TIME-STAMPING POLICY AND PRACTICE STATEMENT

ancert
Agencia Notarial de Certificación

Documentary Control

title:	Time-Stamp Policy and Practice Statement
Type of document:	Policy
name:	Declaración de Prácticas y Política de TSA_ENG.docx
Version:	1.0
Status:	Draft
Confidentiality:	Internal use document
Date:	01/23/2020
Author:	Security Office

Review, Approval		
Reviewed by:	Information Security Manager	Date: 01/23/2020
Approved by:	Security Committee	Date: 02/04/2020

Change history			
Version	**Date**	**Description of the action**	**Pages**
1.0	01/23/2020	Creation of the document.	

Index

1. Introduction

This document contains the time-stamp policy and practice statement of the Notarial Certification Agency SL Unipersonal (ANCERT).

The qualified time stamp service is part of ANCERT's service portfolio as a Qualified Trust Service Provider (TSP, for short) under the terms defined by Regulation (EU) 910/2014 [1].

The structure and numbering of this document is the same as that of the ETSI EN 319 421 standard [4]. This document complements the General Certification Policy [9] and the Certification Practices Statement (DPC) [9] with processes and technical issues for the provision of the TSA service.

These procedures and their proper implementation are audited by an external entity, according to the specifications defined by ETSI standard EN 319 421 [4].

2. References

Legal and technical standards

[1] Regulation (EU) 910/2014.
[2] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
[3] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
[4] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
[5] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
[6] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
[7] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

TSP policies and practice statements

[8] ANCERT: "General Certification Policy".
[9] ANCERT: "Certification Practice Statement for Notarial certificates".
[10] ANCERT: "Certificate Profiles of the Certification Authority".

3. Definitions and abbreviations

3.1. Definitions

Time-Stamping Authority (TSA): TSP issuing time stamps.

Coordinated Universal Time (UTC): time scale (second based), as defined in ITU-R TF.460-6 [2].

TSA Practice Statement (DPTSA): TSA practice statement for the issuance of time stamps.

TSA Practice Statement Disclosure (DPDTSA): statements about the policy and practices that require special disclosure between subscribers and third-party users.

Time-Stamping Policy: rules that apply to the TSA for the issuance of time stamps.

Trust Service Provider (TSP): entity that provides Trusted Services according to the definition of Regulation (EU) 910/2014 [1]

Time stamp (TST): data object that relates the existence of digital data at a specific time. It serves as evidence that some data existed at a certain time in the timeline.

Time-Stamping service: trusted service for the issuance of time stamps.

Subscriber: natural or legal person who uses the services provided by the TSA and who explicitly accepts their terms and conditions.

Third-party users: users receiving and trusting time stamps.

Time-Stamping unit (TSU): hardware and software components managed as a whole and providing time stamps from a single time source. The components can be cloned (redundancy) in order to achieve high availability.

3.2. Abbreviations

TSA: Time-Stamping Authority

TSU: Time-Stamping Unit

TST: Time Stamp Token (time stamp)

UTC: Coordinated Universal Time

eIDAS: Regulation (EU) No. 910/2014

DPTSA: TSA Practice Statement

DPC: Certification Practice Statement

4. General Concepts

4.1. Time-stamping services

Time-Stamping services include two components:

- **Time-Stamping issuance:** technical component responsible for generating the time stamps.
- **Time-Stamping administration:** component that monitors and controls the operation of the Time-Stamping service. This component is responsible for the installation and uninstallation of the Time-Stamping provisioning service. The administration service ensures that the clocks used by the issuance service are correctly synchronized with UTC.

4.2. Time-Stamping authority

A Time-Stamping Authority (TSA) is a Trust Service Provider as described in ETSI EN 319 401 [3] that provides certainty about the preexistence of certain electronic documents at a given time by issuing time stamps (TST).

The TSA of ANCERT assumes all responsibility for the provision of the Time-Stamping services indicated in section 6.5.4. The TSA of ANCERT can run several identifiable Time-Stamping units (TSU).

Within a TSU it is allowed key cloning for their use in redundant components to meet high availability requirements.

The TSA of ANCERT can be identified by the electronic certificate used by its Time-Stamping issuance service, according to section 7.7.1.

4.3. Subscriber

Subscribers are the natural and legal persons that subscribe to the Time-Stamping service and request stamps during the subscription period.

If the subscriber is a legal person, obligations applying to the organization also apply to its corresponding end users. In any case, the legal person will be responsible if the obligations are not correctly fulfilled by the end users. Therefore, that organization must properly inform its end users.

