TIME-STAMP AUTHORITY

Trust Service Practice Statement

Codice documento: REGIT-TSA-TSPS
Versione: 1.1
Redatto da: Serena Giugni
Approvato da: Marco Chiaverini
Data approvazione: 18/03/2025

Sommario

1. Introduction

Register SpA – (VAT/Tax Code 04628270482), registered since 26.04.1995 with the Florence Business Register.

Register SpA (hereinafter also referred to as “Register”) is a historical leader in Italy in the provision of domain registration, hosting, brand protection, and online advertising services.

It is also qualified as a "Certified Email Provider" (PEC), duly registered in the public list of PEC providers coordinated by the Agency for Digital Italy (AgID), and as an accredited Identity Provider by AgID.

This document describes Register's Time-Stamping service, which will be used solely for internal purposes.

1.1 Regulatory References

The following qualified trust services meet the eIDAS requirements (Regulation (EU) No. 910/2014) and comply with the following standards:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates.
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ETSI EN 319 122 - CAdES digital signatures
- IETF (RFC3161) https://www.ietf.org/rfc/rfc3161.txt
- IETF (RFC3628) https://www.ietf.org/rfc/rfc3628.txt

1.2 Document Version and History

Versione del documento e storia delle modifiche			
Versione	**Data**	**Paragrafo**	**Note sui cambiamenti**
1.0	01 May 2019	*Tutti*	*All First version of the document*
1.1	18 March 2025	*3.5*	*Explicit reference to the periodic review of the management system.*

2. Definitions and Abbreviations

This section is aimed at facilitating the interpretation of the terms and acronyms used in this document.

The main regulatory sources referenced are provided in the section on Regulatory References.

Acronimi	Definizione
CA	Certification Authority
CAO	Certificate Authority Officer
TSPP	TSP Policy
TSPPS	TSP Practice Statement
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
QTSA	Qualified Time-Stamping Authority
PKI	Public Key Infrastructure – certificate issuance component.
RAO	Registration Authority Officer
RFC	Request For Comments
TIN	Tax Identification Number
TSA	Time-Stamping Authority
TSU	Time Stamping Unit
TLS	Transport Layer Security
TSP	Trust Service Provider

3. General Concepts

3.1 General Requirements

The policy for Register's time-stamping service is based on the use of public key cryptography, digital certificates, and a reliable temporal reference.

The service is provided by the TSP Register, in compliance with the standards and requirements described in the ETSI EN 319 401 specification, which applies to all services provided by any Trust Service Provider.

The specific policies and practices for the time-stamping service are detailed later in this document.

3.2 Time-Stamping Service

The time-stamping service consists of issuing a temporal evidence, in the form of a Time Stamp Token (i.e., a digital object compliant with the IETF RFC 3161 specifications).

The time-stamp thus issued aims to reliably and opposably bind a UTC temporal reference to a set of electronic data, providing evidence that these data existed at the temporal point indicated in the time-stamp and ensuring that they have not been altered or modified afterward.

3.3 Time-Stamping Authority (TSA)

The Trust Service Provider Register acts as the Time-Stamping Authority (TSA) in the time-stamp issuance process, in accordance with the definition provided in the previous section.

To provide the time-stamping service, the TSA utilizes one or more Time-Stamping Units (TSU), consisting of hardware and software components involved in issuing the time-stamp.

Each TSU managed by Register uses a different private key for the digital signing of time-stamps issued on behalf of the TSA.

3.4 Use of the Service

The use of the time-stamping service is subject to Register's general service terms and conditions and implies acceptance of the policies and procedures outlined in this document, which govern and limit the issuance of time-stamps.

Users of Register's time-stamping service are individuals or organizations authorized to access the service and request the issuance of a time-stamp, using suitable technological tools compliant with the specifications outlined in IETF RFC 3161.

3.5 Policy e Practice Statement

In this document, Register, as TSA, specifies the policy that defines the conditions under which the time-stamping service is provided, in accordance with the ETSI EN 319 401 and ETSI EN 319 421 specifications.

In subsequent chapters of this document, a Practice Statement, compliant with the ETSI EN 319 401 and ETSI EN 319 421 specifications, outlines the practices and procedures implemented by Register to meet the general requirements described in the time-stamping service policy.

The service is subject to checks at least semi-annually to verify compliance with the expected service level, investigate the causes of any incidents or service disruptions, and promote prevention or improvement activities.

Audits are scheduled at least annually, in accordance with internal functions, to cover regulatory, process, organizational, technological, and logistical aspects, often with the intervention of specialized consultants. The aim is to verify the system’s compliance with laws and regulations.

4. Time-Stamp Policy

Register's TSA provides the time-stamping service in accordance with the Best Practices Time-Stamp Policy (BTSP) defined in the ETSI EN 319 421 specification.

