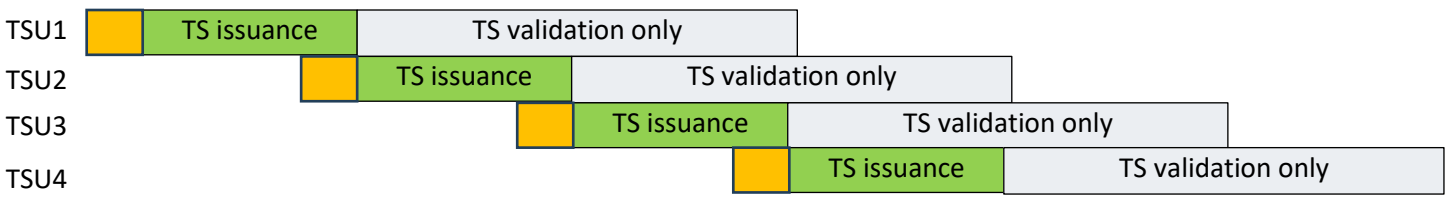
A relying party is an individual or entity that acts in reliance on a TST generated under certSIGN's TSA policy [ETSI EN 319 421]. A Relying Party may be, or not a subscriber.

4.4 TSU life-cycle

certSIGN issues each year a new time-stamp certificate, a TSU, with a validity of max 3 years. The newest unit (TSU1) will issue end-user time-stamps for a duration of one year since its publication in EU TL. Between the TSU certificate issuance and its publication in EU TL may be a difference of 1-2 month.
After one year, when the new time-stamp unit certificate (TSU2) will be issued and then published in the EU TL, the previous time-stamp unit certificate (TSU1) will expire or will have the private keys deleted in order to be used only for validation of the already issued end-user time-stamp certificates.
The new unit TSU2 will become the active TSU that will issue end-user time-stamps.
After another year, a new time-stamp unit certificate will be issued, TSU3, and will be published in the EU TL. The previous time-stamp unit certificate (TSU2) will expire or will have the private keys deleted in order to be used only for validation of the already issued end-user time-stamp certificates.

After another year, a new time-stamp unit certificate will be issued, TSU4, and will be published in the EU TL. The previous time-stamp unit certificate (TSU3) will expire or will have the private keys deleted in order to be used only for validation of the already issued end-user time-stamp certificates.
And the life-cycle continues year by year, according to the image below.





5 Time-stamp policies

5.1 General

certSIGN TSA issues the TST's in accordance with ETSI EN 319 421 and the Time-Stamping Policy. The TST's are issued with an accuracy of 1 second of UTC or better.

5.2 Identification

The identifier of the time-stamp policy specified in the present document is OID:

1.3.6.1.4.1.25017.2.2.1

{iso(1) identified-organization(3) dod(6) internet (1) private(4) enterprise(1) certSIGN (25017) TSA(2) CPS-PC-EU Regulation 910/2014(2)}

- 1 is the number of the TS Unit

By including this object identifier in the generated time-stamps, certSIGN TSA claims conformance with this time-stamp policy.

Time-stamps may include also the OID **0.4.0.2023.1.1**, if this is specified in the time-stamp request content.

5.3 User community and applicability

This policy aims at meeting the requirements of time-stamp for long term validity (e.g. as defined in ETSI EN 319 122), but it generally applies to any use that includes a requirement for equivalent quality. This policy may be used for public time-stamping services or for time-stamping services used within a closed community.

6 Policies and Practices

6.1 Risk assessment

certSIGN TSA performs risk assessments on a regular basis to ensure the quality and reliability of time-stamping services. Security Controls that are defined in a security framework for time-stamping services, are controlled every six months to ensure their efficiency.
certSIGN's Risk Management process covers in detail this topic.

6.2 Trust service practice statement

Quality Assurance is one of the most important values of certSIGN TSA. Therefore, a variety of security controls have been implemented to ensure the quality, performance and operation of the time-stamping service.
Security controls are documented and are regularly reviewed by an independent entity, trustworthy and capable of verifying the adherence to security controls.
Additionally, for compliance with ETSI EN 319 421, the following measures were implemented for the following services.

6.2.1 Time-stamp format

The time-stamp token issued by certSIGN TSA is compliant to RFC 3161 time-stamps. The service issues time stamps with an RSA algorithm and a key length of 4096[1], which accepts SHA512, SHA384, and SHA256 hash algorithm.

6.2.2 Time accuracy

The TST's are issued with an accuracy of 1 second of UTC or better.

6.2.3 Limitations of the service

The time stamp service of certSIGN TSA may be used, without limitation, in relation to any legal transactions.