If the subscriber is a natural person, then this end user will be directly responsible for complying with the obligations.

4.4. Time-Stamping Policy and TSA Practice Statement

The Time-Stamping Policy defines the rules and procedures that apply to the issuance of time-stamps, including all the requirements that the subscriber must meet.

The Time-Stamping Practice Statement describe a set of statements about how the Time-Stamping service has been implemented in order to meet the policy requirements.

This document complements and extends the procedures described in the DPC [9] for the provision of the Time-Stamping service.

5. TSA Policy and general requirements

5.1. General

ANCERT defines in this document its own policy for qualified Time-Stamping service, with an accuracy of 1 second for the time source. This policy is in accordance with the requirements of the technical standard ETSI EN 319 421 [4].

5.2. Identification

In accordance with this policy, time stamps (TST) issued by the TSA of ANCERT include the following identifier (OID):

1.3.6.1.4.1.18920.200.2.1

5.3. User community and applicability

The users of the Time-Stamping service will be the subscribers and third parties that require the service.

ANCERT acts as TSA for the General Council of Spanish Notaries, Notarial Colleges and Spanish Notaries in the exercise of their public function activity.

Other users must previously contract the service with ANCERT in order to access the Time-Stamping service.

5.3.1 Limits of use of the service and the time stamps

Time-stamps will be used for their intended purpose. Other uses or purposes are strictly forbidden.

6. Policies and practices

6.1. Risk assessment

ANCERT has a risk management plan to identify, analyze and evaluate the risks that may affect the Time-Stamping service.

ANCERT has a risk treatment plan in order to prioritize, select and implement the appropriate security measures to deal with the risks identified in the risk management plan.

ANCERT updates the risk analysis with the periodicity established in the risk management plan, and when substantial changes are performed in the service.

ANCERT General Management formally approves the risk treatment plan resulting from the risk management procedures, and accepts the residual risk.

6.2. TSA Practice Statement

ANCERT, as a TSA, develops, implements, enforces and updates this document containing the TSA Practice Statement to meet the requirements of its Time-Stamping policy.

All Procedures and their correct implementation are audited annually by an independent external entity.

Practice Disclosure Statement for the TSA is published independently of this document and is available 24x7 at https://www.ancert.com/cps .

6.3. General requirements of the Practice Statement

This document containing the Time-Stamping practice statement, and other relevant documentation is available 24x7 at https://www.ancert.com/cps .

Organization that manages this document

Agencia Notarial de Certificación, SL Unipersonal

Paseo General Martínez Campos, number 46.- 6º, Elcano Building

28010 Madrid (Spain)

NIF B-83395988

Organization contact information

Any contact with ANCERT, referring to this document may be done by the following means:

- email address: ancert@ancert.com.
- Phone number: 902 348 347.
- Headquarters: Notarial Certification Agency, SL Unipersonal. Martínez Campos Avenue, number 46.- 6, Elcano Building 28010 Madrid (Spain)

Any change in the above data such as Web, mail, address or telephone will be duly reflected on the website www.ancert.com, publicly available (and up-to-date) in the Internet.

Documentation management procedures

ANCERT General Management determines the suitability of this Practice Statement and is responsible for its approval.

ANCERT has an internal procedure for creating, reviewing and formally approving this document.

6.4. Information Security Policy

ANCERT has an information security policy, approved by its General Management, which defines how the organization manages information security.

6.5. Obligations and responsibilities

6.5.1 Obligations of the Time-Stamping Authority

ANCERT guarantees, under its sole responsibility, the fulfillment of the requirements established in the TSA policy.

ANCERT is the only responsible for complying with the procedures described in this policy, even when part or all the operations are outsourced externally.

ANCERT provides certification services in accordance with its current Certification Practice Statement, which details the functions, operating procedures and security measures.

6.5.2 Obligations of the subscriber

Subscribers of the Time-Stamping service must:

- Respect the provisions of the contractual documents signed with ANCERT.
- Comply with ANCERT Time-Stamping policy.
- Use the service according to the specifications of ETSI EN 319 422 [5].
- Verify the electronic signature of the time stamp and verify that the certificate associated with the private key with which the TSA signs the stamp, has not been revoked.
- Check that the cryptographic summary and the policy identifier contained in the time stamp correspond to those requested.
- Store and preserve the time stamps issued by the TSA (in case the subscriber might need them in the future).

