Ed. Febbraio 2024

POSTE ITALIANE TIME-STAMPING AUTHORITY TRUST SERVICE POLICY AND PRACTICE STATEMENT

TSA Policy and PS - Versione 1.3 del 28/02/2024

Posteitaliane

TABLE OF CONTENTS

DOCUMENT HISTORY 1
DOCUMENT CHANGE CONTROL 1
1. INTRODUCTION 2
2. REFERENCES 3
3. DEFINITIONS AND ABBREVIATIONS 4
3.1 DEFINITIONS 4
4. GENERAL CONCEPTS 6
4.1 GENERAL POLICY REQUIREMENTS CONCEPTS 6
4.2 TIME-STAMPING SERVICES 6
4.3 TIME-STAMPING AUTHORITY (TSA) 7
4.4 SUBSCRIBER 7
4.5 TIME-STAMP POLICY AND TSA PRACTICE STATEMENT 8
4.6 OVERVIEW 8
4.7 IDENTIFICATION 9
4.8 USER COMMUNITY AND APPLICABILITY 9
5. POLICIES AND PRACTICES 10
5.1 RISK ASSESSMENT 10
5.2 TRUST SERVICE PRACTICE STATEMENT 10
5.3 TERM AND CONDITIONS 11
5.4 INFORMATION SECURITY POLICY 12
5.5 TSA OBLIGATIONS 12
5.5.1 TSA obligations towards subscribers 12
5.6 INFORMATION FOR RELYING PARTIES 13
6. TSA MANAGEMENT AND OPERATION 14
6.1 INTRODUCTION 14
6.2 INTERNAL ORGANIZATION 14
6.3 PERSONNEL SECURITY 14
6.4 ASSET MANAGEMENT 15
6.5 ACCESS CONTROL 15

6.6 CRYPTOGRAPHIC CONTROLS 16
6.6.1 General 16
6.6.2 TSU key generation 16
6.6.3 TSU private key protection 16
6.6.4 TSU public key certificate 17
6.6.5 Rekeying TSU's key 17
6.6.6 Life cycle management of signing cryptographic hardware 18
6.6.7 End of TSU key life cycle 18
6.7 TIME-STAMPING 18
6.7.1 Time-stamp issuance 18
6.7.2 Clock synchronization with UTC 19
6.8 PHYSICAL AND ENVIRONMENTAL SECURITY 19
6.9 OPERATION SECURITY 20
6.10 NETWORK SECURITY 20
6.11 INCIDENT MANAGEMENT 21
6.12 COLLECTION OF EVIDENCE 21
6.13 BUSINESS CONTINUITY MANAGEMENT 22
6.14 TSA TERMINATION AND TERMINATION PLANS 22
6.15 COMPLIANCE 23

DOCUMENT HISTORY

DOCUMENT CHANGE CONTROL

VERSION	PAGE	CHANGE	RELEASE DATE
1		First release	17/02/2017
1.1	13	Url for ocsp responder	18/10/2018
1.2	13 18	url for document download Limitations of the service TSU key lifetime	16/07/2020
1.3	12	Limitations of the service	28/02/2024

1. INTRODUCTION

This document describes the time stamp service provided by Poste Italiane S.p.A.and how to use it.
You are freely available for viewing and downloading on the website: http://postecert.poste.it and https://www.poste.it/prodotti/firma-digitale-remota.html .

2. REFERENCES

[1] Recommendation ITU-R TF.460-6 (2002): “Standard-frequency and time-signal emissions”.