Within the limit set by the Romania Law, in no event (except for fraud or willful misconduct) certSIGN will be held liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures;
- Any other damages.

certSIGN undertakes no financial responsibility for improperly used time-stamps.

certSIGN will cover the damages it might cause by time-stamp services for persons that build their moral on the legal effects of the qualified certificates up to the equivalent in lei of the amount of 10.000 euro for every risk insured. The insured risk represents every damage caused even if there are more such damages caused by the provider's failure to fulfill the liabilities under the law.

6.2.4 Obligations of the subscribers

For detailed information please, see the "Terms and conditions for time-stamp services".

[1] *Current active TSU issue with a key length of 2048. Next TSU, from Q4 2026, will issue with 4096 bits.*

6.2.5 Obligations of relying parties

For detailed information please see the "Terms and conditions for time-stamp services".

6.2.6 Time-stamp verification

Time-stamp verification includes the following:

Verification of the time-stamp issuer

The issuer is a time-stamping authority that uses an appropriate private key and a digital certificate for issuing the time-stamp. The public key included in the TSU certificate and CA certificates are used to perform the verification that the time-stamp has been correctly signed by the TSA.

Verification of the TSU certificate revocation status

Revocation checking of the TSU certificate shall be done using OCSP service available at http://ocsp.certsign.ro or CRL available at https://crl.certsign.ro/certsign-qualifiedca2023rsa.crl.

Verification of the time-stamp integrity

The cryptographic integrity of the time-stamp, for example the ASN.1 structure is correct, and the datum (the data that have been time-stamped) belong to the application. It can be verified through the certSIGN TSA's web service form certSIGN, offered free of charge.

6.2.7 Applicable law

For detailed information please see "Terms and conditions for time-stamp services".

6.2.8 Service availability

certSIGN TSA has implemented the following measures to ensure availability of the service:

- Redundant setup of IT Systems to avoid single point failures.
- Redundant high speed internet connections to avoid loss of service
- Use of uninterruptable power supplies and electric generator.

Although these measures ensure service availability of the certSIGN TSA, an annual availability of 100% cannot be guaranteed. certSIGN TSA aims to provide an availability of the service of 99% per year.

6.2.9 Practice statement approval procedures

certSIGN is responsible via its Policies and Procedures Management Body for the approval and change of the TSPS. The TSPS is reviewed at least once a year.

The only changes that the PPMB may make to these TSPS specifications without notification are minor changes that do not affect the assurance level of this TSPS, e.g., editorial or typographical corrections, or changes to the contact details.

Errors, updates, or suggested changes to this document are communicated including a description of the change, a change justification, and contact information of the person requesting the change.

The PPMB shall accept, modify or reject the proposed change after completion of a review phase.

Any changes to the CPS are approved by the PPMB and, if necessary, are announced to certSIGN's customers. Subjects/Subscribers shall comply only with the currently applicable CPS.

Subscribers shall comply only with the currently applicable document. Subscribers who do not accept new, modified terms and regulations of TSPS shall make a suitable statement within 15 days of the effective date of the new published version of the TSPS. This will lead to termination of the contract related to time-stamping services provided.

6.3 Terms and conditions

The published document "Terms and conditions for time-stamp services" contains information

about e.g. limitation of the service, subscriber's obligations, information for relying parties or limitations of liability. Additionally, the following information applies:

6.3.1 Implementation of the trust service policy

The present document contains information about the applicable trust service policy. See chapter 5 for further information.

6.3.2 Retention time of logs

TSP event logs are stored in files, on the system disk, until they reach the maximum allowed capacity. After exceeding the allocated space, the logs archived and are available only off-line. Archived logs are stored for at least 10 years.

6.4 Information security policy

certSIGN TSA has implemented an information security policy throughout the company. All employees must adhere to the regulations stated in this policy and the derived security concepts. The information security policy is reviewed on a regular basis and especially when significant changes occur. The Board of certSIGN approves the changes in the information security policy.

6.5 TSA Obligations

6.5.1 TSA obligations towards subscribers

Conformance with the procedures stated in the present document is ensured by certSIGN TSA. An independent supervisory body verifies the efficiency of procedures on a regular basis.

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the clause 11 from the document **Terms and conditions** for the use of the time stamp service offered by certSIGN Time Stamping Authority 2**.**

6.6 Information for relying parties

- Relying Parties verify that the TST has been correctly signed with the corresponding key of the TSU certificate and ensure that the private key used to sign the TST has not been revoked.
- Relying Parties are obliged to take the necessary measures to ensure the TST validity beyond the life-time of certSIGN TSA certificates.
- Must consider any limitations on the time-stamp usage of indicated in the time-stamp policy.
- Must consider any other precautions prescribed in agreements or elsewhere.