6.5.3 Obligations of third parties using time stamps

Upon receiving a time-stamp, third parties must verify the electronic signature of the time-stamp and verify that the certificate associated with the private key with which the TSA has signed the stamp, was not revoked in the moment of the time stamp generation.

6.5.4 Responsibilities of the Time-Stamping Authority

ANCERT operates its TSA in accordance with the TSA policy, its practice statement, and the terms of any other agreement between ANCERT and the subscribers of the Time-Stamping service.

ANCERT limits its responsibility to the production of time stamps under the conditions of this policy, and in no case will it accept any responsibility for the use of such time stamps.

ANCERT will not respond in cases of fortuitous event, force majeure, terrorist attack, wild strike, as well as in cases involving actions constituting a crime or offense that affect its infrastructure, unless there was a serious fault of the Time-Stamping authority. In any case, ANCERT will take all reasonable measures to mitigate the effects of such events.

7. TSA Management and operation

7.1. Introduction

This section includes security and operation controls implemented by ANCERT for the provision of the Time-Stamping service. The following sections refer to sections of the General Certification Policy [8] and, when necessary, they also complete and extend this document for the scope of the provision of Time-Stamping service.

7.2. Security management

TSA security management is described in section 5 ("Physical, management and operations security controls") of the General Certification Policy [8].

7.3. Personnel security

According to section 5.3 (“Personnel controls”) of the General Certification Policy [8].

7.4. Asset Management

ANCERT performs a proper assets management and assigns them protection measures based on their level of risk.

In particular, ANCERT has an inventory of information assets and assigns them a classification in accordance with the procedures for the classification of information and risk analysis.

All information media are managed securely in accordance with the requirements established in the information security policy. ANCERT has procedures to securely destroy information media, that may contain confidential information, when its useful life ends.

7.5. Access control

The TSA of ANCERT has appropriate access controls as defined in section 5.2. "Procedural controls" and 6.5 "Computer security controls" of the General Certification Policy [8].

7.6. Cryptographic controls

7.6.1 General

ANCERT has and implements a cryptographic security policy that regulates the use of cryptographic controls and the duration, use and protection of cryptographic keys throughout their entire life cycle.

7.6.2 TSU key generation

ANCERT generates the cryptographic keys of the TSU in a secure physical environment. Only authorized personnel (with the corresponding trusted role) can perform the key generation operation and always under dual control conditions.

ANCERT has a specific procedure for generating the TSU's keys. The execution steps of this procedure are summarized and documented in the ceremony proceedings.

The generation of the keys is performed in a cryptographic module certified in accordance either with ISO/IEC 15408 (protection profile EN 419 221-5) or the requirements of FIPS PUB 140-2 level 3.

The key cryptographic algorithm is RSA 3072 bits, and its use is limited to 5 years.

7.6.3 TSU private key protection

ANCERT guarantees the confidentiality and integrity of the TSU's private key by using a cryptographic module certified in accordance with ISO / IEC 15408 (protection profile EN 419 221-5) or complying with the requirements of FIPS PUB 140-2 level 3 for all signature operations.

The administration of the cryptographic module necessarily requires the simultaneous concurrence of two (2) cryptographic devices (out of four (4)) protected by an access code.

The password will be known only by one person responsible for that device. None of them will know more than one of the access codes.

ANCERT can back up a copy of the TSU's private key. This copy must be stored in a separate unit from the one where it is usually stored, and recovered (when needed) only by personnel subject to the personnel's trust policy. These personnel must be expressly authorized for this purpose and must be limited to those who need to do so.

The security controls to be applied to the backup copies of the TSU are of equal or superior level to those applied to the keys usually in use.

7.6.4 TSU public key certificate

ANCERT guarantees the integrity and authenticity of the public key of the TSU by means of an electronic certificate issued by ANCERT.

The TSA's certificate is published on the ANCERT website www.ancert.com .

The TSA's certificate follows the profile detailed in section 7.7.1.

7.6.5 Rekeying TSU's key

The TSA's keys are replaced either before the end of their period of use, the end of the validity period of the TSA's certificate or when it's necessary to change the algorithm or key length.

The regeneration of a new key implies the issuance of a new electronic certificate. ANCERT generates a new TSU key every 4 years.

7.6.6 Life cycle management of signing cryptographic hardware

ANCERT has an internal procedure for the management of the life cycle of the cryptographic modules, ensuring that they are not manipulated during their shipment and reception, storage, start up, and guaranteeing also their deletion when they are removed. All key management procedures

for cryptographic modules are performed by designated authorized personnel with trusted roles, under dual control, in a physically secure environment.

