Trans Sped

TSP

Your Trusted Service Provider

Certification Practice Statement and TimeStamp Policy

Version 2.1

Date of effect: August 2021

Certification Practice Statement and TimeStamp Policy

Version 2.1

General information	
Version	*2.1*
Security classification	*Public*
Approved by	*Camelia Ivan*
Date of approval	*August 2021*
Date of effect	*August 2021*

Change history			
Version	**Description**	**Effect date**	**Author(s)**
1.0	Initial version	January 2017	Mario STOICA
2.0	Internal review	February 2020	Camelia IVAN
2.1	Content reviewed and updated according to ETSI standards	August 2021	Camelia IVAN

CUPRINS

1. INTRODUCTION 5
2. PURPOSE 5
3. REFERENCE 6
4. DEFINITIONS AND ABBREVIATIONS 7
4.1. Definitions 7
4.2. Abbreviations 7
5. GENERAL CONCEPTS 9
5.1. Timestamping services 9
5.2. TimeStamp Authority 9
5.3. Subscriber 9
5.4. Certification Practice Statement and TimeStamp Policy 9
6. TIMESTAMP POLICY 11
6.1. Overview 11
6.2. Policy Identification 11
6.3. Policy Applicability 11
6.4. Compliance 11
7. OBLIGATIONS AND RESPONSIBILITIES 12
7.1. TSA Obligations 12
7.2. Subscribers Obligations 12
7.3. Third Party Obligations 12
7.4. Responsibilities 13
7.5. Publication and notification of policies 13
7.6. Certification Practice Statement Approval 13
8. REQUIREMENTS FOR TSA PRACTICES 14
8.1. Statement 14
8.2. Cryptographic Key Lifecycle Management 15
8.3. TimeStamping 16
8.4. TSA management and operation 17
8.4.2. Classification and management of goods 18
8.4.7. Installation and maintenance of trust systems 20
8.4.8. Compromise of TSA services 20

8.4.9. Termination of TSA activity 20
8.4.10. Compliance with legal requirements 20
8.4.11. Logging operations regarding the operation of the timestamping service 21
8.4.12. Network access 21
8.4.13. Incident management 22
8.4.14. Business continuity management 22
8.5. Organizational measures 22

1. INTRODUCTION

This document describes the practices, procedures and policies related to the timestamping service provided by Trans Sped S.A. Trans Sped S.A. with the headquarter in 38 Despot Vodă Street, 020656, Bucharest, Romania (hereinafter referred to as "Trans Sped") is a Qualified Trust Service Provider that issues qualified digital certificates that can be used to create electronic signatures or electronic seals with legal value, according to the eIDAS Regulation (910/ 2014).

Trans Sped offers the time-stamping service as part of its trust services, in accordance with Law no. 451/2004 and the eIDAS regulation. The purpose of timestamps is to determine exactly when an electronic document was created or signed. Timestamps enable the implementation of advanced signature schemes required in the context of large-scale development of electronic services.

To provide the time stamping service, Trans Sped has implemented a Time Stamping Authority - Trans Sped TSA.

This document contains the timestamping policy that describes the general rules that are followed by Trans Sped TSA and the code of practices and procedures that describes the processes and procedures by which these rules are implemented.

The structure and content of this document are in accordance with the standard EN 319 421 v1.1.1 (2016-3) Electronic signatures and infrastructures (ESI); Policy and security requirements for trusted service providers that issue timestamps.

This document is publicly available on the Trans Sped website:

www.transspoed.ro/repository.

2. PURPOSE

This document specifies the requirements for the operation of Trans Sped TSA and defines the operating and management practices of Trans Sped TSA so that users and third parties can trust the services provided by Trans Sped TSA. The implemented solution complies with the requirements of the eIDAS regulation, Law no. 451/2004 regarding the time stamp and MCSI Order no. 492/2009 regarding the technical and methodological rules for the application of Law no. 451/2004 regarding the time stamp. The solution is based on the use of public key cryptography, digital certificates, cryptographic hash functions and a trusted time source. This document, together with Trans Speed’s internal organization, processes, and procedures, may be used by an independent body to assess the reliability of the timestamping services provided by Trans Sped.