7 TSA Management and Operations

7.1 Introduction

certSIGN TSA has implemented an information security management system to maintain the service security.
The provision of a TST in response to a request remains at the discretion of certSIGN TSA, depending on the subscriber's agreement

7.2 Internal organization

certSIGN's organizational structure, policies, procedures and controls are applicable to certSIGN TSA.
Organizational procedures comply with the rules and regulations defined in section 2.1 of this document.

a) Legal entity

The Time-Stamping Authority is provided by certSIGN SA.

certSIGN SA, is a technology company that specializes in developing and manufacturing IT security products, solutions and services:

certSIGN SA
Address: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania
Phone: 004-021-31.19.901
Web: www.certsign.ro

b) The information security management and quality management of the service is carried out within the security concept of the service.

7.3 Trusted personnel

certSIGN ensures that the person performing the job responsibilities, in accordance with the role assigned within the Time Stamping Authority:

- Is a high school graduate (at least),
- Signed a contract that describes his role and responsibilities within the system,
- Followed a training program in accordance with his/her obligations and the tasks associated to his/her job, or provided credentials for expert knowledge, experience and qualifications,
- Was trained on the protection of personal data and confidential or private information,
- Signed a contract containing clauses related to the protection of sensitive information (from certSIGN's security stand point) and of the confidential and private data of Subscribers,
- Does not fulfill tasks that could generate conflicts of interest

certSIGN's employed personnel that fulfills a trust role shell be appointed by the Policies and Procedures Management Body.
In certSIGN, the following trust roles are defined, which can be assigned to one or more people:

- **Security administrator** – Global responsibility for implementing security policies and procedures.
  - Initiates the installation, configuration and management of certSIGN's software and hardware applications (including network resources); initiates and suspends the services provided by certSIGN; coordinates the administrators, initiates and oversees the key generation and the generation of shared secrets; approves rights in terms of security and user access privileges; checks the event logs; supervises internal and external audits; receives and responds to audit reports; supervises the elimination of deficiencies found after the audit.

  - Supervises the operators;
  - Checks the compliance with the Time Stamping Policy and with the Practices and Procedures Statement;
- **System administrator** – Authorized to install, configure and manage the systems and applications of the Time Stamping Authority.
- **System operator** – Responsible with the daily operation of the TSA's systems and applications. Authorized to execute back-up and system restart operations; transfers the back-up copies of the archive and of the current data outside certSIGN's location.
- **HSM Administrator** – Manages the security module and creates operator cards.
- **HSM Operator** – Turns the time stamping application on.
- **Electronic register administrator** – makes sure that all records are made and stored in accordance with the Time Stamping Policy.
- **System auditor** – authorized to access the archives and audit logs of the Certification Authority's trust systems. Responsible with conducting internal audits for compliance with the Certification Authority's Practices and Procedures Statement; this responsibility extends to the Registration Authority operating within certSIGN.

The number of people required to perform a task

The key generation process – for time stamp signing – is one of the operations that require special attention. It requires the presence of at least two people: a security administrator and a system administrator. The shared secret holders – who keep their part of the key in a safe location - also participate in the process of generating a TSU's key.

The presence of the security administrator and of an appropriate number of shared secret holders is also required when loading the cryptographic key in the hardware security module.

Activating the private key requires the quorum according to the threshold scheme; this means that the presence of the shared secret holders is also required every time the service is restarted.

Any other operation or role, described in this Practice Statement can be performed by a single person, specifically designated for this purpose.

Identification and authentication for each role

certSIGN's personnel is subject to identification and authentication whenever the camera or a computer system equipped with access control systems is accessed. Identification and authentication are done by one of the following methods, or a combination of them:

- Name and password
- Electronic stored private key and PIN
- Hardware private key stored (on a cryptographic device) and PIN
- Access card with picture

Each account assigned:

- It must be unique and directly assigned to a specific person,
- Cannot be shared with any other person,
- It is restricted in conformity with the position (which stems from the role performed by the person concerned), based software certSIGN system, operating system and application controls.

Each cryptographic device or user access card is handed out by the security administrator on the basis of a statement.

Staff training requirements

Staff performing roles and tasks as a result of assuming a role in the Timestamp Authority must be trained on:

- Regulations of the Code of Practice Statement,
- Time stamping policies,
- Security measures in place,
- Software applications of the Time Stamping Authority,
- Yearly updates on new threats and current security practices,
- Responsibilities arising from roles and tasks performed in the system.

Penalties for unauthorized actions

In case of discovery or suspicion of unauthorized access, the security administrator will investigate the incident and may suspend a person's access to the certSIGN system. Disciplinary measures for such incidents are described in the appropriate policies and procedures and comply with the law.

Personnel employed on contract

Personnel employed on contract (external services, developers of subsystems or apps, etc.) obey the same security measures as the permanent staff. In addition, staff employed on contract, during their activity in the certSIGN location, must always be accompanied by an employee of certSIGN, except for those who have received notification from the security administrator and can access classified information internally or in accordance with the rules in force.

