TSA Practices Statement and

Timestamping Policy

Paseo de la Castellana,79 -28046- Madrid (Spain)

Telephone: 902 902 172 (Calls from Spain)

International +34 933 935 946

Website: 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) International (+34) 933 935 946

Website: www.anf.es

INDEX

1. Introduction

1.1. Overview

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.

A time stamps allows to demonstrate that data existed before a specific time. This technique allows proving that the signature or a specific electronic document to which it is associated was generated before the date contained in the time-stamp.

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, certified for the provision of the time-stamping service.

The present document specifies policy and security requirements relating to the operation and management practices of the ANF AC as a **Time-Stamping Authority** (hereinafter, ANF AC TSA) for issuing **qualified electronic time stamps**, as well as establish the conditions of use, obligations and responsibilities of the different entities involved.

ANF AC's TSA is in conformity to:

- Regulation (EU) 910/2014 (eIDAS), article 42. It collects and regulates the issuance of time stamps, defining them as "means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time."
- Spanish Law 6/2020, of november 11th, regulating certain aspects of electronic trust services.
- ETSI EN 319 421: *"Policy and Security Requirements for Trust Service Providers issuing Time-Stamps."*
- ETSI EN 319 422: *"Time-stamping protocol and time-stamp token profiles."*
- ETSI EN 319 401: *"Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"*
- ETSI TS 119 312: *"Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"*
- IETF RFC 3161 *"Internet X.509 Public Key Infrastructure Time-stamp Protocol"*

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.

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 Regulation.

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.
- the requirements for the custody of evidence, qualified long-term preservation of qualified signatures and seals.

ANF AC will not carry out custody of evidence and qualified long-term preservation unless the corresponding qualified service is contracted.

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

In case of conflict between the CPS and the TSA CPS, the provisions of the TSA CPS shall prevail. In addition, this document is published in Spanish and English versions, in case of conflict the Spanish version will prevail.

1.2. Name of the document and identification

Name of the document	TSA Practices Statement and Timestamping Policy		
Version	1.6		
OID	1.3.6.1.4.1.18332.15.1		
Approval date	02/04/2021	**Publication date**	02/04/2021

1.2.1. Reviews

Version	Changes	Approval	Publication
1.6.	Review and inclusion of TSU.	02/04/2021	02/04/2021
1.5.	Recommendation from eIDAS auditor	18/04/2017	18/04/2017
1.4.	Adaptation to eIDAS	01/06/2016	01/06/2016
1.3.	Review.	02/09/2014	02/09/2014
1.2.	Review.	01/06/2012	01/06/2012
1.1.	Review.	01/05/2010	01/05/2010
1.0.	Initial version of the document.	26/10/2004	26/10/2004

1.3. Definitions and acronyms

1.3.1. Definitions

For the purposes of the present document, the definitions given in ANF AC CPS and the following apply:

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.

Hash function: it is an operation that is performed on a data set of any size, so that the result obtained is another data set of fixed size, regardless of the original size, and that has the property of being uniquely associated with the data initials.

Hardware Security Module (HSM): device certified in accordance with the provisions of ETSI EN 319 421, used to perform cryptographic functions and store keys in secure mode.

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.[1]

Relying party: The recipient of a time-stamp who relies on that time-stamp.

TimeStamping Authority (TSA): TSP providing time-stamping services using one or more time-stamping units (TSUs).

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 establishing evidence that these data existed at that 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.

[1] *ROA collaborates with the Higher Council for Scientific Research (CSIC), controlling and monitoring the synchronization of the main time distribution machines in Spain, three of which (two located at INSOB and a third in Madrid) belong to the Section.* *https://armada.defensa.gob.es/ArmadaPortal/page/Portal/ArmadaEspannola/ciencia_observatorio/prefLang-es/06_Hora*

TSA system: composition of IT products and components organized to support 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.

1.3.2. Acronyms

For the purposes of the present document, the following abbreviations apply:

BIPM Bureau International des Poids et Mesures

CA Certification Authority

HSM Hardware Security Module

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

1.4. Contact information

Department	Legal Department
Email 1	soporte@anf.es
Email 2	mcmateo@anf.es
Address	Paseo de la Castellana, 79
Locality	Madrid
Postal code	28046
Telephone number	932 661 614 (Calls from Spain) International (+34) 933 935 946

2. General concepts

This document refers to ANF AC CPS for the generic policy requirements established in ETSI EN 319 401, common for its trust services.