[2] ETSI EN 319 401: “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”

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

[4] ETSI EN 319 422: “Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles”

[5] ETSI EN 319 411-1: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”

[6] ETSI EN 319 122 - CAdES digital signatures

[7] IETF (RFC3161) https://www.ietf.org/rfc/rfc3161.txt

[8] IETF (RFC3628) https://www.ietf.org/rfc/rfc3628.txt

3. DEFINITIONS AND ABBREVIATIONS

3.1 DEFINITIONS

AgID	National Digital Agency
Certification Body	Third party auditor, part of national supervisory body's processes.
Coordinated Universal Time (UTC)	Time scale based on the second as defined in Recommendation ITU-RTF.460-6 [1]
External parties	Suppliers of products necessary for the provision of the service
Relying party	Recipient of a time-stamp who relies on that time-stamp
Subscriber	Legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations
Time-stamp	Data in electronic form which binds other electronic data to a particular time stablishing evidence that these data existed at that time
Time-stamp policy	Named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements
Time-Stamping Authority (TSA)	TSP providing time-stamping services using one or more time-stamping units
Time-stamping service	Trust service for issuing time-stamps
Time-Stamping Unit (TSU)	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	Electronic service that enhances trust and confidence in electronic transactions
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 that particularly require emphasis or 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-stamp
TSA system	Composition of IT products and components organized to support the provision of time-stamping services
UTC(k)	Time scale based on the second as defined in ITU-R Recommendation TF.460-5 (TF.460-5)

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 and the following apply:

CA: Certification Authority
IT: Information Technology
TSA: Time-Stamping Authority
TSP: Trust Service Provider
TSU: Time-Stamping Unit
UTC: Coordinated Universal Time

4. GENERAL CONCEPTS

4.1 GENERAL POLICY REQUIREMENTS CONCEPTS

The present document references ETSI EN 319 401 for generic policy requirements common to all classes of trust service providers.

These policy requirements are based on the use of public key cryptography, public key certificates and reliable time sources.

Subscriber and relying parties are expected to consult the TSA's practice statement to obtain further details on how this time-stamp policy is exactly implemented by the particular TSA (e.g. protocols used in providing this service).

This document is edited, published and updated by Poste Italiane. Any change to this document is submitted to the internal review process, is approved by the Top Management and notified to National Digital Agency (AgID) and to the certification body.

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 time-stamps.
- *Time-stamping management*: this service component monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the time-stamping provision service.

The obligations of all external organizations supporting Poste Italiane services are governed through regular agreement.

4.3 TIME-STAMPING AUTHORITY (TSA)

Poste Italiane is a trust service provider as defined in ETSI EN 319 401 which issues time-stamps. The TSA is trusted by the users (i.e. Subscribers as well as Relying Parties) to issue secure TSTs.

Poste Italiane TSA takes overall responsibility for the provision of time-stamping services identified in section 4.2.

Poste Italiane TSA has responsibility for the operation of one or more Time-Stamping Units (TSU), which create and sign TSTs on behalf of the TSA. Each TSU has a different key.

4.4 SUBSCRIBER

The subscriber refers to either an individual or an organization that have agreed to the Poste Italiane TSP Subscriber Agreement.

When the subscriber is an individual, he / she will be held directly responsible if his / her obligations are not correctly fulfilled.

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

4.5 TIME-STAMP POLICY AND TSA PRACTICE STATEMENT

This clause explains the relative roles of time-stamp policy and TSA practice statement. It places no restriction on the form of a time-stamp policy or practice statement specification.

The time-stamp policy specifies how general requirements are met for trusted time-stamping services. Poste Italiane TSA specifies in its practice statement how these requirements are met.

Poste Italiane TSA time-stamp policy is defined independently from operating environmental details of Poste Italiane TSA.

Poste Italiane TSA practice statement is tailored to the Poste Italiane TSA's organizational structure, facilities, operating procedures, as well as computing environment.

The present document specifies the time-stamp policy and the practice statement for Poste Italiane TSA.Time-Stamping Policies.

4.6 OVERVIEW

Poste Italiane's TSA time-stamp policy is a set of rules that indicates the applicability of a TST to a particular community or class of application with common security requirements, which include the TSU, private keys, and profiles of public key certificates are compliant with technical specifications of the RFC 3161 and RFC 3628 and meet the general requirements described in ETSI EN 319 421 v1.1.1.

Means used in requesting for time-stamps include the Transfer Control Protocol (TCP) and Hypertext Transfer Protocol (HTTP).

Poste Italiane TSA holds private keys used in signing time-stamps.

Timestamp tokens are issued with an accuracy of ± 1 second, as indicated in TSA Obligations Toward Subscribers and TSA Disclosure Statement.