3. REFERENCE

[LEGE-ES]	Law no. 455/2001 on electronic signatures
[LEGE-TS]	Law no. 451/2004 regarding the time stamp
[ORDIN-TS]	MCSI order no. 492/2009 regarding the technical and methodological norms for application of Law no. 451/2004 regarding the time stamp
[EU-REG]	REGULATION (EU) NO. 910/2014 OF THE PARLIAMENT EUROPEAN AND OF THE COUNCIL of 23 July 2014
[ORDIN-eIDAS]	Order no. 449/2017 regarding the procedure for granting, suspending and withdrawing the status of Qualified Trust Service Provider in accordance with Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014
[ETSI1]	EN 319 401 v2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI2]	EN 319 421 v1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps
[RFC3161]	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
[FIPS]	FIPS PUB 140-2: Security Requirements for Cryptographic Modules

4. DEFINITIONS AND ABBREVIATIONS

4.1. Definitions

Subscriber: a legal person with several users or a natural person, an individual user who uses the time-stamping services of Trans Sped TSA and who explicitly or implicitly agreed to the terms and conditions of Trans Sped.

Third Party: An entity that trusts the timestamps issued by Trans Sped TSA.

Timestamp: object that certifies the fact that certain data was presented at a certain point in time to the timestamp service provider.

NTP (Network Time Protocol): network protocol for synchronizing the clock of a variable-latency networked computer system.

Public cryptographic key: From the pair of keys used in asymmetric algorithms, the public cryptographic key is the one made available to the public, e.g., on a public cryptographic key server. Its purpose is to encrypt messages sent to the key holder and to verify the digital signatures that the latter has made using the corresponding private key. A public cryptographic key certified by a Certification Authority is called a certificate.

Time Stamp Authority (TSA): trusted third party that issues time stamps.

Time Stamp Unit (TSU): hardware or software used to generate time stamps.
Coordinated Universal Time (UTC): Time scale based on seconds, defined by Recommendation ITU-R TF.460-5. UTC is equivalent to solar time at the prime meridian (00).

4.2. Abbreviations

ETSI European Telecommunications Standards Institute

FIPS Federal Information Processing Standards

HTTP Hypertext Transfer Protocol NTP Network Time Protocol

OID Object Identifier

RFC Request for Comments

RSA Rivest Shamir Adleman Algorithm SHA Secure Hash Algorithm

TSA Time Stamping Authority

TSPS Time Stamping Practice Statement

TSU Time Stamping Unit

HSM Hardware Security Module

UTC Coordinated Universal Time

5. GENERAL CONCEPTS

5.1. Timestamping services

This document complies with the standard ETSI EN 319 401, ETSI 319 421 V1.1.1 (2016 0 -3), ETSI 319 422 V1.1.1 (2016 0 -3) regarding the requirements to be met by trust service providers.
Timestamping services consist of:

- Provisioning Timestamps: The component that deals with the generation of timestamps.
- Timestamp management: The component that monitors and controls the operation mode of timestamp services. For example, this component ensures that the clock used in the timestamping process is correctly synchronized to UTC.

This breakdown of timestamping services is only intended to clarify the requirements specified in this document and does not impose any restrictions on how timestamping services are implemented.

5.2. TimeStamp Authority

The authority trusted by users (subscribers or third parties) to issue timestamps is called the Timestamp Authority (TSA). TSA bears full responsibility for the provision of the timestamping services identified in chapter 5.1.
A Time Stamping Authority (TSA) may have one or more Time Stamping Units (TSUs) that generate and sign timestamps on behalf of the TSA. Each TSU must be uniquely identifiable and must have its own signing key.
A temporary stamping authority (TSA) is a certification service provider within the meaning of Regulation (EU) NO. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.
Trans Sped confirms that the Time Stamping Authority (TSA) is audited at least once every 24 months by a verification body and the audit report is brought to the attention of the national supervisory body within 3 working days.

5.3. Subscriber

The subscriber can be a legal entity with several users or a natural person, individual user.
When the subscriber is a legal entity, some of the obligations that apply to that legal entity will also apply to its own users. In any case, that legal entity is responsible if its own users do not fulfill their obligations correctly. That legal entity is expected to inform its users accordingly.
If the subscriber is a natural person, he is directly responsible if his obligations are not fulfilled correctly.