7.6.7 End of TSU key life cycle

ANCERT defines a period of use of the TSU's private key of 5 years. The validity period of the TSU's associated certificate is 6 years.

ANCERT does not use a TSU private key once its validity period is exceeded.

ANCERT has operational procedures to ensure that the TSU uses a new password before the previous one expires, and that it is destroyed when it reaches the end of its use.

7.7. Time-Stamping

7.7.1 Time-stamp issuance

The issuance of time-stamps is in accordance with the protocol and profile defined in ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles". [5]

Time-stamp request

The client must make the time stamp requests in accordance with the structure defined in RFC 3161 [6].

The protocol for sending the time-stamp request shall be HTTP or HTTPS in accordance with the definition in section 3.4 of RFC 3161 [6].

The cryptographic summary algorithms accepted by the ANCERT TSA are: SHA-256, SHA-512 and SHA-1. ANCERT recommends to its subscribers not to use SHA-1 as a summary algorithm, although it is maintained for compatibility reasons.

Time-stamp response

Time stamps generated by the TSA are in accordance with the profile defined in section 5.2 of ETSI EN 319 422 [5].

Time-stamps summary algorithm is SHA-256.

Time-stamps signature algorithm is *sha256WithRSAEncryption*.

Time-stamps include an extension of type *qcStatements* with the declaration *esi4-qtstStatement-1* according to section 9.1 of ETSI EN 319 422 [5] to indicate that the time stamp is qualified.

Time-stamps include the electronic certificate corresponding to the public key of the TSU.

Certificate Profile

The TSU's certificate is issued by the certification authority "ANCERT Certificados Notariales de Sistemas V2".

The profile is defined in section “Certificate of Qualified Time-Stamping Authority” of ANCERT document: "Certificate Profiles of the Certification Entity". [10]

The validity period of the certificate is 6 years. The certificate includes the extension *PrivateKey Usage Period* in order to define 5 years as the period of use for the private key.

7.7.2 Clock synchronization with UTC

ANCERT obtains the time of its systems from a connection to the Royal Navy Observatory (ROA) following the NTP protocol over the Internet.

ANCERT maintains controls to ensure that the TSU clock meets the following requirements:

- It is synchronized with UTC with the declared accuracy of 1 second.
- The calibration is maintained so that a shift in the date and time of is not expected.
- Therearecontrolstodetectchangesincalibrationand/orsynchronisationproblemsthatcancompromisethedefinedprecision.
- Drifts and jumps of the clock preventing its UTC synchronization, are detected.
- Clock synchronization is maintained when a leap second is notified by the competent entity.

If a loss of synchronization of the time source or jumps greater than the declared accuracy is detected, ANCERT will stop the issuance of time stamps.

7.8. Physical and environmental security

According to section 5.1 "Physical security controls" of the General Certification Policy [8].

7.9. Operations security

According to section 6.6 “Technical controls of the life cycle” of the General Certification Policy [8].

7.10. Network security

According to section 6.7 “Network security controls” of the General Certification Policy [8].

7.11. Incident management

According to section 5.7. “Key commitment and disaster recovery” of the General Certification Policy [8].

7.12. Collection of evidence

According to section 5.4. “Security audit procedures” of the General Certification Policy [8].

In addition to these requirements, ANCERT collects evidence of the following records:

- All events that are related to the management of the life cycle of the TSU keys and their associated certificate.
- All events related to the UTC clock synchronization of the TSU.
- All events related to the detection of synchronization loss.

7.13. Business continuity management

According to section 5.7. "Key commitment and disaster recovery" of the General Certification Policy [8].

In addition to these requirements, in case of loss or compromise of the TSU clock calibration, ANCERT will perform the following actions:

- Stop the issuance of time-stamps until the recovery from the incident.
- Notify the incident to the subscribers, third-party users of time stamps and the competent authority. In the event that before the incident was detected, time-stamps that were affected would had been issued, all parties would be informed of which the affected time-stamps are (through their serial numbers and/or their period of issue).

7.14. TSA termination and termination plans

According to section 5.8 "Termination of service" of the General Certification Policy [8].

In addition to the above requirements, when the service is ended the TSA's certificate is revoked.

7.15. Compliance

ANCERT TSA's services comply with the requirements of Regulation (EU) 910/2014. [1].

Regarding the establishment of adequate security measures to prevent unauthorized processing and confidentiality of the personal data of users, the TSA's procedures will be according to section 9.4 "Protection of personal data" of the General Certification Policy [8]