ANF AUTORIDAD DE CERTIFICACIÓN

Time-Stamping Authority Policy and Practice Statement

Paseo de la Castellana, 79 - 28046 - Madrid (España)
Teléfono: 902 902 172 (Llamadas desde España)
Internacional +34 933935 946
Fax: +34 933 031 611 · Web: www.anf.es

Security Level

Public Document

Important Notice

Address: Paseo de la Castellana, 79 – 28046 – Madrid (Spain)

Telephone: 902 902 172 (Calls from Spain) – (+34) 933 935 946 (International calls)

Fax: (+34) 933 031 611. Web: www.anf.es

Version Information

Version Control			
Date	Version	Changes	Autor
26/10/2004	1.0	Initial version	Florencio Díaz
01/05/2010	1.1	Review	Florencio Díaz
01/06/2012	1.2	Review	Florencio Díaz
02/09/2014	1.3	Review	Florencio Díaz
01/06/2016	1.4	Adaptation to eIDAS	Florencio Díaz

Important document information	
Class	Policy
Title	Time-Stamping Authority Policy and Practice Statement
Version	1.1
Author	Florencio Díaz
Responsible Auditor of the document:	Enric Castillo Mari Carmen Mateo
Filename	Time Stamping Authority Policy and Practice Statement
Creation Date	May 1st, 2010
Status	Approved
Approved on	June 1st, 2016
Approved by	Governing Board of the PKI

Index

Introduction

ANF Certification Authority (hereinafter, ANF AC) is a corporate entity, constituted under Spanish Organic Law 1/2002 of March 22nd, and registered in the Spanish Ministry of Internal Affairs with national number 171.443 and VAT number G-63287510.

ANF AC is offering trust services and related technical solutions in the EU and LATAM. These services ensure the security and verified electronic communication with public institutions, as well as with companies in their daily activities.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC establishes the possibility of acting as a Qualified Trust Service Provider (Hereinafter, eIDAS). In this regard, ANF AC is established as a Qualified Trust Service Provider.

The present document is aimed to meet the general requirements of the international community to provide trust in electronic transactions, including, amongst others, applicable requirements from Regulation (EU) No 910/2014.

Inspired by the ETSI EN 319 400 series, ANF AC has divided its documentation into three parts:

- Certification Practices Statement of ANF AC, describes general practices common to all trust services;
- The Time Stamping Authority Policy and Practice Statement describes the specific parts for providing the Time-Stamping service;
- The technical profiles are found in separate documents.

To meet these requirements, electronic information must be protected, among other things, against manipulation and loss. It is necessary to be able to assess the observation of compliance requirements in a professional environment, integrity and confidentiality are often the main criteria.

Electronic time stamps can deliver this proof of integrity in a simple manner, legally binding, permanent, inexpensive and, on request, anonymously.

The electronic time stamp are data in electronic form that link other data in electronic form with a specific time, providing evidence that this data existed at such time. Therefore, it documents the "when" and "what". An electronic signature, is often referred to as personal signature as it documents the "who" and "what". Unlike electronic signature, a time stamp is not bound to people and their actions. Thus, it can be integrated much simpler and fully automatically into electronic processes.

To verify an electronic signature, it can be necessary to prove that the signature from the signer was applied when the signer's certificate was valid. This is necessary in two circumstances:

1) *during the validity period of the signer's certificate, the signer may revoke it before the end of its validity, e.g. because the signer's private key has been compromised;*
2) *after the end of period of validity of the signer's certificate, since issuance entities are not obliged to process the revocation status information beyond the end of the period of validity of the certificates issued.*

1 Scope

The present document specifies policy and security requirements relating to the operation and management practices of the ANF AC as a Time Stamp Authority (hereinafter, ANF AC TSA) for issuing qualified electronic time stamps. These can be used in support of electronic signatures or for any application requiring to prove that a datum existed before a specific time.