Therefore, the time-stamps issued by Register admit the following OID as the policy identifier:

0.4.0.2023.1.1

The OID is defined alongside the BTSP and is structured as follows:

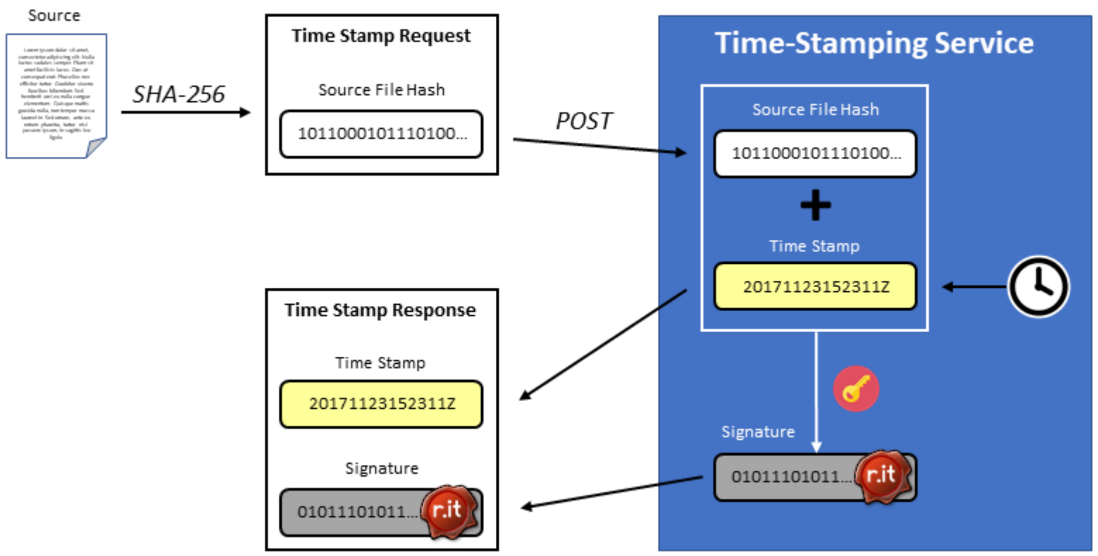
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy(1)

Including this identifier in all time-stamps issued by Register attests to their compliance with the BTSP.

5. TSA Operations

5.1 Provision of Time-Stamps

Register's time-stamping service is accessible through a secure SSL HTTP interface and complies with IETF RFC 3161 and ETSI EN 319 422 specifications.
It accepts a Time-Stamp Request and responds with a Time-Stamp Response, as illustrated in the following diagram:



5.1.1 Time-Stamp Request

The application accepts requests in HTTP POST, with the Content-Type header set to:

application/timestamp-query

The body of the request must be a Time-Stamp Request object (as defined in IETF RFC 3161, section 2.4.1), properly encoded. As per ETSI EN 319 422 specifications, the fields reqPolicy, nonce, and certReq are supported.

The request must contain the hash of the original data to which the time-stamp is to be applied. The only accepted algorithm for generating this hash is SHA-256..

5.1.2 Time-Stamp Response

Upon receiving a valid Time-Stamp Request, the application always provides a Time-Stamp Response (as defined in IETF RFC 3161, section 2.4.2), properly encoded in an HTTP response with Content-Type:

application/timestamp-reply

In particular, according to ETSI EN 319 422, the fields accuracy and nonce are supported and used as specified.

If the time-stamp cannot be issued, a Time-Stamp Response containing a specific error code is generated to identify the issue. In all other cases, the response contains a Time-Stamp Token, which is the formal representation of the time-stamp.

The signature applied to the time-stamp by Register's TSA uses the RSA algorithm with asymmetric keys, with a key length of at least 2048 bits.

5.2 TSU Certificate

For time-stamp issuance, Register's TSA uses one or more units called TSU (Time-Stamping Unit), which actually provide the time-stamping service on behalf of the TSA.

The TSU applies a digital signature to the time-stamps it issues, using the RSA algorithm with a specific asymmetric key pair unique to each unit.

The certificate associated with the TSU keys complies with ETSI EN 319 412-3 and ETSI EN 319 422 specifications: in particular, the attributes countryName, organizationName, organizationIdentifier, and commonName are properly populated. The commonName uniquely identifies a specific TSU belonging to Register's TSA.

Furthermore, as specified in IETF RFC 3161, the certificate specifies the Extended Key Usage OID corresponding to the issuance of time-stamps (1.3.6.1.5.5.7.3.8).

The key length associated with the certificate is at least 2048 bits.

The certificate has a validity period of 90 days.

5.3 Temporal Reference Accuracy

The accuracy of the temporal reference used by Register's TSA for timestamping is ‘better than’ 1 second, in accordance with the Best Practices Time-Stamp Policy (BTSP) defined in the ETSI EN 319 421 specification.