7.4 Asset management

All resources of the Time Stamping Authority (information, systems and applications) are regularly inventoried and classified in terms of security and importance for the business. Processes have been put in place by which the management of those resources (entry, exit, storage, transfer, and use) is strictly controlled through measures directly proportional to their importance and classification.

certSIGN uses a controlled change management process. Before being used in production by certSIGN, every application is installed so as to allow current version control and to prevent unauthorized installation of software or falsification of the existing ones. Development, testing and production are distinct areas and transfer of information and application from one area to another is controlled.
Similar rules apply when replacing hardware components, such as:

- Physical devices are provided in a way that allows monitoring and evaluating each device's route, to its place of installation,
- The delivery of a replacement physical device is similar to the delivery of the original device; the replacement is performed by qualified and trusted personnel.

7.5 Access control

Any access to a resource is done through a controlled process involving the participation of managers, system administrators and security administrator. The need to know principle and the separation of duties principle are respected. Periodically, the existing access rights are checked to determine whether they are appropriate.

Different security layers in relation to physical and logical access ensure a secure operation of the time- stamping service. For instance:

- Secured physical environment
- Segregation of network segments
- Segregation of duties
- Firewalls
- Network and Service Monitoring
- Hardening of IT Systems

In case a person, which carries out operations for the time-stamping services, changes the role or leaves the organization, all the security tokens from that person are withdrawn.

Relationships with third parties

The process primarily relates to relationships with services providers and its control involves ensuring the security of the information accessed by these services providers.

Capacity management

The process by which certSIGN constantly monitors the load of the systems providing the trust services, to ensure the quality and the performance undertaken through policies and contracts.

Monitoring

The technological systems, services and personnel are constantly monitored to ensure the quality and safety of the services please customers and ensure compliance with the laws, rules and their own standards.

Physical security

Access to certSIGN's premises is controlled both through an access control system with proximity cards and, permanently, through security agents. The same system with access cards controls the access to the rooms with resources that are considered critical. Intrusion detection systems along with a closed-circuit video surveillance system are also installed.

7.6 Cryptographic controls

In certSIGN, the Timestamping service implementation complies with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA for use of suitable cryptographic techniques when providing qualified timestamping services.

7.6.1 TSU's key generation

The TSU key pair is generated by dual control, in certSIGN's location, in the presence of a group of trustees (according to the matrix of roles for the certSIGN TSA) in a FIPS 140-3 level 3, or ISO 15408 Common Criteria EAL 4+ compliant hardware security module (HSM). The private key is permanently kept in encrypted format on this device and never leaves the device in unencrypted format.

Actions taken when the key pair is generated are recorded, dated and signed by each person present during the key pair generation. Records are kept for audit reasons or for regular system checks.

The key is generated and exists throughout its entire lifetime in a physically and electromagnetically protected electronic environment.

After the key pair for time-stamp signing is generated and the private key is activated in the hardware security module, it can be used in cryptographic operations, according to #4.4, until its validity period expires or until it is compromised.

The TSU uses a RSA key pair with a length of 4096[2]-bit. This key pair is used only for signing TSTs.

7.6.2 TSU's private key protection

The hardware security modules used by Certification Authorities comply with the FIPS 140-3 level 3, or ISO 15408 Common Criteria EAL 4+ standards. The digital signature is created using the RSA algorithm in combination with the SHA512, SHA384 or SHA256 cryptographic summary.

The dual-control access is achieved through the distribution of shared secrets to licensed operators. The secrets are stored on cryptographic cards or tokens, protected by a PIN and transferred to their respective authenticated owners. For operations such as initiating the hardware cryptographic module and transferring the private key, an access threshold scheme (type k of n) is implemented through shared secrets distribution.

The shared secret transfer procedure involves the presence of the secret holder throughout the key generation process and during its distribution process, accepting the given secret and the responsibilities arising from keeping it.

Before receiving their part of the secret, each holder of the shared secret must be present, in person, when the secret is shared, to verify the correctness of the created secret and its distribution. Each part of the shared secret must be transferred to the holder on a cryptographic card protected by a PIN chosen and known solely by the holder.

The creation and the receiving of the shared secret are confirmed by a handwritten signature on a form, a copy of which is preserved in the archives of the Certification Authority and by the secret holder.

The shared secret holders must protect their part against disclosure. The holder avows that:

- He/she will not disclose, copy or share the secret with anyone and will not use his/her part of the secret in an unauthorized manner,
- He/she will not disclose (directly or indirectly) that he/she is the holder of the secret

The shared secret holder must responsibly fulfill the duties and obligations as required by this Practices and Procedures Statement in every possible situation. A shared secret holder must notify the secret's issuer in case of theft, loss, unauthorized disclosure or if the security of the secret was compromised, immediately after the incident. A shared secret holder is not responsible for failure to fulfill the duties / obligations due to reasons that are impossible to control by himself/herself, but is responsible for inopportune disclosure of the secret or for neglecting the obligations to notify the secret issuer about the inopportune disclosure or the breach of the secret's security as a result of the holder's mistakes, negligence or irresponsibility.

certSIGN TSA creates a backup copy of the private keys used for time-stamp signing. The copies are used during the implementation of the emergency key recovery procedures (e.g. in case of disaster). The copies of the private keys are protected by the shared secret created during the generation of the original keys.