5.4. Certification Practice Statement and TimeStamp Policy

This chapter explains the role of the Time Stamp Policy and Code of Practices and Procedures for a TSA. TSA's Timestamping Policy and Code of Practice and Procedures comply with the requirements specified in ETSI EN 319 401 applicable to trust service providers.

5.4.1. Role

The TSA Timestamp Policy states "what requirements must be met," while the TSA Code of Practices and Procedures states "how those requirements must be met." The relationship between

the Time Stamp Policy and TSA's Code of Practices and Procedures is like the relationship between a company's policy that states business requirements while operational units define the practices and procedures by which business requirements are to be met.
This document contains both the timestamping policy and the Trans Sped TSA code of practices and procedures:
The Trans Sped TSA Time Stamp Policy describes the general requirements that time stamp services meet.
The Trans Sped TSA Code of Practice and Procedures describes how these requirements are met.

5.4.2. Level of detail

The Time Stamp Policy is a less detailed document than the TSA Code of Practices and Procedures. The Trans Sped TSA Code of Practice and Procedures describes in detail the terms and conditions and operational procedures used to generate and manage timestamps. The Trans Sped TSA Code of Practices and Procedures implements the general rules defined by the Trans Sped TSA Time Stamp Policy. The Trans Sped TSA Code of Practice and Procedures demonstrates how Trans Sped TSA meets the technical, organizational and procedural requirements defined by the Trans Sped TSA Time Stamp Policy.

5.4.3. Approach

The approach of the Timestamping Policy differs significantly from that of the Code of Practices and Procedures. The Timestamping Policy is defined independently of the specific details of TSA's mode of operation, while the Code of Practices and Procedures reflects TSA's organizational structure, operating procedures, facilities, and IT systems.

6. TIMESTAMP POLICY

6.1. Overview

This chapter defines the requirements that Trans Sped TSA undertakes to meet when generating timestamps. Trans Sped TSA issues time stamps in accordance with the requirements of the eIDAS Regulation, Law no. 451/2004 regarding the time stamp, MCSI Order no. 492/2009 regarding the technical and methodological rules for the application of Law no. 451/2004 on time stamping and standard specifications EN 319 421 v1.1.1 (2016-03) ETSI 319 421 V1.1.1 (2016 0 -3), ETSI 319 422 V1.1.1 (2016 0 -3).

6.2. Policy Identification

The Trans Sped TSA policy identifier is as follows: OID = 1.3.6.1.4.1.39965.1.2.1
The basic ETSI policy identifier followed is as follows: 0.4.0.2023.1.1
itu-t(0) organization-identifier(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1)
base-policy-ts (1)

The Trans Sped TSA Policy Identifier is included in each issued timestamp.

6.3. Policy Applicability

This document does not set any limitation on the applicability of timestamps issued in accordance with this policy. Trans Sped provides reliable, time-stamping services in accordance with current legislation.

6.4. Compliance

Trans Sped includes the Policy Identifier (OID) set out in Chapter 6.2 in all issued timestamps. To demonstrate compliance, Trans Sped undertakes to:

1. fulfill the obligations defined in chapter 7.1.
2. implement the control measures specified in chapter 8.

Compliance with the Timestamping Policy is periodically verified by independent, internal, or external audits.

7. OBLIGATIONS AND RESPONSIBILITIES

7.1. TSA Obligations

7.1.1. General obligations

Trans Sped undertakes to ensure compliance with the requirements established by the Time Stamping Policy and with the following regulations:

- European Regulation 910/2014 (eIDAS)
- Law no. 451/2004 regarding the time stamp.
- MCSI order no. 492/2009 regarding the technical and methodological norms for the application of Law no. 451/2004 regarding the time stamp.
- Specifications of the standard EN 319 421 v1.1.1 (2016-03).

Trans Sped undertakes to implement the control measures established by the Code of Practices and Procedures described in this document.

7.1.2. TSA's obligations to subscribers

Trans Sped provides permanent access to the timestamping service, except during maintenance periods, times when the time source is unavailable or in the event of force majeure events beyond Trans Sped's control (e.g., war, strike, legal restrictions, etc.). Maintenance periods must be agreed in advance with subscribers or announced in advance on the Trans Sped website.
In addition, Trans Sped undertakes to:

- implementing a reliable and trustworthy communications infrastructure and IT applications.
- providing the timestamping service in accordance with widely accepted industry standards.
- issue only correct timestamps and not allow backdating of documents.