To ensure this constraint is met, a system based on the NTP protocol is used: each TSU machine has an NTP client installed, which ensures the synchronization of the system clock with the temporal reference of Register’s internal time servers. These internal time servers, in turn, regulate their clocks with the clocks of reference time servers for the UTC signal. This platform is compliant with the Network Time Protocol described in IETF RFC 5905.

Register's internal time servers implement a continuous synchronization system with the configured reference servers, dynamically selecting the one with the shortest temporal distance.

For each of Register’s internal time servers, multiple stratum 1 reference servers (i.e., time servers that synchronize their internal clocks with atomic clocks) are configured. These are chosen for accessibility over different network paths to minimize the risk of a geographical network issue preventing continuous synchronization of the internal platform.

By using *stratum 1* as reference servers, Register’s internal time servers are *stratum 2*, each configured as a peer to the others, forming an isolated network. Even in the absence of an external connection, the time servers drift less quickly than a single server could.

Internal time servers undergo periodic reviews to ensure that the reference time servers are accessible and remain *stratum 1*. The relationship with reference servers is updated dynamically: if one of the configured reference servers becomes more reliable (i.e., with lower delay) or the previously selected server starts drifting (with increasing jitter), the time server will switch to the new *stratum 1*.

The various TSU servers, via their NTP clients, synchronize with Register’s internal time servers, becoming *stratum 3*. They implement the same continuous synchronization and dynamic reference selection process as the internal time servers, discarding and replacing any internal time server that becomes unsynchronized.

If the monitoring system detects that the reference clock of one of the TSUs deviates by more than 1 second from UTC time, the corresponding machine will automatically be removed from the cluster and will no longer be used for issuing timestamps until its internal clock is resynchronized and the machine is restored to service.

5.4 Logs

The Register TSA system generates a series of logs of different types, each of which is recorded and subsequently kept for the time period required by the applicable regulations.

Specifically, the following logs are produced:

- *Physical access logs:* All physical access to premises, machines, and devices that make up the timestamping system are recorded in a specific log.

- *Synchronization logs:* System clock synchronization operations carried out according to the NTP protocol are logged in a specific log.

- *Security logs*: Operations involving the generation, installation, and revocation of certificates used by the TSU are logged in dedicated logs.

- *Traffic logs*: Interactions with the timestamping service by clients produce HTTP traffic logs, which are appropriately handled.

- *Application logs*: The application managing the operation of the TSU generates application logs that record the issuance of timestamps.

5.5 Timestamp Verification

The verification of timestamps issued by Register’s TSA can be carried out with the following steps:

a. Generation of the SHA-256 hash from the original data;
b. Combination of the hash with the timestamp embedded in the timestamp;
c. Verification of the signature in the timestamp using the TSU's public key;
d. Formal verification of the TSU certificate and its validity.

Any software that meets the IETF RFC 3161 specifications can automatically complete the above process.

6. Management and Maintenance of the TSA

6.1 Security Measures (Physical, Procedures, Personnel)

The logical and physical security measures follow those defined and described within the security plan and the procedures referenced within it.

6.2 Management of Cryptographic Controls

6.2.1 Generation and Installation of TSU Keys

Every 90 days, the TSU signing key is generated directly on the HSMs through the dedicated management appliance, and the same applies to the corresponding CSR.

Once signed, the certificate is imported into the HSMs and paired with the signing key.

6.2.2 Protection of the Private Key

The private key is stored within the Thales HSMs and is not exportable. The platform contains two HSMs, accessed via a load balancing system, and two Thales appliances to ensure continuous operation.

6.2.3 TSU Public Certificate

The TSU public certificates will be available directly on the internet without the need for authentication via a dedicated web server with a secure connection (https), providing only this service.

6.3 Software Maintenance

6.3.1 Updating Proprietary Applications

The core application of the TSU is a proprietary software, developed in Java. Any modification to this software is subject to the internal change management procedures of the TSP Register, and additionally requires the execution of a dedicated testing suite. This suite covers the main technical requirements specified in IETF RFC 3161 and ETSI EN 319 422 to ensure that any modification does not compromise the core functionalities of the system.

The monitoring platform also continuously checks at regular intervals to ensure that the timestamping service is provided correctly and that the timestamps produced are valid and compliant with the specifications.

6.3.2 Updating Third-Party Software

Operating systems and cryptographic appliances are systematically updated for security bugs through official vendor channels. The procedure details are described in the internal procedures referenced in the security plan.

6.4 TSA Termination Plan

In the event that Register's TSA ceases its operations, the following procedure will be implemented:

a. The intention to terminate the service will be communicated to AgID and users at least 60 days before the planned cessation date.

b. Register commits to maintaining access to certificates and public keys for verifying previously issued timestamps for a reasonable period after cessation, or alternatively, transferring them to a replacement entity that will make them available for the same period.

c. Upon service cessation, all TSU private keys will be irreversibly destroyed, and the corresponding certificates will be revoked.

6.5 Incident Management and Risk Assessment

Incident management and risk analysis are included within the TSA's Timestamping Service Security Plan.