The present document can be used by independent entities as the basis for confirming that ANF AC TSA is a trusted entity of the issuance of qualified electronic time stamps in accordance to eIDAS.

This document does not specify:

- protocols used to access the ANF AC TSA;
- how the requirements identified herein can be assessed by an independent entity;
- the requirements for making the information available to such independent entities;
- the requirements that must be met by such independent entities.

ANF AC issues Time-Stamping Tokens in accordance to the ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" standard.

The Root CA certificates and other necessary certificates for the functioning of this PKI are available in the following link:

In case of conflict between the CPS and the TSA CPS, the provisions of the TSA CPS shall prevail. In case of conflict between the English original document and the Spanish translation, the English original shall prevail.

2 References

2.1 Normative references

1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
2. Spanish Law 59/2003 of Electronic Signature
3. [LDP] Law on Data Protection
4. [CPS] Certification Practices Statement of ANF AC
5. IETF RFC 3161 "Internet X.509 Public Key Infrastructure Time-stamp Protocol"
6. ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
7. ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"
8. ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

2.2 Informative references

1. Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
2. IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification"
3. Terms and Conditions for time-stamping customers in www.anf.es
4. ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
5. ISO/IEC 15408 (parts 1 to 3): "Information technology – Security techniques -- Evaluation criteria for IT security".
6. FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

3 Definitions and abbreviations

3.1 Definitions

- **Coordinated Universal Time (UTC)**: Time scale based on the second as defined in Recommendation ITU-R TF.460-6. For all practical purposes, UTC is equivalent to the solar time average in the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and the solar time derived from the irregular Earth rotation. The UTC is the principal standard of the hour by which the world regulates clocks and the time.
- **NTP**: "Network Time Protocol (NTP) is a networking protocol for clock synchronization of computer systems over network packet routing with variable latency. The standard for reference is the IETF RFC 1305 (Network Time Protocol (NTP v3)).
- **Real Instituto y Observatorio de la Armada - San Fernando (Cádiz) (ROA)**: for legal purposes declared as National Standard of this unit, as well as maintenance and official dissemination of the scale "Coordinated Universal Time" (UTC(ROA)), considered for all purposes as the basis of the legal time throughout the national territory (R.D. 23 October 1992, num. 1308/1992). It is part of the BIPM laboratory network.
- **Relying party**: The recipient of a time-stamp who relies on that time-stamp.
- **Stamping Authority (TSA)**: It is the TSP providing time-stamping services using one or more time-stamping units.
- **Subscriber**: Legal or natural person to whom a time-stamp is issued.
- **Time-stamp**: Data in electronic form which binds other electronic data to a time, providing evidence that these data existed at such time.
- **Time-stamp policy**: A set of rules that indicate the applicability of a time-stamp to a community and/or class of application of the common security requirements. This is a specific type of trust service policy as defined in ETSI EN 319 421.
- **Time-stamping service:** trust service for issuing time-stamps.
- **Time-Stamping Unit (TSU)**: The set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time. .
- **Trust Service Provider (TSP)**: entity which provides one or more trust services.
- **TSA Disclosure statement**: set of statements about the policies and practices of a TSA which particularly require emphasis in the disclosure to subscribers and relying parties, for example to meet regulatory requirements.
- **TSA practice statement**: statement of the practices that a TSA employs in issuing time-stamps.
- **TSA system**: Set of IT products and components employed to provide support to the provision of time-stamping services.
- **UTC(k)**: time scale given by the laboratory "k" and which has a close relation to the UTC, with the goal to reach ±100 ns.