The time source of the Trans Sped timestamping service uses the GPS signal together with a set of Network Time Protocol (NTP) servers as the time source. Using this configuration, the deviation is +/- 1 second or more accurate using UTC.

7.2. Subscribers Obligations

Subscribers must use Trans Sped TSA's timestamping service in accordance with the specifications in Chapter 4 (Requirements for a Timestamping Client) of the EN 319 422 v1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI) standard; Timestamping protocol and timestamping profiles.
Subscribers must verify that the timestamps have been signed correctly and that the TSU private key used to sign the timestamps has not been revoked. Trans Sped may include in the contracts concluded with each individual subscriber, additional requirements that they must comply with.
For more information, please consult the Terms and Conditions available at www.transsped.ro

7.3. Third Party Obligations

Third parties that trust timestamps issued by Trans Sped TSA must verify that the timestamps have been signed correctly and that the TSU private key used to sign the timestamps has not been revoked. When verifying a timestamp after the TSU certificate expires, third parties must ensure that the hash function, cryptographic algorithms, and key lengths used can still be considered secure.
For more information, please consult the Terms and Conditions available at www.transsped.ro

7.4. Responsibilities

Trans Sped is liable for the proven damage caused to any person who bases his conduct on the legal effects of the time stamps issued, in accordance with the legal provisions in force. Trans Sped is not liable in cases where it proves that, although it performed the necessary diligence, it could not prevent the damage from occurring. Also, Trans Sped is not responsible for damages caused by force majeure and/or fortuitous events. Trans Sped is not responsible for damages caused to subscribers or third parties caused by negligence or failure to comply with the obligations presented in chapters 7.2 and 7.3.

7.5. Publication and notification of policies

Whenever the Code of Practices and Procedures is amended and the amended version is approved by Trans Sped management, it will be published in the repository available on the website.

7.6. Certification Practice Statement Approval

The Code of Practices and Procedures is reviewed and approved by Trans Sped management prior to publication in the repository.

8. REQUIREMENTS FOR TSA PRACTICES

Trans Sped undertakes to implement control measures in accordance with the requirements outlined below. Requirements are described in the form of security objectives.

8.1. Statement

8.1.1. Statement of TSA Practices

Trans Sped TSA is committed to demonstrating the necessary reliability in providing timestamping services. In this case:

a) Trans Sped TSA has performed a risk analysis to assess the resources and the threats they are exposed to determine the necessary security measures.

b) Trans Sped TSA has a set of practices and procedures used to implement the requirements identified by this policy.

c) Established practices and procedures include the obligations of all entities that provide support for timestamping services.

d) Trans Sped TSA makes available to subscribers and third parties, practices, and procedures, as well as other relevant documents, so that they can assess compliance with the Time Stamp Policy.

e) Trans Sped TSA informs subscribers and third parties about the terms and conditions regarding the use of time-stamping services.

f) Trans Sped TSA has a procedure for approving practices and procedures by the company's management.

g) Company management ensures that practices and procedures are implemented correctly.

h) Trans Sped TSA has established a process to review and update practices and procedures.

8.1.2. Disclosure statement

Trans Sped TSA informs all subscribers and third parties of the terms and conditions regarding the use of timestamping services. Specifically, users are informed about:

a) TSA contact details.
b) The applied Temporal Stamping Policy.
c) The hash algorithms accepted for the calculation of the summary of the data on which the time stamp is to be applied.
d) The estimated lifetime of the signature used to sign the timestamps (which depends on the hash algorithm used, the signature algorithm used and the length of the private key).
e) Accuracy of time from time stamps in relation to UTC.
f) Any limitations on the use of the timestamping service.
g) Obligations of subscribers, in accordance with chapter 7.2.
h) Obligations of third parties, in accordance with chapter 7.3.
i) Information on how to verify time stamps.
j) The period for which TSA keeps the logs.
k) Applicable legislation.
l) Any limitation of liability.
m) The method of settling disputes.

n) If TSA was audited and by which body.