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.

2.1. TimeStamping 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 Practices Statement.

ANF AC TSA adheres to the standards and regulations established in section 1.1 of this document to keep trustworthiness of the time-stamping services for subscribers and relying parties.

2.2. TimeStamping service participants

2.2.1. Qualified Trust Services Provider (QTSP)

ANF AC is the Trust Service Provider (TSP) that provides time stamping services to the public, in the provision of time stamping services it intervenes as Time Stamping Authority.

ANF AC TSA is a Qualified Trust Services Provider (QTSP) as described in the eIDAS Regulation, it is included in the Spanish TSL.

ANF AC does not rely on third-party collaborating entities for the provision of time stamping services, it maintains general responsibility and ensures that the performance requirements mentioned in this document are met.

2.2.2. TimeStamping Authority (TSA)

The TSA has the overall responsibility for the provision of the time-stamping services and for the operation of one or more TSUs which creates TSTs.

The qualified electronic time stamping service is audited at least every 24 months by a conformity assessment body, delivering the assessment report to the Supervisory Body within a maximum period of 3 business days. When the supervisory body requires the TSA to remedy any breach of the requirements, the TSA shall act accordingly and in due course. The control body shall be informed of any changes to the TSA provision.

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

The TSA may operate several identifiable time-stamping units. ANF AC TSA is identified in the TSU certificated used for signing TST.

2.2.3. Subscriber

The subscriber is a legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.

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.

2.2.4. TSA Relying party

A relying party is an individual or entity that acts in reliance of a TST generated under ANF AC's TSA Practices Statement and Timestamping Policy. A Relying Party may, or may not also be a subscriber.

3. Time Stamping Policy

3.1. General

ANF AC TSA issues the TST's in accordance to ETSI EN 319 421 y ETSI EN 319 422. ANF AC TSA only issues qualified electronic time-stamps. This TSU do not issue non-qualified electronic time-stamps.

Each TSU is uniquely identified by being associated with a public key certificate which uses a different subject name, using a sequential number.

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

3.2. Identification

The identifier of the Qualified Electronic Time Stamping Policy, specified in this document is:

OID 1.3.6.1.4.1.18332.15.1

To indicate that the time stamp is qualified, then the "Policy" field in the TSTInfo of the time stamp shall incorporate one of the following OIDs:

- 1.3.6.1.4.1.18332.15.1. Corresponding to this TSA Practice Statement and TimeStamping Policy, or
- 0.4.0.2023.1.1. Corresponding to best-practices-ts-policy defined in section 5.2. of ETSI EN 319 421

4. Policies and Practices

4.1. Risk Assessment

ANF AC TSA conducts risk assessments on a regular basis to ensure the quality and reliability of timestamping services. In order to ensure its effectiveness, there are safeguard measures and security controls that are defined in a security framework appropriate to the provision of the time stamp service. With a minimum annual periodicity, and whenever there is a change in the infrastructure or procedures, a review of the security policies is carried out and an audit is carried out against the international ISO and ETSI standard.

4.2. 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.

4.2.1. 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 minimum key length of 2048 bits, which accept any of the following hash algorithms:

- SHA256
- SHA384
- SHA512

4.2.2. 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.

4.2.3. Limitations of the service

ANF AC is responsible for the variation of the time reference, in relation to the time provided by the service of the Royal Institute and Observatory of the Navy, included in the qualified electronic time stamp at the time of the request, but in no case of the veracity nor content of the electronic data sent by the subscribers of the service, which are the object of the electronic time stamp issued.

ANF AC will not respond to subscribers or trusting third parties, whose behavior in the use of the qualified electronic time stamping service has been negligent, the failure to observe the provisions herein should be considered for these purposes and in any case as negligence. Statement of Practices and Time Stamping Policy,

in the Service Contract, in the Terms and Conditions, and especially in the provisions of the sections referring to the obligations and responsibility of the subscribers and the relying parties.

ANF AC does not guarantee the cryptographic algorithms nor will it be liable for damages caused by successful external attacks on the cryptographic algorithms used, especially if it has kept due diligence according to the current state of the art, this document and its addendum, and what is established in the eIDAS Regulation and Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

ANF AC will not be liable for any software that it has not provided directly.