3.2 Abbreviations

For the purposes of the present document, the abbreviations:

BIPM Bureau International des Poids et Mesures
CA Certification Authority
IT Information Technology
TAI International Atomic Time
TSA Time-Stamping Authority
TSP Trust Service Provider

TST Time Stamp Token
TSU Time-Stamping Unit
UTC Coordinated Universal Time

4 General Concepts

4.1 Concepts and general requirements

It follows the requirements established in the CPS of ANF AC

4.2 Time-stamping services

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

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

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

4.3 Time-stamping services parties

4.3.1 Time-stamping authority (TSA)

A Trust Service Provider (TSP) providing time-stamping services to the public, is called the Time-Stamping Authority (TSA). The TSA has the overall responsibility for the provision of the time-stamping services identified in clause 4.2. The TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the TSA. The TSA responsible for issuing a time-stamp is identifiable.

ANF AC TSA hereby confirms, that the TSA is audited at least every 24 month by a conformity assessment body. The assessment report is submitted within 3 working days to the national supervisory body where the supervisory body requires the TSA to remedy any failure to fulfil requirements; the TSA will act accordingly and in a timely fashion manner. The supervisory body shall be informed of any change in the provision of the TSA.

ANF AC TSA may make use of other parties to provide parts of the time-stamping services. However, the TSA always maintains overall responsibility (as per clause 6.5) and ensured that the policy requirements identified in the present document are met.

ANF AC TSA may operate several identifiable time-stamping units.

ANF AC TSA is a qualified trust service provider as described in eIDAS which issues time-stamps.

ANF AC TSA is identified in the TSU certificated used for signing TST.

Contact Information:

ANF Autoridad de Certificación
Paseo de la Castellana, 79 – 28046 – Madrid (Spain)
Telephone: 902 902 172 (Spain) (+34) 933 935 946 (International)
Fax: (+34) 933 031 611 Web: www.anf.es

4.3.2 Subscriber

When the subscriber is an organization, it comprises several end-users or an individual end user and some of the obligations that apply to that organization must apply 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 such organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

4.3.3 TSA relying party

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

4.4 Time-stamp policy and TSA practice statement

ANF AC TSA Time-Stamping Policy is based on the Time-Stamping Policy specified in ETSI EN 319 421 and is applied to TSAs issuing TSTs.

This ANF AC TSA Practice Statement is a part of ANF AC Trust Services Practice Statement as specified in ETSI EN 319 421, applicable by ANF AC TSA as issuer of TSTs.

5 Time-stamp policies

5.1 General

ANF AC TSA issues the TST's in accordance to ETSI EN 319 421 and the Time-Stamping Policy.

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

5.2 Identification

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

1.3.6.1.4.1.18332.15.1

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) ANF Autoridad de Certificación (18333) TSA(15) CPS-PC-EU Regulation 910/2014(1)}

- Iso (1)
- Org (3)
- Dod (6)
- Internet (1)
- Private (4)
- Enterprise (1)
- ANF Autoridad de Certificación (18332)
- TSA (15)
- CPS-CP in accordance to EU Regulation 910/2014 (1)

By including this object identifier in the generated time-stamps, ANF AC TSA claims conformance to this time-stamp policy.

5.3 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 it 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.

6 Policies and Practices

6.1 Risk assessment

ANF AC TSA 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 framework of the time-stamping services, are controlled every three months to ensure their efficiency.

Detailed explanation regarding this topic is described in the security concept:
"Threat analysis and measures selection" and "Risk analysis".

6.2 Trust service practice statement

Quality Assurance is one of the most important values of ANF AC TSA. Therefore, a variety of security controls have been implemented to ensure the quality, performance and operation of the time-stamping service.

The security controls are documented and are regularly reviewed by an independent entity, with trustworthy and capable to verify the adherence of the security controls.

Additionally, to being compliant to ETSI TS 119 421, the following measures have been applied respectively in the following services.