8.2. Cryptographic Key Lifecycle Management

8.2.1. TSU key generation

Trans Sped TSA is committed to ensuring that cryptographic keys are generated under strictly controlled conditions. In this case:

a) The generation of the TSU signing key is done in a secure physical environment, by reliable personnel, under double control.
b) The generation of the TSU signing key is done inside a cryptographic module (HSM – Hardware Security Module), certified FIPS 140-2 Level 3.
c) The key generation algorithm, the signing algorithm and the length of the signing keys comply with national and international recommendations in the field of cryptography.

8.2.2. TSU Private Key Protection

Trans Sped TSA is committed to ensuring the confidentiality and integrity of TSU private signing keys. In this case:

a) The private signing key of the TSU is kept and used by means of a cryptographic module (HSM – Hardware Security Module), certified FIPS 140-2 Level 3.
b) If the private signing key of the TSU is saved, then the copying, storage and restoration operations will be done by trusted personnel, under double control, in a secure physical environment.
c) Any backup copy of the TSU private signing key is protected for confidentiality by the cryptographic module before it is stored outside of this device.

8.2.3. TSU public key distribution

Trans Sped TSA undertakes to ensure the integrity and authenticity of TSU public signing keys during their distribution to third parties. In this case:

a) The public key for signing the TSU is made available to third parties in the form of a public key certificate.
b) The public key certificate for signing the TSU is issued by a trusted certification authority.

8.2.4. Changing the TSU key

TSU private signing keys have a lifetime depending on the strength of the algorithm used and the length of the keys. Expired private keys are not archived and are destroyed immediately upon expiration. TSU public key certificates are stored for 15 years to allow verification of previously issued timestamps.

8.2.5. Destruction of the TSU key

Trans Sped TSA undertakes to ensure that the TSU's private signing keys are no longer used after the lifetime period has expired. In this case:

a) operational and technical procedures have been established that allow the installation of a new key when the old one expires.
b) The private TSU signing key that has expired, including backup copies, is destroyed so that it cannot be restored.

c) The TSU does not allow the generation of new timestamps if its private signing key has expired.

8.2.6. Management of the cryptographic module used for signing timestamps

Trans Sped TSA is committed to ensuring the security of the cryptographic module throughout its life cycle, from the manufacturer to its removal from production. In this regard, Trans Sped TSA verifies that:

a) The cryptographic module was not opened during delivery.
b) The cryptographic module was not opened during storage.
c) Installation, activation, and duplication of the TSU signing keys within the cryptographic module is performed only by trusted personnel, under double control, in a secure physical environment.
d) The cryptographic module works correctly.
e) The private signing keys of the TSU stored on the cryptographic module are deleted after decommissioning.

8.3. TimeStamping

8.3.1. Timestamp

Trans Sped TSA is committed to ensuring that timestamps are issued securely and contain the correct time. In this case:

a) Timestamps issued include an identifier of the policy under which they are issued.
b) Each time stamp has a unique identification number.
c) Time source of the Trans Sped timestamping service uses the GPS signal together with a set of Network Time Protocol (NTP) servers as the time source. Using this configuration, the deviation is +/- 1 second or more accurate using UTC.
d) If the Trans Sped clock loses synchronization, then the TSU will no longer issue time stamps.
e) The timestamp includes the summary of the data (hash value) for which you want it to be timestamped.
f) The timestamp is signed using a key generated exclusively for this purpose.

8.3.2. Time accuracy

The time source of the Trans Sped timestamping service uses the GPS signal together with a set of Network Time Protocol (NTP) servers as the time source. Using this configuration, the deviation is +/- 1 second or more accurate using UTC.
Trans Sped TSA is committed to designing and implementing the necessary measures to detect changes in internal clock calibration and timing problems that may compromise the accuracy established by this policy.

8.3.3. Timestamp format

The timestamp provided by Trans Sped TSA is in accordance with RFC 3161. The service provides timestamps with RSA algorithm and a key length of 2048 which supports SHA 256 hash algorithm.