4.7 IDENTIFICATION

The identifier of the time-stamp policy specified in the present document is: 0.4.0.2023.1.1
{itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)}
The object identifier is referenced in every time-stamp issued by Poste Italiane TSA and claims conformance to the time-stamp policy that is supported in the TSA disclosure statement made available to subscribers and relying parties.

4.8 USER COMMUNITY AND APPLICABILITY

This policy is aimed at meeting the requirements of time-stamp for long term validity (e.g. as defined in ETSI EN 319 122) but is generally applicable to any use which has a requirement for equivalent quality.

This policy may be used for public time-stamping services or time-stamping services used within a closed community.

5. POLICIES AND PRACTICES

5.1 RISK ASSESSMENT

Poste Italiane TSP performs risk assessments on a regular basis to ensure the quality and reliability of the time-stamping services.
Security Controls that are defined in a security concept of the time-stamping services are controlled regularly in order to ensure the efficiency of the controls.

5.2 TRUST SERVICE PRACTICE STATEMENT

The present document defines the general elements of the policy and practice of CSP and provides TSS in the capacity of general conditions.
The Policy sets out the conditions and rules which CSP adheres to.
The Practice describes how CSP implements the described Policy and the procedures that it adheres to in the provision of TSS.
Poste Italiane TSA issues TST to each concerned party by following standard (non-guaranteed) service level.
A rule in Poste Italiane TSA Policy is to issue TST, following the practice and procedures included in this document.
Any user who needs guaranteed service level for TSS, concludes an Agreement for use of Poste Italiane TSS and SLA.
Additionally, to be compliant to ETSI EN 319 401 , for each time-stamp the following policies are supported by Poste Italiane TSA:

- **Time-stamp format**
  The issued time-stamp token by Poste Italiane TSA are compliant to RFC 3161 time-stamps. The service issues RSA2048 encrypted time-stamps that accept the hash algorithm *SHA256*.

- **Time accuracy**
  The time-stamping service uses this time signal and a set of *ntp* servers as time sources. With that setup the time-stamping service reaches an accuracy of the time of +/-1s or better with respect to *UTC*.
- **Limitations of the service**
  The QTSP Poste Italiane has entered into an insurance contract to cover the risks of the activity and the damage caused to third parties, the text of which has been sent to the Italian superbody AgID. The economic values are shown:
  - 1,000,000 euros per single claim;
  - 2.000.000 euros per year.
- **Subscriber's obligations**
  Please see "Terms and conditions for timestamp customer" for detailed information.
- **Relying party's obligations**
  Please see "Terms and conditions for timestamp customer" for detailed information.
- **Verification of the timestamp**
  Timestamp verification includes the following steps:

Step I: Verification of the timestamp revocation status
Check of the TSU certificate validity period and of the signing key validity is verified using current revocation status for the TSU's certificate via ocsp, available at http://postecert.poste.it/pi-TS-ocsp or at cdp http://postecert.poste.it/piTSP/CATSA.crl.

Step II: Verification of the timestamp integrity
The cryptographic integrity of the timestamp, for example the correct ASN.1 structure, and the belonging datum (the data that has been timestamped) can be verified with client "firmaOK!"

5.3 TERM AND CONDITIONS

A qualified time stamp is an electronic certificate, which states when certain data existed. Poste Italiane TSP is a qualified trust service provider according to the rules of eIDAS regulation.

The execution of qualified time stamps and time signatures are provided via the Internet only in context of service and/or license agreements. Poste Italiane guarantees the availability of time stamp service except in the case of programmed maintenance activity, that is previously notified to the subscribers. Poste Italiane TSP has the authority at any time to perform maintenance, upgrades or modifications without that these losses be taken into account when calculating the availability of key services.
Poste Italiane TSP will inform the customer before the planned date about the interruption of key services such as maintenance, upgrades, or modifications, at least fourteen days.
Timestamp protocols, meaning every issued timestamp, are kept for at least 20 years.