6.2.1 Time-stamp format

The issued time-stamp token by ANF AC TSA is compliant to RFC 3161 time-stamps. The service issues time stamps with an RSA algorithm and a key length of 2048, which accept any of the following hash algorithms:

- SHA256
- SHA384
- SHA512

6.2.2 Time accuracy

The time-stamping service is in Spain, where a time signal is provided through the ROA's (Real Observatorio de la Armada) laboratory recognized by the international public entity Bureau International des Poids et Mesures (BIPM). For legal purposes, it is declared as National Standard of this unit, as well as maintenance and official dissemination of the scale "Coordinate Universal Time" (UTC(ROA)), considered for all purposes as the basis of the legal time throughout the national territory (R.D. October 23th, 1992, no. 1308/1992).

The time-stamping service using the ROA time signal, and a set of NTP servers as source of time. With this configuration, the time-stamping service reaches a precision of +/- 100 ms or superior in relation to the UTC.

6.2.3 Limitations of the service

The time stamp service of ANF AC TSA may only be used in relation to legal transactions, which value at the time of their use does not exceed Euro 500,000 in the individual case and a total of EURO 5,000,000 per calendar year.

6.2.4 Obligations of the subscribers

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

6.2.5 Obligations of relying parties

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

6.2.6 Time-stamp verification

Time-stamp verification includes the following tasks:

Task I: *Verification of the time-stamp issuer*
The issuer is a time-stamping authority that uses appropriate electronic certificates for issuing the time-stamp. The public keys of the used certificates, are included in the TSU and CA certificates, and are published to enable the verification that the time-stamp has been signed correctly by the TSA.
The certificates may be found in the following link:

www.anf.es

Task II: *Verification of the time-stamp revocation status*
An OCSP service is available to verify the revocation status of the certificates used in the time-stamp. The address for accessing the OCSP responder service is included in the certificate used to sign the time-stamp.

Task III: *Verification of the integrity of the time-stamp*
The cryptographic integrity of the time-stamp, for example the ASN.1 structure is correct, and the datum (the data that has been time-stamped) belong to the application. It can be verified through the ANF AC TSA's web service form ANF AC, that is offered free of charge in the following link: www.anf.es

6.2.7 Applicable law

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

6.2.8 Service availability

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

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

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

6.3 Terms and conditions

Within the published document "Terms and conditions for time-stamp services", it contains information about e.g. limitation of the service, subscriber's obligations, information for relying parties or limitations of liability. Additionally, the following information apply:

6.3.1 Implementation of the trust service policy

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

6.3.2 Retention time of logs

TSP event logs are retained for at least three months. Time-stamp protocols, meaning every issued time-stamp, are kept for at least 15 years.

6.4 Information security policy

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

6.5 Obligations

6.5.1 TSA obligations

The obligations of the TSA regarding subscribers and trusted third parties are specified in this document, and in the section 9.5.1 of the ANF AC CPS.

6.5.2 TSA subscribers' obligations

The general obligations specified in section 9.5.3 of ANF AC CPS apply:

- The subscriber is obligated to verify the signature of the TST and ensure that the private key used to sign the TST has not been revoked.
- The subscriber is obligated to use secure cryptographic functions for time-stamping requests.
- The subscriber is obligated to inform its end-users (e.g. Relying Parties) about the correct use of the time-stamps and the conditions of the ANF AC and ANF AC TSA.

6.5.3 TSA relying parties' Obligations

The general obligations specified in section 9.5.4 of ANF AC CPS are applicable.

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

6.6 Liability

The liability provisions are established in section 9.6, 9.7 and 9.8 of ANF AC CPS.

- The liability provisions stated in ANF AC CPS are applicable.
- The liability of ANF AC towards the subscribers is stipulated in the agreements signed with them.
- ANF AC is not liable for the mistakes in the verification of the validity of time stamps or for the wrong conclusions conditioned by omissions or for the consequences of such wrong conclusions.
- ANF AC shall assume no liability for the loss of value of the validity confirmation proof due to force majeure.

7 TSA Management and Operations

7.1 Introduction

ANF AC TSA has implemented an information security management system to maintain the security of the service.