8.3.4. Service Limitations

In the context where the subscriber has a contractual relationship for the provision of timestamps with Trans Sped TSA, the timestamp service provided by Trans Sped TSA may be used for the purpose of any lawful transaction, without limitation, if there are no other specific conditions. specified at contract level.
Within the limits established by Romanian legislation, in no case (except for fraud or misconduct) Trans Sped will not be responsible for:

- Any financial loss.
- Any loss of data
- Any negative consequences directly or indirectly caused by the use, provision, licensing, execution or non-execution of certificates or electronic signatures.
- Any other negative consequences.

Trans Sped has no financial responsibility for improper use of timestamps.

8.3.5. Verification of timestamps

For the verification of a time stamp issued by Trans Sped TSA, the following aspects will be considered:

- Timestamp Issuer Verification: The issuer of a timestamp is a TSA that must use appropriate certificates to issue that timestamp. The public keys of the timestamp certificates are included in the TSU, and the CA certificates are published to allow verification that the timestamp was correctly signed by the TSA. The TSU certificates from Trans Sped are available for verification at: www.transsped.ro.
- Checking the revocation status of the time stamp: Trans Sped makes available to interested entities an OCSP service for checking the revocation status of the certificates used by the TSU for signing the time stamp. The OCSP service access address is included in the TSU certificate, used for signing the time stamp.
- Timestamp integrity check: To check the integrity of a timestamp, consider checking the cryptographic integrity of the timestamp (e.g., if the ASN.1 structure is correct, and the data belongs to the application). This information can be verified via the Trans Sped TSA web service provided free of charge by Trans Sped.

8.3.6. Service availability

Trans Sped TSA has implemented the following measures to ensure service availability:

- Redundant provision of IT systems to avoid "single point of failure."
- Redundant high speed internet connections.
- Use of uninterruptible power supplies (UPS) and electrical generators.

Although these measures ensure the availability of Trans Sped TSA services, 100% annual availability cannot be guaranteed. Trans Sped TSA aims to ensure a service availability of 99% per year.

8.4. TSA management and operation

8.4.1. Security management

Trans Sped ensures that administrative and managerial procedures are applied within the company

and that they are in accordance with industry practices. In particular:

a) Trans Sped bears full responsibility for providing the timestamping service in accordance with this policy.
b) Trans Sped has an information security policy that is known and respected by all employees and collaborators of the company.
c) The infrastructure necessary for information security management within Trans Sped is maintained and improved. Any change that has implications on the level of security ensured is approved by the management of Trans Sped.
d) Security controls and operating procedures related to Trans Sped TSA are documented, implemented, and maintained.

8.4.2. Classification and management of goods

Trans Sped ensures that information and other assets are properly protected. In particular, Trans Sped maintains an inventory of assets and classifies them according to protection requirements, in accordance with the results of the risk analysis.

8.4.3. Personnel security

Trans Sped ensures that selected personnel contribute to increasing confidence in the way TSA operates. In particular:

a) Trans Sped uses only personnel with knowledge and experience in the field of electronic signatures and time stamps for TSA operation.
b) Roles and responsibilities in the line of security assurance are included in the job descriptions. The trusted roles, upon which Trans Sped TSA security depends, are clearly identified.
c) Trans Sped ensures separation of responsibilities and compliance with the principle of least privilege, training and awareness of employees.
d) Staff perform their duties in accordance with security policies and procedures.

Trust roles for Trans Sped TSA assume the following responsibilities:

- Security Administrator: Overall responsibility for the implementation of security policies and procedures.
- System Administrator: Authorized to install, configure, and administer TSA systems and applications.
- Operator: Responsible for the day-to-day operation of TSA systems and applications. Authorized to perform system rescue and restore operations.
- Internal Auditor: Authorized to access the archives and audit logs of TSA's trusted systems.

The appointment of the people who will occupy trusted roles is made by the company's management, which carries out detailed checks on their antecedents.

8.4.4. Physical and environmental security

Trans Sped ensures that physical access to critical systems is controlled and physical risks to the company's valuables are minimized and complies with the requirements of the ETSI EN 319 401 standard. In particular:

a) For the service of providing timestamps, as well as for managing timestamps:

- physical access to the locations where the time marking services are set up is allowed only

to authorized personnel.