[2] *Current active TSU has a key length of 2048 bits. Next TSU, from Q4 2026, will be with 4096 bits.*

The operation of introducing a private key in a cryptographic module applies in the following cases:

- Occasionally, when creating backups of the private key stored in a cryptographic module (e.g. in case of module failure or if the module is compromised) the introduction of a key pair into a different security module may be required,
- When the transfer of a private key from the operational module used for the entity's standard operations to another module is required; the situation may occur when invoking the Disaster Recovery plan or if the operational mode needs to be destroyed.

The introduction of a private key in a security module is a critical operation; therefore, to prevent disclosure, alteration or falsification of the private key, a set of measures and procedures should be implemented.

The introduction of a private key in the TSU's hardware security module of the certSIGN TSA requires the restoration of the key from cards in the presence of an adequate number of shared secret holders that protect the module containing the private keys.

The method of activating the private key used for time-stamp signing refers to the activation of the key before every use.

During import, generation or restoration, the private key of a TSU is deactivated. The key activates when the service is turned on.

Once activated, a key can be used as long as the service is running. When the service shuts down, the key deactivates.

The activation of private keys is always preceded by operator authentication. The authentication is performed based on a cryptographic card held by the operator. After inserting the card into the cryptographic module and using a PIN code, the private key remains active, until the card is removed from the module.

The method of deactivating the private key refers to the deactivation of the key after it was used or at the end of a session during which the key was used.

For the TSU private key, its deactivation is done when the service stops for any operation.

The hardware protection of the private key means that it is never available in clear, not even in the memory of the application.

In certSIGN's case, the deactivation of a private key is performed by people with trusted roles, but only in cases when the service is stopped for updates, maintenance or for other reasons.

7.6.3 TSU Public key certificate

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

a) TSU signature verification (public keys) are available to relying parties that trust in a public key certificate. The certificates are published in the following link: https://www.certsign.ro/en/resources/chain-of-trust-g2/
b) The TSU does not issue a time-stamp before its signature verification (public key). When the certificate is loaded in the TSU, the TSA verifies that the certificate was duly signed (including verification of the certificate chain of a trusted certification authority).
c) Only one TSU certificate with its private key is issued.
d) TSU certificates are not renewed.

e) Validity information regarding the TSU certificates is updated periodically and the CRLs or OCSP services are available with the references located in the certificates.

The time-stamps issued by certSIGN TSA are qualified electronic time-stamps as per Regulation (EU) No 910/2014 and the TSU signature verification (public) key certificate is issued by certSIGN Qualified 2023 RSA CA, under ETSI EN 319 411-2 certificate policy. The time-stamp certificate contains one instance of the qcStatements extension in the certificate extension field with the syntax as defined in IETF RFC 3739, clause 3.2.6.

7.6.4 TSU's key renewal

The life-time of the TSU certificate corresponds to the period of the chosen algorithm and to the key length.

The keys of the TSU shall have a maximum operating life of 3 years. A certificate can be issued for all expected lifetime. The duration of the TSU class is limited by:

- The period of validity of the root issuer entity certificate.
- Once a year or when significant changes occur, the person holding the function "Cryptography Supervisor" verifies all cryptographic algorithms used in the TSA checking that each algorithm is recognized as suitable
- If an algorithm enters a situation of risk, it shall no longer be considered as adequate; the Security Manager shall train the TSA on the cease of usage of the affected keys and on the loading of new keys.

7.6.5 Life cycle management of cryptographic hardware

certSIGN TSA assures that:

a) The integrity of the cryptographic security modules was not affected during its transport from the manufacturer.
b) The integrity of the cryptographic security modules was not affected during their storage, prior to their installation
c) They are installed, managed and operated by trusted personnel.
d) The cryptographic security modules work correctly
e) The private signing keys stored on the cryptographic security modules are destroyed the moment it is taken out of production.

The inspection is protocolled.

Additionally, the following applies:

a) The Installation and activation of TSU's signing keys in cryptographic hardware is done only by personnel in trusted roles using, at least, dual control in a physically secured environment.
b) The TSU private signing keys stored in a TSU cryptographic module is erased upon retiring the device in a manner that is practically impossible to recover them.

7.6.6 End of TSU's key life cycle

After private keys expiration, the private keys within the cryptographic module are destroyed in a way that they can no longer be retrieved.