The provision of a TST in response to a request is at the discretion of ANF AC TSA depending on the subscriber's agreement

7.2 Internal organization

ANF AC TSA's practices are described in section 9 of the ANF AC CPS.

ANF AC's organizational structure, policies, procedures and controls are applicable to ANF AC TSA.

The organizational procedures comply with the rules and regulations defined in section 2.1 of this document.

a) Legal entity
   The Time-Stamping Authority is provided by ANF AC TSA.
   ANF AC TSA, is a technology company that specializes in developing and manufacturing of intelligent, complex and secure electronic products:

   ANF Autoridad de Certificación 2016
   Paseo de la Castellana, 79 – 28046 - Madrid (Spain)
   Telephone: 902 902 172 (Spain) (+34) 933 935 946 (International)
   Fax: +34 933 031 611 Web: www.anf.es

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

7.3 Trusted personnel

The practices defined in section 5.2 and 5.3 of ANF AC CPS are applicable.

ANF AC TSA has understood that talented and motivated employees are a key factor for the success of the business. Therefore, the hiring practices are a very important process in the organization. Only well-educated, with respect to their job role, and trustworthy personnel fulfil operations of the time-stamping service.

The "role" concept enforces the segregation of duties to ensure that only entitled personnel perform the important operational tasks.

Before personnel is appointed to trusted roles, ANF AC verifies that the necessary knowledge is possessed, or it is transferred via training courses and that they have passed the necessary tests proving the acquisition of knowledge.

ANF AC personnel is free from conflict of interests that might prejudice the impartiality of the ANF AC TSA operations.

7.4 Asset management

The practices identified in section 5, 6.4 and 6.5 ANF AC CPS are applicable.

All IT systems used within the service are clearly identified, categorized and filed in an asset management database.

All media is handled securely.

Data from disposed media is securely deleted, either by an electronic erase of the data or by physically destroying the disposed media.

7.5 Access control

The practices identified in section 6.4 and 6.5 of ANF AC CPS are applicable.

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

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

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

7.6 Cryptographic controls

7.6.1 TSU's key generation

The key generation practices described in section 6.1 and 6.2 of ANF AC CPS are applicable.

Personnel restrictions described in section 5.2 and 5.3 of ANF AC CPS are applicable.

The TSU uses a RSA key pair with a length of 2048-bit. This key pair is used only for signing TSTs.

All cryptographic modules are associated with the same public key certificate.

a) The generation of the TSU's signing key(s) is undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3), under at least, the control of two trusted personnel. The personnel authorized to carry out this function is limited to those required to do so under the TSA's practices.
b) The generation of the TSU's signing key(s) is carried out within a cryptographic module which is conformant to FIPS PUB 140-2 [I.9], level 3, or ISO 15408 Common Criteria EAL 4+.
c) The TSU key generation algorithm, the signature algorithm, the length of the key used to sign the time-stamps, is recognized by the national supervisory entity and by the current technical state of art as being fit for the signing of time-stamps issued by the TSA.

7.6.2 TSU's key protection

The practices of TSU key protection, storage, backup and recovery, described in section 6.2 and 6.3 of ANF AC CPS are applicable.

The TSU's private key shall be backed up and stored safely for the unlikely event of key loss due to unexpected power interruption or hardware failure.

A key backup shall be obtained in the Keys Generation Ceremony. The backup of the private key is kept in secret and its integrity and authenticity is preserved in a safe box.

7.6.3 Public key certificate

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

a) TSU signature verification (public keys) are available to relying parties that trust in a public key certificate. The certificates are published in the following link:

www.anf.es

b) The TSU does not issue a time-stamp before its signature verification (public key). When the certificate is loaded in the TSU, the TSA verifies that the certificate was duly signed (including verification of the certificate chain of a trusted certification authority).
c) Only one TSU certificate with its private key is issued.
d) TSU certificates are not renewed.
e) Validity information regarding the TSU certificates is updated periodically and the CRLs or OCSP services are available with the references located in the certificates.