- control measures are implemented to prevent loss, destruction or compromise of assets or interruption of company activities.
- controls are implemented to prevent the compromise or theft of information or information processing systems.
- access control measures are implemented to the cryptographic modules used for signing time stamps.

b) The following measures are additionally provided for the timestamp management service:

- Timestamp Management Services are operated in an environment that provides physical protection against compromise through unauthorized access to systems and data.
- Physical protection is ensured by creating clearly defined security perimeters.
- Physical and environmental control measures are implemented to protect the locations surrounding the systems and facilities used to implement these services. These measures ensure, at a minimum, physical access control, natural disaster protection, fire protection, power outage protection, burglary protection and disaster recovery.
- Controls are implemented to protect against unauthorized offsite removal of timestamping services equipment, information, storage media, and software.

8.4.5. Operational management

Trans Sped ensures that the components of the TSA system are secured and operated correctly so as to minimize the risk of disruption to the timestamp service. In particular:

c) The integrity of TSA system components and information are protected against viruses, malicious or unauthorized code.

d) Incident reporting and response procedures are designed so that losses resulting from security incidents are minimized.

e) Storage media used in TSA's trusted systems must be managed securely to prevent destruction, theft or unauthorized access.

f) Operational procedures are developed and implemented for trust or administrative roles that impact the provision of timestamping services.

g) Storage media are managed securely, in accordance with the requirements imposed by the information classification scheme. Storage media containing sensitive data are destroyed when they are no longer needed.

h) The capacity of the equipment is monitored. Forecasts of future capacity needs are also made to ensure that there is always sufficient processing power and storage space available.

i) TSA ensures that it can act in a timely and coordinated manner to rapidly respond to incidents and limit the impact of security breaches. All incidents are reported as soon as possible.

8.4.6. Management of access to systems

Trans Sped ensures that access to TSA systems is permitted only to authorized personnel. In particular:

a) Control measures (e.g., firewall) are implemented to protect TSA's internal network against unauthorized access.

b) Ensures proper management of user accounts to maintain system security.

c) Ensure that access to information and applications is restricted in accordance with the access

control policy and that TSA systems allow the separation of trusted roles, especially those of administrator and operator. The use of system utilities is strictly restricted and controlled.

d) TSA personnel are properly identified and authenticated before they can use the applications specific to the timestamp service.
e) The actions of the TSA staff are logged.

The following measures are additionally provided for the timestamp management service:

a) Network components (e.g., routers) are kept in a secure physical environment and their configuration is periodically audited.
b) Continuous monitoring and alarming solutions are implemented to enable timely detection, recording and reaction to any unauthorized access to a resource.

8.4.7. Installation and maintenance of trust systems

Trans Sped uses reliable systems and products that are protected against modification. In particular:

a) In the design and development phase of the requirements for any system development project carried out by Trans Sped, the security requirements are analyzed.
b) Change control procedures are applied for commissioning, modification, updating of operational software applications.

8.4.8. Compromise of TSA services

In the event of an event affecting the security of the TSA services, such as the compromise of the TSU's private keys or the de-calibration of the clock used in the time-stamping process, Trans Sped will inform subscribers and third parties accordingly. The process of issuing timestamps is stopped until the cause of the event is fixed.

8.4.9. Termination of TSA activity

If Trans Sped TSA terminates its operations for any reason, it will notify the national supervisory authority prior to the effective termination. If Trans Sped TSA ceases to provide timestamping services, it minimizes potential disruption to subscribers and third parties and will continue to allow access to information necessary to validate previously issued timestamps. In particular:

a) Trans Sped TSA informs subscribers and third parties about the decision to stop providing time-stamping services.
b) Trans Sped TSA transfers to another TSA Authority or, as the case may be, to the Regulatory and Supervisory Authority, the operational electronic record of issued time stamps, the documentation related to the algorithms and procedures for generating time stamps, the digital public key certificate for signing timestamps, as well as other information necessary to demonstrate the correctness and validation of previously issued timestamps.
c) TSU private keys, including backup copies, are destroyed so that they cannot be recreated.
d) TSU certificates are revoked.

8.4.10. Compliance with legal requirements

Trans Sped will take all measures to ensure compliance with the legal requirements in force, with:

- European Regulation 910/2014 eIDAS
- Law no. 455/2001 on electronic signatures.