7.7 Time-stamping

7.7.1 Time-stamp issuer

certSIGN TSA offers time-stamping services using RFC 3161 "Time Stamp Protocol (TSP)". The service URL is specified in the subscriber's agreement. Each TST contains the Time-Stamping

Policy identifier, a unique serial number and a certificate containing the identification information of the certSIGN TSA`s TSU.
The TSU, in the time-stamp requests, accepts SHA512, SHA384 or SHA256 hash algorithms and uses the SHA512, SHA384 or SHA256 cryptographic hash function to sign the TST.
The TSU keys are 4096-bit[3] RSA keys. The key is used only for signing TSTs.
TSA logs all issued TSTs. The TSTs are logged for an indefinite period. certSIGN TSA can prove the existence of a TST at the request of a relying party. certSIGN TSA can request the relying party to cover the costs of such service.
The TSU does not issue any TST when the end of the validity of the TSU private key has been reached.

7.7.2 Clock synchronization with UTC

certSIGN ensures that its clock is synchronized with UTC within an accuracy of 1 second or better, using the NTP protocol.
certSIGN monitors its clock synchronization and ensures that, if the time indicated in a TST drifts or jumps out of synchronization with the UTC, this is detected. In case the TSA clock drifts out of accuracy, no time-stamp shall be issued until the clock is synchronized.
Specifically, the following topics are covered:

- Continuous calibration of the TSU clock
- Monitoring of the accuracy of the TSU clock
- Thread analysis against attacks on time-signals
- Behavior while skipping/adding leap seconds
- Behavior while drifting larger that 1s from the UTC

7.8 Physical and environmental security

Computer systems, terminals and information resources of certSIGN operators are placed in a dedicated area, physically protected against unauthorized access, destruction or disruption of activity. These locations are monitored. Each input and output is recorded in the event log (system logs); the stability of the power sources and temperature are also monitored and controlled.

Physical access

Physical access within certSIGN is controlled and monitored by an integrated alarm system. certSIGN's has fire prevention systems, intrusion detection systems and power supply systems in case of emergency.

certSIGN work schedule is from Monday to Friday between 9.00 and 18.00. Outside this time interval, including public holidays, access to certSIGN premises is allowed only to persons authorized by the Management of certSIGN.
Areas belonging to certSIGN are divided into:

- Office areas,
- IT areas,
- CA operators' area
- RA operators and administrators' area,
- Developing and testing area.

IT areas are equipped with monitored security system built on the basis of motion, intrusion and fire. Access to this area is granted only to authorized personnel. Monitoring of access rights is carried out based on electronic cards and appropriate readers, mounted next to the entry area. Every entry to and exit from the area is automatically recorded in the event log.

[3] *Current active TSU has a key length of 2048 bits. Next TSU, from Q4 2026, will be with 4096 bits.*

Access to the *operators' area* is allowed only based on an electronic card and its appropriate reader. Since all sensitive information is protected by the use of locked cabinets, while access to operator's or administrator's terminal requires prior authorization, the implemented physical security is considered adequate. Keys to the area are accessible only to authorized personnel. The area may be occupied solely by certSIGN personnel and authorized individuals, the latter being granted access only if accompanied.

Unattended individuals are not allowed in this area. Programmers and developers do not have access to sensible information. If such access is necessary, the presence of the security administrator is required. Projects being implemented and their software are tested on the development environment of certSIGN.

Mains electricity and air conditioning

Operators and administrator's area and the area of development and testing have air conditioning. From the power cut, emergency power sources (UPS) allow to pursue work undisturbed until the automatic involvement of the generator.

Water exposure

The risk of flooding of the servers is low because the distance from water pipes is high. In addition, flood sensors are installed in the data rooms and monitored 24*7 by the security personnel located just off the server who is instructed to immediately announce certSIGN administrator and administrator of the building in case of an incident.

Fire protection

certSIGN's location has a prevention system and fire protection in accordance with standards and regulations;

Storage of information storage devices

Depending on the sensitivity of information, electronic media containing archives and current data backups are stored in metal safes located in a high security room. Access to the room and safety deposit boxes is restricted to authorized personnel.

Waste Disposal

Paper and electronic media containing important information in terms of certSIGN security are destroyed after the retention period. Hardware security modules are reset and erased according to the manufacturer.

These devices are also reset and erased when sent to service or repair.

Backup storage outside the location

Cryptographic cards needed for disaster recovery services are stored in special containers located outside certSIGN location.

Offsite storage also applies to archives, current copies of information processed by the system and certSIGN application installation kits. This allows the emergency restoration of any function of certSIGN within the deadlines set by the insurance plan for business continuity.

7.9 Security of operations

The technical requirements presented in this chapter refer to the security controls specific to computers and applications, used within certSIGN. Security measures were taken at all levels, starting at the physical level and all the way through the application level.