5.4 INFORMATION SECURITY POLICY

Poste Italiane has implemented an information security policy throughout the company. All employees must adhere to the regulations stated in that policy and derived security concepts. The information security policy is reviewed on a regular basis and when significant changes occur. Poste Italiane Top Management approves the changes of the information security policy.

5.5 TSA OBLIGATIONS

The conformance with the procedures that are stated in the present document is ensured by Poste Italiane. An independent supervisory body verifies the efficiency of the procedures on a regular basis.

5.5.1 TSA obligations towards subscribers

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the clause 6.3, Terms and conditions.

5.6 INFORMATION FOR RELYING PARTIES

The obligations of a Subscriber (see clause 6.5.1) are valid for relying parties too. In addition, the relying party shall do the following:

- verify that the time-stamp has been correctly signed and that the private key used to sign the time stamp has not been compromised until the time of the verification;
- take into account any limitations on the usage of the timestamp indicated by the timestamp policy;
- take into account any other precautions prescribed in agreements or elsewhere.

6. TSA MANAGEMENT AND OPERATION

6.1 INTRODUCTION

Poste Italiane has implemented an information security management system to maintain the security of the service.

6.2 INTERNAL ORGANIZATION

For proper operations of the time-stamping service, Poste Italiane maintains a non-disclosed document, security concept that specifies all operational controls concerning personnel security, access controls and risk assessment. That internal document is used by independent bodies to confirm compliance of the service against ETSI TS 119 421.

6.3 PERSONNEL SECURITY

Poste Italiane has understood that talented and motivated employees are a key factor for business success. Therefore, hiring practices is a very important process at Poste Italiane. Only well-educated, with respect to their job role, and trustworthy personnel fulfill operations in the time-stamping service. A role concept enforces the segregation of duties to ensure that entitled personnel only do important operational tasks.

Before that personnel is appointed in trusted roles, the TSP verifies that the necessary knowledge exists or is going to be transferred via trainings and that all background-screening tasks are completed. TSP personnel is free from conflict of interests that might prejudice the impartiality of the TSP operations.

6.4 ASSET MANAGEMENT

Poste Italiane TSP maintains an inventory of all its assets and assigns a classification for the protection requirements to all assets consistent with the risk analysis. All media is handled securely. Data from disposed media is securely deleted when no longer required.

6.5 ACCESS CONTROL

The TSP's system access is limited to authorized individuals. In particular:

- Controls (e.g. firewalls) protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties. Firewalls are configured to prevent all protocols and accesses not required for the operation of the TSP.
- The TSP manages user access of operators, administrators and system auditors. The administration includes user account management and timely modification or removal of access.
- Access to information and application system functions are restricted in accordance with the access control policy. The TSP system provides sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, the use of system utility programs is restricted and controlled.
- TSP personnel are identified and authenticated before using critical applications related to the service.
- TSP personnel are accountable for their activities.

Sensitive data are protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

6.6 CRYPTOGRAPHIC CONTROLS

6.6.1 General

The form and purpose of timestamps are defined by ETSI EN 319 422 standards. The value of a timestamp is determined by the trust of the timestamp provider. The role of a timestamp is to establish evidence indicating that data existed at particular time. The TSU provides trust and evidence-quality timestamps with these features:

- No timestamp can be fraudulently created outside of the timestamp service.
- Every timestamp produced is traceable to two audited events, the source code compilation, and the lockdown of the TSU.
- The HSM FIPS 140-2 Level 3 certification ensures keys cannot be extracted; only an unaltered timestamp server can create trusted timestamps.
- The TSU's clock is synchronized to official time sources via NTP through a primary source using a GPS signal and through a secondary source using a service exposed bythe internet from 'INRIM (National Electrotechnical Institute "Galileo Ferraris" of Torino).
- The TSU records a signed log of all clock adjustments.

6.6.2 TSU key generation

Poste Italiane's TSA ensures that any cryptographic keys are generated under controlled circumstances.
The generation of the TSU's signing key(s) are undertaken in a physically secured environment as described by personnel in trusted roles under, at least, dual control.
The personnel authorized to carry out this function are limited to those assigned to the specific roles under TSA's practices.