ANF AC will not respond in cases of fortuitous event, force majeure, terrorist attack, strike, social riots, as well as in cases involving actions constituting a crime or misdemeanor that affect its infrastructure.

The amount that for damages that should be paid by judicial imperative, ANF AC to each injured third party or member of the Electronic Community in the absence of specific regulation in the contracts or agreements, is limited to a maximum of FIVE THOUSAND EUROS (€ 5,000).

4.2.4. Time-stamp verification

The subscriber and the third party who trusts, the prior to placing their trust in the electronic time stamp, must proceed to its verification in accordance with the provisions of clause 6.7.5 "Validation of Time Stamp" of this document.

4.2.5. Applicable law

- Regulation (EU) 910/2014 (eIDAS), article 42.
- Spanish Law 6/2020, of november 11th, regulating certain aspects of electronic trust services..

4.2.6. 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 guarantee the availability of the ANF AC TSA service, an annual availability of 100% cannot be guaranteed. ANF AC TSA aims to provide an annual service availability of 99%, and assumes with its subscribers Service Level Agreement (SLA - Service Level Agreement) published at, http://www.anf.es

4.3. Terms and condition

Within the published document *"Terms and Conditions for ANF AC eIDAS services" (OID 1.3.6.1.4.1.18332.5.1.3)* published at https://www.anf.es/en/repositorio-legal/, 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:

4.3.1. Implementation of the trust service policy

The present document informs about the applicable trust service policy. See chapter 5 for further information regarding the scope of the obligations and responsibilities of the parties.

4.3.2. 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.

4.4. 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.

5. Obligations and liability

5.1. TSA obligations (ANF AC)

5.1.1. Obligations

ANF AC, acting as Time Stamping Authority (TSA), undertakes to:

- Respect the provisions of this TSA Practice Statement and Time Stamp Policy.
- Protect its private keys safely.
- Guarantee that its clock is synchronized with UTC within the stated accuracy of one (1) second using NTP.
- Supervise the synchronization of its clock and guarantees that, if the time indicated in a TST drifts or goes out of synchronization with UTC, such a case is detected.
- In case the TSA clock is derived from accuracy, no time stamps will be issued until the clock is synchronized.
- The time stamping service is located in Spain, where a time signal is provided through the ROA (Royal Observatory of the Navy), a laboratory recognized by the international public body Bureau International des Poids et Mesures (BIPM).
- Declared for legal purposes as National Pattern of said unit, as well as the maintenance and official dissemination of the "Coordinated Universal Time" (UTC (ROA)) scale, considered for all purposes as the basis of legal time throughout the national territory (RD 23 October 1992, no. 1308/1992)
- The timestamp service uses this ROA timestamp, and a set of NTP servers as time sources. With that configuration, the timestamp service achieves an accuracy of +/- 100 ms or better relative to UTC.
- Log records are retained for at least three (3) months. Time stamp protocols, which means each time stamp issued, is kept for at least fifteen (15) years.
- ANF AC will inform all Subscribers before ANF AC stops providing the time stamp services and will maintain the documentation related to the completed services and the necessary information in accordance with the processes established in the CPS ANF AC TSA.

5.1.2. 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.
- ANF AC, to face the risk of liability for damages that may be caused by the time stamp service, has subscribed the corresponding civil liability insurance, and has increased the amount required by current legislation, up to the amount of FIVE MILLION EUROS (€ 5,000,000)
- The liability of ANF AC towards the subscribers is stipulated in the agreements signed with them.
- The provisions on liability defined in the CPS of ANF AC apply, especially in sections 9.6, 9.7 and 9.8.
- The service limitations and liability disclaimer established in this document apply.

5.1.3. Disclamer of liability

ANF AC will not be responsible for:

- Errors in verifying the validity of time stamps or erroneous conclusions conditioned by omissions or by the consequences of such erroneous conclusions.