The controls that belong to the certSIGN TSA have the following security measures:

- Mandatory authentication at the operating system level and applications
- Discretionary access control,
- Possibility of being audited in terms of security,
- The computer is accessible only to authorized personnel with trusted roles in certSIGN,
- Segregation of duties, according to their role within the system,
- Identification and authentication of roles and personnel performing these roles,
- Preventing reuse of an object by another process after it is issued by the authorized,
- Cryptographic protection of exchanges of information and protection of databases,
- Log archiving operations performed on a computer and data necessary audit,
- A secure path that allows the identification and authentication of roles and personnel performing these roles,
- Key restoration methods (only in the case of hardware security modules), the application and the operating system,
- Means monitoring and alerting in case of unauthorized access to computing resources.
- The integrity of TSA systems and information shall be protected against viruses, malicious and unauthorized software.
- Media used within the TSA systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.
- Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

certSIGN uses trustworthy systems and products that are protected against modification and ensures the technical security and reliability of the processes supported by them.
An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by certSIGN or on behalf certSIGN to ensure that security is built into IT systems.
Every application, prior to be used for production within certSIGN, is installed so as to allow control of the current version and to prevent unauthorized installation of programs or the forgery of the already existent once.
Similar rules apply to hardware components replacement, such as:

- Hardware is supplied in a manner allowing its tracing and evaluation of the route of the component to the place of its installation,
- Replacement hardware delivery is carried out in a manner similar to delivery of original hardware; the replacement is carried out by trusted and trained personnel.

The purpose of security management control is to supervise certSIGN systems' functionality providing assurance that the system operates correctly and in accordance with the accepted and implemented configuration.
Controls applied to certSIGN system allow continuous verification of application integrity, their version and authentication and verification of hardware origin.
Change control policies and procedures are applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies certSIGN's security policy.

Current configuration of certSIGN system, any changes to them as well as any to releases, modifications and emergency software fixes of any operational software are documented.
Configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies
certSIGN implement internal security procedures for ensuring that:

- Security patches are applied within a reasonable time after they come available;
- Security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh
- The benefits of applying them;
- The reasons for not applying any security patches are documented

certSIGN implements an internal capacity management procedure which ensures that for the ICT infrastructure for the TSA services the capacity demands is monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are available.

7.10 Network security

certSIGN protects its network and systems against attack. For that purpose and based on risk assessments and best practices we implement an integrated set of security controls:

a) Our systems are segmented into networks or zones based considering functional, logical, and physical (including location) relationship between trustworthy systems and services. certSIGN applies the same security controls to all systems co-located in the same zone.

b) Access and communications between zones are restricted to those necessary for the operation of certification services. Not needed connections and services are explicitly forbidden or deactivated. The established rule set is reviewed on a regular basis.

c) All systems that are critical to the certification services operation are kept in one or more secured zone(s)

d) Dedicated network for administration of IT systems and operational network are separated. Systems used for administration of the security policy implementation are not used for other purposes. The production systems for the certification services are separated from systems used in development and testing (e.g. development, test and staging systems).

e) Communication between distinct trustworthy systems are only established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

f) If a high level of availability of external access to a specific certification service is required, the external network connection is redundant to ensure availability of the services in case of a single failure.

g) A regular vulnerability scan on public and private IP addresses identified by certSIGN is performed quarterly and evidence is recorded that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

h) certSIGN certification services undergo an yearly penetration test on the related systems at set up and after infrastructure or application upgrades or modifications that certSIGN determines are significant. Evidence is recorded that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

Servers and trusted workstations of certSIGN system are connected through a local network

(LAN), devised in more sub-networks provided with controlled access. Access from the Internet to any segment is protected by means of intelligent firewall.

Security controls are developed on the basis of firewall and traffic filtering on the routers and Proxy services that protect certSIGN's internal network domains from unauthorized access including access by Subjects/ Subscribers and third parties. Firewalls are configured to prevent all protocols and accesses not required for the operation of certSIGN TSA.

Means of protection of the network security accept only messages submitted with the usage of http, https, NTP, POP3 and SMTP protocols. Events (logs) are recorded in the system journals and allow supervision of correctness of the usage of services provided by certSIGN. The time-stamping client and the time-stamping server support the time-stamping protocol via HTTPS as defined in clause 3.4 of IETF RFC 3161.

certSIGN maintains and protect all TSA systems in at least a secure zone and has in place a security procedure that protects systems and communications between systems inside secure zones and high security zones.

certSIGN configures all TSA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the TSA's operations.

certSIGN grants access to secure zones and high security zones only to trusted roles.