6.6.3 TSU private key protection

Poste Italiane TSA keeps its private keys in Hardware Security Modules evaluated as "E4 high" according to ITSEC criteria (or equivalent), or using a FIPS 140-2 Level 3.
The HSMs are kept in a secure physical dedicaded structure. Access to both the facility and the private keys is protected by access control mechanisms.

The private keys can only be activated by two persons and are, once decrypted using the proper authorization, never written to any permanent or magnetic storage media.
The use of FIPS 140-2 Level 3 or ITSEC “E4 high” certified cryptographic modules prevents that private keys can be exported from the modules in clear. No copy of any private key is kept on magnetic media in unencrypted form. Private keys used for time-stamping are backed up, copied, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.
The personnel authorized to carry out this function are limited to those assigned to specific roles under Poste Italiane TSA role concept.

6.6.4 TSU public key certificate

Poste Italiane TSA shall guarantees the integrity and authenticity of the TSU signature verification (public) keys with at least the following particular requirements:

- TSU signature verification (public) keys is made available to relying parties in a public key certificate.
- The TSU signature verification (public) key certificate is issued by a certification authority operating under ETSI EN 319 411-1.
- The TSU shall not issue time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device.
- When obtaining a signature verification (public key) certificate, the TSA should verify that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

6.6.5 Rekeying TSU’s key

TSU keys will have the expected lifetime of 3 years. A certificate is issued for the whole expected lifetime.

Before the validity period is reached, the TSU private signing keys need to be replaced. Poste Italiane activates the signing TSU’s key change procedure every year.

6.6.6 Life cycle management of signing cryptographic hardware

Poste Italiane TSA applies the following particular requirements:

- Time-stamp signing cryptographic hardware shall not be tampered with during shipment.
- Time-stamp signing cryptographic hardware shall not be tampered with when and while stored.
- Installation, activation and duplication of TSU's signing keys in cryptographic hardware are done only by personnel in trusted roles using, at least, dual control in a physically secured environment.
- TSU private signing keys stored on TSU cryptographic module are erased upon device retirement in a way that makes practically impossible to recover them.

6.6.7 End of TSU key life cycle

The expiration date for TSU's keys is less than or equal to the end of validity of the associated public key certificate.
The TSU key generation algorithm, the resulting signing key length and signature algorithm used by Poste Italiane TSA for signing time-stamps key are as specified in ETSI TS 119 312.

6.7 TIME-STAMPING

6.7.1 Time-stamp issuance

The structure of the time-stamp token complies with the requirements of ETSI EN 319 422 V1.1.1 (2016-03).
Poste Italiane's TSA ensures that time-stamp tokens are issued securely and include the correct date and time.
In particular:

- the time values the TSU uses in the time-stamp token is traceable to UTC
- the value of time included in the time-stamp token does not differ from UTC more than the accuracy defined in the policy and in the time-stamp itself

- if the time stamp provider's clock is detected as being out of the stated accuracy, then time stamp tokens are not issued
- the time-stamp are signed using a key generated exclusively for this purpose
- the time-stamp generation system rejects any attempt to issue a time stamp when the end validity of the TSU private key has been reached.

6.7.2 Clock synchronization with UTC

Poste Italiane's TSA ensures that its clock is synchronized with UTC within the declared accuracy following the requirements:

- the calibration of the TSU clocks shall be maintained such that the clocks shall not be expected to drift outside the declared accuracy;
- the declared accuracy is of 1 second or better;
- the TSU clocks are protected against theats which could result in an undetected change to the clock that takes it outside its calibration;
- the TSA shall ensure that, if the time that would be indicated in a time-stamp token drifts or jumps out of synchronization with UTC, this is detected;
- records concerning all events relating to synchronization of a TSU's clock to UTC are logged. This includes information concerning normal re-calibration or synchronization of clocks use in time-stamping;
- records concerning all events relating to detection of loss of synchronization are logged.

6.8 PHYSICAL AND ENVIRONMENTAL SECURITY

Poste Italiane TSP controls physical access to components of its PKI system, whose security is critical to the provision of its trust services and to minimize risks related to physical security.