- Non-compliance with their obligations if said non-compliance is due to failures or security problems of the supervisory body *(Ministerio de Industria, Energía y Turismo)*, the data protection supervisory authority *(Agencia Española de Protección de Datos)*, the Trust List or any other public entity.
- Non-compliance if said non-compliance was caused by force majeure.
- Due to the interruption of the service in compliance with section 7.7.2. of ETSI EN 319 421, whereby if ANF AC TSA detects that the time to be entered in a time stamp deviates or loses synchronization with UTC, it is obliged to stop the broadcast. When the service shutdown is carried out in compliance with said rule, the subscriber will not have the right to claim.
- The Subscriber, with the acceptance of the time stamp, exempts ANF AC from all responsibility, and in particular, undertakes to hold ANF AC harmless from any damage arising from any action or omission that results in liability, damage or loss, expense. of any type, including judicial and legal representation that may be incurred, due to the publication and use of the time stamp, when any of the following causes concur:
- Falsehood or erroneous manifestation made by the user of the time stamp.
    i. Error by the user of the time stamp when providing the request data, if in the action or omission he mediated fraud or negligence with respect to ANF AC, the registration entity or any Relying Party that trusts the time stamp.
    ii. Negligence in the protection of the private key, in the use of a reliable system or in maintaining the necessary precautions to avoid the compromise, loss, disclosure, modification or unauthorized use of said key.
    iii. Use by the Subscriber of a name, or other information in the certificate, that infringes the intellectual or industrial property rights of third parties.
    iv. Improper use of the private key of the certificate, for operations that are not authorized in it.
    v. Failure to pay the fees for issuance, renewal, payment of the Cryptographic Device, electronic signatures or any other that the subscriber has contracted.
- The Relying Parties who relies on the certificate undertakes to hold ANF AC harmless from any damage arising from any action or omission that results in liability, damage, loss or expense of any kind, including judicial and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes concur:
    i. Breach of the obligations of the third party who trusts the certificate.
    ii. Reckless reliance on a time stamp, depending on the circumstances.
    iii. Failure to verify the status of a certificate, to determine that it is not suspended or revoked.
    iv. Verification of the certificate using devices not approved by ANF AC.
    v. Do not use the signature re-marking service when any of the cryptographic components is at risk in accordance with the publication that ANF AC makes on the Website for this purpose.

5.2. Subscriber / Customers obligations

The general obligations specified in this document and in clause 9.5.3 of the CPS ANF AC are applicable:

- The subscriber is obliged not to use ANF AC's qualified electronic time stamping service, until the corresponding service use contract has been formally signed. Having an ANF AC time stamp

consumption client program, or even having access control credentials to the service does not give you the right to use it.

- The subscriber will respect what is established in the CPS of ANF AC and in this document, as well as what is agreed in the contractual documents and, especially, the Terms and Conditions of ANF AC.
- The subscriber is obliged to:
    - verify the signature of the TST,
    - that the signature has been prepared with a TSU certificate from ANF AC, and
    - check that the certificate used to sign the TST was valid.
- To perform these checks, a qualified signature service and qualified electronic stamps must be used.
- The subscriber must take the necessary measures to guarantee the validity of the TST beyond the lifetime of the certificates used by ANF AC TSA.
- If the subscriber does not use an ANF AC timestamp client, they will need to verify that the hash contained in the timestamp matches the hash sent in their TST request.
- If the subscriber does not use an ANF AC timestamp client, the subscriber is obliged to use the secure cryptographic functions for timestamp requests.
- The subscriber is obliged to verify the veracity and content of the electronic data sent to the electronic time stamp of ANF AC.
- If the subscriber has not contracted the service for the custody of evidence and long-term preservation of electronic signatures and seals, the storage and conservation of the time stamps issued by the TSA is the responsibility of the subscriber.
- The subscriber is obliged to inform his end users (for example, trusting third parties) about the correct use of time stamps and the conditions of ANF AC and ANF AC TSA.
- The subscriber will not use electronic time stamps as a temporary reference outside of the limits established for them in their corresponding policy.

5.3. Relying parties obligations

The general obligations specified in this document and in clause 9.5.4 of the CPS ANF AC are applicable:

- Relying parties who trust before placing their trust in an ANF AC electronic time stamp (TST) must:
    - check the correspondence of the TST with the electronic data to which it is associated,
    - verify that the TST has been signed with the corresponding key of the certificate of the TSU of ANF AC, and
    - that the certificate used to sign the TST was current.
- To perform these checks, a qualified signature service and qualified electronic seals must be used.
- Trusting third parties must take the necessary measures to guarantee the validity of the TST beyond the lifetime of the certificates used by ANF AC TSA.
- They must take into account any limitation of use in accordance with the policy indicated on the time stamp.
- Trusting third parties will not enforce electronic time stamps as a temporary reference outside of the limits established for them in their corresponding policy.
- They must take into account any other obligation prescribed in this Statement of Practice and its addendum, as well as in the Terms and Conditions corresponding to the electronic time stamping service.