7.11 Incident management

System activities concerning access to IT systems, its user systems, and service requests are monitored. Especially:

a) Monitoring activities take into account the sensitivity of any information collected or analyzed.

b) Abnormal system activities that indicate a potential security violation, including intrusion into the TSP network, are detected and reported as alarms.

c) The TSP IT systems monitor the following events: Start-up and shutdown of the logging functions; availability and utilization of the needed services with the TSP network.

d) The TSP acts in a timely and coordinated manner to respond quickly to incidents and to limit the impact of security breaches. The TSP appoints trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.

e) The TSP notifies the corresponding parties, in line with the applicable regulatory rules of any security breach or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

f) The national supervisory body is informed within 24h after the discovery of a critical security breach.

g) Audit logs are monitored or reviewed regularly to identify evidence of malicious activity.

h) The TSP shall resolve critical vulnerabilities within a reasonable period after their discovery. If this is not possible the TSP will create and implement a plan to mitigate the critical vulnerability or the TSP will document the factual basis for the TSP's determination that the vulnerability does not require remediation.

i) Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimized.

7.12 Collection of evidence

The TSP records are kept accessible for an appropriate period, including after the activities of the TSP have ceased. All the relevant information concerning data issued and received by the TSP are guarded to provide evidence in legal proceedings and to ensure continuity of the service.

Especially:

a) The confidentiality and integrity of current and archived records concerning operation of services is maintained.

b) Records concerning the management of services are confidential and filed in accordance with described business practices.

c) Records concerning the management of services, if necessary, are made available for the purposes of providing evidence of the correct operation of the services for legal proceedings.

d) The TSP registers in the precise moment, the significant environmental events, key management and clock synchronization. The time used to record events, as required in the audit log, is synchronized with the UTC continuously.

e) Records concerning services are held for a period after the expiration of the validity of the signing keys or of any service token to provide trust for the necessary legal evidence in accordance to the present document.

f) The events are logged in a way that they cannot be deleted or destroyed (except if they can be reliably transferred to long-term media).

7.13 Business continuity management

Backups of the databases of all issued TSTs by certSIGN TSA are kept in an off-site storage. If the TSU private key is compromised or suspected to be compromised, certSIGN TSA shall inform Subscribers and Relying Parties and shall stop using the compromised key.

In case of TSU certificate revocation, the necessary actions shall be performed in accordance with the Recovery Plan.

In case of clock synchronization loss, certSIGN TSA suspends its operations to prevent further damage. The Recovery Plan is activated to restore the synchronization and the service.

The time-stamping service itself is in a physical secured environment that minimizes the risk of natural disasters (e.g. fire).

The private keys of the TSU are stored in a cryptographic security module.

In case private keys become compromised, the archive of saved time-stamps helps differentiate between correct and false time-stamps in an audit trail.

The HSM is isolated from the public network and, if necessary, the following measures shall be taken:

- Notify the Security Manager for him to coordinate the measures to be taken.
- Start a security audit of the remaining private keys (integrity checks, log file analysis).
- Notify the incident to relying parties.
- In case of natural disasters (e.g. fire, earthquake, storm), if it causes the loss of the facility, the time-stamping service could become suspended until the disaster recovery facility is activated.

7.14 TSA termination and termination plans

- In the event the TSA terminates its operations for any reason whatsoever, it shall notify the national supervisory entity prior to termination.
- A timely notice shall be provided to all relying parties to minimize any disruptions that are caused because of the termination of the services.
- Furthermore, in collaboration with the supervisory entity, the TSP shall coordinate the necessary measures that ensure retention of all the relevant archived records prior to the service termination.
- Moreover, the following applies:
    a) The TSP maintains an up-to-date termination plan.
    b) Before the TSP terminates its services, at least the following procedures apply:
        i. the TSP shall inform the following of the termination: all subscribers

and other entities with whom the TSP has agreements or other form of established relations. This information shall be made available to other relying parties;

ii. TSP shall terminate the authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens;

iii. The TSP shall transfer to a reliable entity, for a reasonable time, its obligations of maintaining all necessary information to provide evidence of the operations of the TSP, unless it can be demonstrated that the TSP is not the owner of such information;

iv. The TSP private keys, including backup copies, shall be destroyed, or withdrawn from use, in a way that the private keys can no longer be retrieved.

v. certSIGN TSA takes the necessary steps to have the TSU certificates revoked.

vi. When possible, the TSP shall use a system that allows the transfer of the services provided to its client to another TSP.

c) The TSP has an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons by which the TSP is unable to cover the costs by itself, to the possible extent, within the constraints of the applicable legislation regarding bankruptcy.

d) The TSP shall maintain or transfer to a reliable entity its obligations of making its public key or trust service tokens available to relying parties for a reasonable period.

7.15 Compliance

certSIGN TSA ensures compliance with applicable law at all times. Specifically, it is compliant to:

a) Regulation (EU) 910/2014, with the modifications from Regulation (EU) 1183/2024
b) Romanian Law no.214/2024
b) ETSI TS 319 421
c) IETF (RFC 3161)

Validation of the compliance with these regulations is performed during the conformity assessment.