Poste Italiane TSP ensures that the location and construction of the facility housing the TSA equipment are consistent with facilities to house high value and sensitive information.

6.9 OPERATION SECURITY

Poste Italiane TSA ensures that the TSA system components are secure and correctly operated, with minimal risk of failure. In particular:

- The integrity of TSA system components and information is protected against viruses, malicious and unauthorized software.
- Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions is minimized.
- Media used within the Poste Italiane TSA trustworthy systems are securely handled to protect media from damage, theft, unauthorized access and obsolescence.
- Procedures are established and implemented for all trusted and administrative roles that impact on the provision of time-stamping services.
- Capacity demands are monitored continuously to ensure that Poste Italiane TSP can meet the claims of availability given to all customers. Future capacity projections are updated regularly to ensure that no break in service will occur at any future point.

6.10 NETWORK SECURITY

Poste Italiane TSP protects its network and system from attack, in particular:

1) segmenting Certificate Systems into networks or zones based on their functional, logical, and physical relationship;
2) separating test, certification and production platform from other environments not concerned with live operations;
3) maintaining and protect Issuing Systems, Certificate Management Systems, and Security Support Systems in a Secure Zone;
4) configuring each network boundary control (firewall, switch, router, gateway) with rules that support only the services, protocols, ports, and communications that the TSA has identified as necessary to its operations;
5) configuring all TSU systems by removing all accounts, services, protocols and ports that are not used in the TSA's operations;
6) according access only trusted roles to high secure zone.

6.11 INCIDENT MANAGEMENT

Poste Italiane TSP:

1) monitors start-up and shutdown of the logging functions and the availability of the network services
2) appoints trusted role personnel to follow up on alerts of potentially critical security events
3) If an unplanned interruption of TSA service occurs, opens a related incident and manages it in order to identify, to register in Trouble Ticketing system, to prioritize and to diagnose the incident
4) Escalation - should the Support Staff need support from other organizational units
5) acts in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security
6) 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
7) notifies the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein
8) Informs the national supervisory body AgID within 24h after discovery of a critical security breach via e-mail
9) Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimized.

6.12 COLLECTION OF EVIDENCE

Poste Italiane TSP records and keeps accessible for an appropriate period of 20 years, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. In particular:

- The confidentiality and integrity of current and archived records concerning operation of services is maintained.
- Records concerning the operation of services are completely and confidentially archived in accordance with disclosed business practices.

- Records concerning the operation of services are made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.
- The precise time of significant TSP environmental, key management and clock synchronization events are recorded. The time used to record events as required in the audit log is synchronised with UTC continuously.
- Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP terms and conditions.
- The events are logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

6.13 BUSINESS CONTINUITY MANAGEMENT

Poste Italiane TSP defines and maintains a continuity plan to enact in case of a disaster. In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, failure of critical components of its trustworthy system, including hardware and software, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur with appropriate remediation measures.

6.14 TSA TERMINATION AND TERMINATION PLANS

In the event that the Poste Italiane TSA terminates its operation, it shall notify its national supervisory body AgID prior to termination.

Following an up-to-date termination plan, Poste Italiane TSP provides a timely notice for all relying parties in order to minimize any disruptions that are caused because of the termination of the services.

- The TSP will inform at least 60 days before the termination the following entities: all subscribers and other entities with which Poste Italiane has agreements or other form of established relations, among which relying

parties, Poste Italiane and relevant authorities (AgID and the certification body). In addition, this information shall be made available to other relying parties;;

- TSP will terminate 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;
- The TSA will maintain or transfer to a reliable party its obligations to make available its public key or its certificate to relying parties for a reasonable period;
- The TSP has an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.
- Where possible TSP tries to make arrangements to transfer provision of trust services for its existing customers to another TSP.
- TSU private keys, including backup copies, are destroyed in a manner such that the private keys cannot be retrieved.

6.15 COMPLIANCE

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

- Regulation (EU) N°910/2014
- ETSI TS 119 421
- IETF (RFC 3161)

Whenever possible, the TSP makes its services available to persons with disabilities.

poste.it

Posteitaliane