- Law no. 451/2004 regarding the time stamp.
- MCSI order no. 492/2009 regarding the technical and methodological rules for the application of Law no. 451/2004 regarding the time stamp.
- Regulation (EU) 679/2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR)
- Law no. 190/2018 on measures to implement Regulation (EU) 2016/679

8.4.11. Logging operations regarding the operation of the timestamping service

Trans Sped ensures that all relevant information regarding the operation of the timestamping service is recorded and retained to enable dispute resolution, detection of attempts to compromise TSA security and TSA auditing. In particular:

a) The confidentiality and integrity of current and archived records is ensured.
b) Records regarding the operation of the timestamping service are securely archived.
c) Important TSA events are recorded, such as those related to key management or clock synchronization.
d) The records are kept in accordance with the legal provisions in force.

Trans Sped maintains an operational electronic register of time stamps issued, permanently available for online consultation. The structure and operating conditions of the electronic register are those established by MCSI Order no. 492/2009 regarding the technical and methodological rules for the application of Law no. 451/2004 regarding the time stamp.

8.4.12. Network access

Trans Sped ensures network and system protection against malicious attacks. In particular:

a) The Trans Sped network is segmented and built in this way following risk analysis. This analysis considered the functional, logical, and physical relationship between trust systems and services.
b) Trans Sped restricts access and communications between areas used by trusted services. Unnecessary services are disabled, and unnecessary connections are prohibited by a set of periodically revised rules.
c) All critical items used by Trans Sped are kept in a safe and secure environment.
d) Dedicated networks used for the administration of the IT system are established, which are separated from the other networks. The system used for administration will not be used for purposes other than those specified.
e) Trans Sped has a test environment used by developers that is separate from the production environment.
f) Communication between distinct trusted systems can only be established through trusted channels, which are logically distinct from other communication channels and ensure the safe identification and protection of the parties involved and the modification or disclosure of data.
g) The internet connection is redundant, ensuring functionality in case the signal is not adequate.
h) Trans Sped periodically performs penetration tests and scans of the system to identify its vulnerabilities. Penetration testing and vulnerability scanning are performed by qualified

personnel who adhere to the code of ethics and provide accurate reports on a regular basis.

8.4.13. Incident management

System activities, users and services used by Trans Sped are monitored. In particular:

a) Activity monitoring considers the collected and analyzed information.
b) Activities that do not fall within the imposed rules of the system and indicate a possible breach of security, including network intrusion, are detected, and reported as alarms to authorized persons designated by Trans Sped.
c) Trans Sped systems monitor the following events:

- connecting and disconnecting from the network
- the availability and activity of the necessary services used in the network.

d) The management has appointed personnel who act in a timely and coordinated manner, to respond quickly to incidents and to limit the impact of possible security breaches. Designated personnel are tasked with tracking critical security events and ensuring that relevant incidents are reported in accordance with internal procedures.
e) Trans Sped informs the involved parties of any breach of security or loss of integrity, which has a significant impact on the reliable service provided and personal data. Supervisory bodies are notified within 24 hours of discovering a critical security breach.
f) Logs generated because of monitoring are periodically checked to identify possible malicious activities.
g) Trans Sped will fix critical vulnerabilities discovered within a reasonable period. If the vulnerability cannot be fixed, it tries to reduce the impact until it has the necessary resources (tools, updates, etc.). If a critical vulnerability will not be fixed, a document will be prepared stating why no action is required.
h) Reporting and response procedures are designed to minimize the impact an incident may have.

8.4.14. Business continuity management

All IT systems involved in the timestamping service provide at least N + 1 redundancy and are physically located in a secure environment that mitigates the risk of natural disasters. Timestamping service private keys are securely stored in a FIPS 140-2 Level 3 HSM that also provides N+1 redundancy. If private keys become compromised, periodic backups help distinguish between correct and false timestamps in an audit process. Following a natural disaster that causes the loss of premises, the timestamping service will operate using the equipment intended for this type of incident, and the activity will be redirected to a predetermined work point in the Business Continuity Management procedure.

8.5. Organizational measures

Trans Sped proves to be a reliable company. For this, Trans Sped has implemented and certified the following management systems: Quality management system according to ISO 9001:2015, Information security management system according to ISO/IEC 27001:2013, Environmental management system according to SR EN ISO 14001: 2005, Occupational Health and Safety Management System according to OHSAS 18001:2008.