7.6.4 TSU's key renewal

The life-time of the TSU certificate corresponds to the period of the chosen algorithm and the key length (see clause 7.6.1c).
The keys of the TSU shall have a maximum operating life of 5 years. A certificate can be issued for all expected lifetime. The duration of the TSU class is limited by:

- The period of validity of the root issuer entity certificate.
- Once a year or when significant changes occur, the person holding the function "Cryptography Supervisor" verifies all cryptographic algorithms used in the TSA checking that each algorithm is recognized as suitable, as indicated in clause 7.6.1c).
- If an algorithm enters a situation of risk it shall no longer be considered as adequate; the Security Manager shall instruct the TSA the cease of usage of the affected keys and load new keys.

7.6.5 Life cycle management of cryptographic hardware

The practices of the management of the HSM life cycle are described in section 6.2 of ANF AC CPS.

The used cryptographic hardware is inspected by trustworthy personnel (in the presence of two persons) during shipment and storing. Specifically, the hardware is verified for

a) Any damages of security seals
b) Any damages of the case of the hardware (e.g. scratches, bumps…)
c) Any damages of the packing of the hardware

The inspection is protocolled.

Additionally, the following applies:

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

7.6.6 End of TSU's key life cycle

After expiration of the private keys, the private keys within the cryptographic module are destroyed in a way the private keys cannot be retrieved.

The "Cryptography Supervisor" defines the key validity in accordance to clause 7.6.1c).

7.6.7 Root certification authority

ANF AC TSA operates an own Public Key Infrastructure consisting of a "Root Certification Authority" and an OCSP Responder service.

The Root CA is operated offline, all the aspects related to physical and technical security are detailed in the ANF AC CPS, published in public and free access repositories:

www.anf.es

7.7 Time-stamping

7.7.1 Time-stamp issuer

ANF AC TSA offers time-stamping services using RFC 3161 "Time Stamp Protocol (TSP)". The service URL is specified in the subscriber's agreement. Each TST contains the Time-Stamping Policy identifier, a unique serial number and a certificate containing the identification information of the ANF AC TSA`s TSU.

The TSU, in the time-stamp requests, accepts SHA256, SHA384, SHA512 hash algorithms and uses the SHA-256 cryptographic hash function to sign TST.

The TSU keys are 2048-bit RSA keys. The key is used only for signing TSTs.

TSA logs all issued TSTs. The TSTs are logged for an indefinite period. ANF AC TSA can prove the existence of a TST at the request of a relying party. ANF AC TSA can request the relying party to cover the costs of such service.

The TSU does not issue any TST when the end of the validity of the TSU private key has been reached.

7.7.2 Clock synchronization with UTC

ANF AC ensures that its clock is synchronized with UTC [ROA] within an accuracy of 1 second or better, using the NTP protocol.

ANF AC monitors its clock synchronization and ensures that, if the time indicated in a TST drifts or jumps out of synchronization with the UTC, this is detected. In case the TSA clock drifts out of accuracy, no time-stamp shall be issued until the clock is synchronized.

Specifically, the following topics are covered:

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

7.8 Physical and environmental security

The practices identified in section 5.1 and 6.5 of ANF AC CPS are applicable.

A highly secured physical environment is necessary. This physically secured environment houses the TSA.

The time-stamping management facilities are operated in an environment that protects physically and logically the transaction services with controls of unauthorized access to systems or data. Each entry in the physically secure area is subjected to independent monitoring of the TSA. In the security area, the person who accesses the facilities is accompanied, registering the identity, entry and exit time.

Physical protection is achieved through the creation of clearly defined security perimeters (e.g. physical barriers) around the time-stamping management.

Physical and environmental security controls protect the facility that houses system resources.

The TSA's physical and environmental security policy, for systems concerning with the time-stamping management, addresses the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

Physical and organizational controls protect against external access to information, media and software relating to the time-stamping services.

7.9 Security of operations

The practices identified in section 6.3, 6.4 and 6.5 of ANF AC CPS are applicable.

ANF AC TSA has implemented a mature system of system and security controls to ensure service quality and availability. These controls are:

a) An analysis of security requirements is carried out on the design specifications and the requirements for any stage of the systems development project undertaken by the organization or on behalf of the TSP to ensure that security is built into the information technology's systems.
b) As a change control procedure, version control is applied for modifications and corrections of the software.
c) The integrity of TSP’s systems and information is protected against viruses, malicious and unauthorized software.
d) The means used within the TSP systems are secure and protect against damage, theft, unauthorized access and obsolescence.
e) Within the period in which records need to be retained, the media management procedures protect against obsolescence and deterioration of the means of telecommunication.
f) Application of appropriate procedures for all administrative functions of trust and that have an impact on service delivery.

g) The TSP has specified and applied procedures for ensuring that security patches are applied within a reasonable time after they have become available. A security patch does not need to be applied if it introduces additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. The reason for not applying any security patches shall be documented.

7.10 Network security

The practices identified in section 6.5 of ANF AC CPS apply. The TSP protects its network and systems from attacks:

a) The TSP network is segmented into networks or zones based on risk assessment considering the functional, logical, and physical (including location) relationship between trustworthy systems and services.
b) The TSP restricts access and communications between zones to those necessary for the operation of the TSP. No connections are needed and services are explicitly forbidden or deactivated. The established rule set is reviewed on a regular basis.
c) All the elements of the TSPs critical systems (e.g. Root CA systems, TSU) are kept in a secured zone.
d) A dedicated network for administrating the IT systems, that is separated from the operational network, is established. Systems used for administration shall not be used for non-administrative purposes.
e) The test platform and the production platform are separated. The test platform is found in an environment not concerned with live operations (e.g. development).
f) Communication between the different trustworthy systems can only be established through trusted channels that are logically distinct from other communication channels, and provide an assured identification of its end points and protection of the data from modification or disclosure.
g) The external network connection to the internet is redundant to ensure availability of the services in case of a single failure.
h) The TSP performs a regular vulnerability scan on public and private IP addresses identified by the TSP, the vulnerability of each analysis is performed by a person or entity with the skills, tools, proficiency, code of ethics and independence necessary to provide a reliable report.
i) The TSP, after configuring the infrastructure with updates or modifications that the TSP considers relevant, it performs a penetration test in the systems.
j) The TSP obtains evidence records that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

7.11 Incident management

The practices identified in section 4.15 of ANF AC CPS are applicable. Further information can be obtained in the document "Process management of incidents".

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

a) Monitoring activities take account the sensitivity of any information collected or analyzed.
b) Abnormal system activities that indicate a potential security violation, including intrusion into the TSP network, are detected and reported as alarms.
c) The TSP IT systems monitor the following events: Start-up and shutdown of the logging functions; availability and utilization of the needed services with the TSP network.

d) The TSP acts in a timely and coordinated manner to respond quickly to incidents and to limit the impact of security breaches. The TSP appoints trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.
e) The TSP notifies the corresponding parties, in line with the applicable regulatory rules of any security breach or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.
f) The national supervisory body is informed within 24h after the discovery of a critical security breach.
g) Audit logs are monitored or reviewed regularly to identify evidence of malicious activity.
h) The TSP shall resolve critical vulnerabilities within a reasonable period after their discovery. If this is not possible the TSP will create and implement a plan to mitigate the critical vulnerability or the TSP will document the factual basis for the TSP's determination that the vulnerability does not require remediation.
i) Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimized.

7.12 Collection of evidence

The practices identified in section 4.12 of ANF AC CPS are applicable.

At the time a security incident becomes detected, it might be not obvious, if that security incident is subject of further investigations. Therefore, it is important, that any proof, the status of IT system or information is securely saved before they become unusable or destroyed.

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

a) The confidentiality and integrity of current and archived records concerning operation of services is maintained.
b) Records concerning the management of services are confidential and filed in accordance with described business practices.
c) Records concerning the management of services, if necessary, are made available for the purposes of providing evidence of the correct operation of the services for legal proceedings.
d) The TSP registers in the precise moment, the significant environmental events, key management and clock synchronization. The time used to record events, as required in the audit log, is synchronized with the UTC continuously.
e) Records concerning services are held for a period after the expiration of the validity of the signing keys or of any service token to provide trust for the necessary legal evidence in accordance to the present document.
f) The events are logged in a way that they cannot be deleted or destroyed (except if they can be reliably transferred to long-term media).

7.13 Business continuity management

The practices identified in section 4.15 of ANF AC CPS are applicable.

Backups of the databases of all issued TSTs by ANF AC TSA are kept in an off-site storage.

If the TSU private key is compromised or suspected to be compromised, ANF AC TSA shall inform Subscribers and Relying Parties and shall stop using the compromised key.

In case of revocation of the TSU certificate, the necessary actions shall be performed in accordance to the decision of the Crisis Committee and the Recovery Plan.

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

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

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

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

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

- Notify the Security Manager for him to coordinate the measures to be taken.
- Start a security audit of the remaining private keys (integrity checks, log file analysis).
- Notify the incident to relying parties.
- Start the substitution procedure to return to a N+1 redundancy. In case of natural disasters (e.g. fire, earthquake, storm), if it causes a loss of the facility, the time-stamping service could become suspended until the facility is rebuilt and it has been evaluated by an independent entity. The loss of calibration or clock synchronization of a TSU is covered in clause 7.7.1 of this document.

7.14 TSA termination and termination plans

The practices identified in section 4.16 and 4.17 of ANF AC CPS are applicable. Additionally:

- In the event the TSA terminates its operations for any reason whatsoever, it shall notify the national supervisory entity prior to termination.
- A timely notice shall be provided to all relying parties to minimize any disruptions that are caused because of the termination of the services.
- Furthermore, in collaboration with the supervisory entity, the TSP shall coordinate the necessary measures that ensure retention of all the relevant archived records prior to termination of the service.
- Moreover, the following applies:
    a) The TSP maintains an up-to-date termination plan.
    b) Before the TSP terminates its services, at least the following procedures apply:
        i. the TSP shall inform the following of the termination: all subscribers and other entities with whom the TSP has agreements or other form of established relations. This information shall be made available to other relying parties;
        ii. TSP shall terminate the authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens;
        iii. the TSP shall transfer to a reliable entity, for a reasonable time, its obligations of maintaining all necessary information to provide evidence of the operations of the TSP, unless it can be demonstrated that the TSP is not the owner of such information;
        iv. The TSP private keys, including backup copies, shall be destroyed, or withdrawn from use, in a way that the private keys cannot be retrieved.
        v. ANF AC TSA takes the necessary steps to have the TSU certificates revoked.
        vi. When possible, the TSP shall use a system that allows the transfer of the services provided to its client to another TSP.

c) The TSP has an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons by which the TSP is unable to cover the costs by itself, to the possible extent, within the constraints of the applicable legislation regarding bankruptcy.
d) The TSP shall maintain or transfer to a reliable entity its obligations of making its public key or trust service tokens available to relying parties for a reasonable period.

7.15 Compliance

ANF AC TSA ensures compliance with applicable law at all times.

Specifically, it is compliant to:

a) Regulation (EU) N°910/2014
b) Spanish Law 59/2003, of December 19th, on electronic signature.
c) ETSI TS 119 421
d) IETF (RFC 3161)

Validation of the compliance with these regulations is performed during the conformity assessment as described in section 8 of ANF AC's CPS.