6. TSA Management and operations

6.1. 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.

6.2. 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 1.1 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
   - Paseo de la Castellana, 79 – 28046 - Madrid (Spain)
   - Telephone: +34 932 661 614 (Spain)
   - (+34) 933 935 946 (International)
   - 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.

6.3. 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.

6.4. 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.

6.5. 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.

6.6. TSA Certificate *(TSU)*

ANF AC has and follows procedures that guarantee the cryptographic security of the service, these practices are documented in "Controls of Cryptographic Security CA - TSA" OID: 1.3.6.1.4.1.18332.57.1.2

TSA Certificates are not renewed.

6.6.1. TSA Key Generation

The TSA (TSU) private keys are generated and kept in a secure cryptographic device (HSM) that meets the requirements detailed in FIPS 140-2 level 2 or higher, or with an EAL level 4+ or higher according to ISO / IEC 15408, not being imported to other cryptographic modules.

The generation of the TSU's signing key(s) is undertaken in a physically secured environment (as per clause 5.8 of this document) by personnel in trusted roles (as per clause 5.3 of this document), under at least, the control of two trusted personnel. This key pair is used only for signing TSTs.

RSA algorithm with a minimum key length of 2048 bits. The certificates will have a duration appropriate to the cryptographic security in accordance with the recommendations published in ETSI TS 119 312, counting from the moment the validity period of the associated certificate begins.

Each Timestamp Unit will l have a single time-stamp signing key active at a time.[2]

In the use of time stamps for high-level procedures of the Esquema Nacional de Seguridad (National Security Scheme), the indications of the security standard CCN-STIC-807 will be followed.

6.6.2. 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.

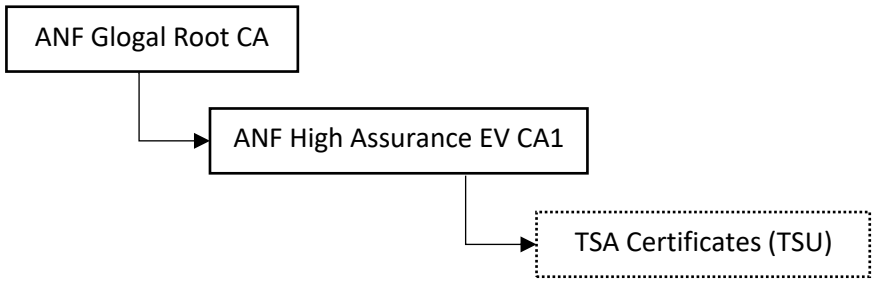
The private key of the TSU is protected in an HSM cryptographic module certified in ISO 15408, Common Criteria EAL 4+.

Copies of the private key of the TSU are not made.

6.6.3. TSA Certificate Disclosure

Electronic Time Stamps issued under this policy are signed by specific certificates, which in turn have been issued under the Certification Chain of the root Certification Authority with CN = ANF Global Root CA

The TSA service certificate is attached to the response of each timestamp that is issued and is published at https://www.anf.es/certificados-ca-raiz/



Certification Authority Root Certificate (Root CA), **ANF Global Root CA**:

ANF Global Root CA *(expires **2036**)*			
Subject	CN = ANF Global Root CA	**Serial number**	01 64 95 ee 61 8a 07 50
	SERIALNUMBER = G63287510		
	O = ANF Autoridad de Certificación	**Public Key**	RSA (4096 Bits)
	C = ES	**Signature Algorithm**	Sha256RSA
Validity period	From 2016-05-20 to 2036-05-15		
Fingerprint SHA-1	FC9843CC9922615001A17374CE8A3D79580FEA51		
Fingerprint SHA-256	E0AFBD2C0EE95A68CD9A3C590B2D3FE07C0A6D0BE796AE5291E424D47792178E		

Certification Authority Intermediate Certificate (Root CA), **ANF High Assurance EV CA1**:

ANF High Assurance EV CA1

[2] ETSI EN 319 421 section 7.6.2. f)

Subject	CN = ANF High Assurance EV CA1	**Serial number**	06 5d 66 65 46 a4 59 00
	SERIALNUMBER = G63287510	**Public key**	RSA (4096 Bits)
	OU = ANF Autoridad Intermedia Tecnicos		
	O = ANF Autoridad de Certificación	**Signature algorithm**	Sha256RSA
	C = ES		
Validity period	From 2016-05-20 to 2026-05-18		
Fingerprint SHA-1	67939B3CA77E5F6FDEC07EC96371A87C77197962		
Fingerprint SHA-256	1C28A8C009F25850B9155533D4A9A14C534B24DA84756E82D6150B5062D63704		

The Qualified Time Stamping service will use the following TSU certificates to provide the service::

ANF Qualified Time-Stamping Unit 1360			
Subject	CN = ANF Qualified Time-Stamping Unit 1360	**Serial number**	996112230137107613581495663
	OI = VATES-G63287510	**Public key**	RSA (2048 Bits)
	OU = TSU		
	O = ANF Autoridad de Certificación	**Signature algorithm**	Sha256RSA
	C = ES		
Certificate Policy	1.3.6.1.4.1.18332.15.1		
Validity period	Valido desde el 2021-04-15 hasta el 2025-04-14		
Private key use period	2024-04-14		
Fingerprint SHA-1	05:D6:BC:52:B9:81:73:4C:90:3A:7A:F8:0A:D3:1D:82:93:EE:76:11		
Fingerprint SHA-256	2E:C5:A6:1B:5D:77:2E:10:9F:BB:76:A1:D6:6C:0F:B2:C6:06:A2:A2:34:BF:9D:F3:A0:97:B8:5E:AA:65:09:24		

ANF Qualified Time-Stamping Unit 1361			
Subject	CN = ANF Qualified Time-Stamping Unit 1361	**Serial number**	996750780693200761702941647
	OI = VATES-G63287510	**Clave Pública**	RSA (2048 Bits)
	OU = TSU		
	O = ANF Autoridad de Certificación	**Algorítmo defirma**	Sha256RSA
	C = ES		
Certificate Policy	1.3.6.1.4.1.18332.15.1		
Validity period	Valido desde el 2021-04-15 hasta el 2025-04-14		
Private key use period	2024-04-14		
Fingerprint SHA-1	34:4E:E2:0D:ED:5F:E7:5A:37:A6:2C:A5:69:84:39:07:68:27:FB:3F		
Fingerprint SHA-256	92:3F:7F:DD:D5:A0:EB:17:B4:C2:4A:48:27:D1:AD:F5:BA:BF:D3:F6:96:B7:C3:FD:D6:DF:9B:2C:0B:76:6B:A8		

ANF Qualified Time-Stamping Unit 1362

Subject	CN = ANF Qualified Time-Stamping Unit 1362	**Serial number**	996426365797221774638995437
	OI = VATES-G63287510	**Clave Pública**	RSA (2048 Bits)
	OU = TSU		
	O = ANF Autoridad de Certificación	**Algorítmo defirma**	Sha256RSA
	C = ES		
Certificate Policy	1.3.6.1.4.1.18332.15.1		
Validity period	Valido desde el 2021-04-15 hasta el 2025-04-14		
Private key use period	2024-04-14		
Fingerprint SHA-1	B4:C8:83:6A:35:AE:14:08:60:15:37:C5:E3:03:51:57:E1:8D:52:28		
Fingerprint SHA-256	88:18:5A:3E:D9:95:53:9E:B9:EA:7C:4B:D9:6D:6F:85:96:0D:5A:13:2E:DB:6D:77:01:DF:67:0F:5C:AC:B4:E7		

The TSU certificates include, following the recommendations of the ETSI EN 319 421 and ETSI EN 319 422 standards, the privateKeyUsage extension, which limits the use of the Private Key by establishing a date of cessation of use of the key, prior to expiration of the public key, so as to ensure sufficient time for the renewal of the TSTs issued by a TSU before the expiration of its certificate.

TSU electronic certificates include the extension "id-kp-timestamping" which indicates that this certificate will be used for the exclusive purpose of issuing electronic time stamps.

6.6.4. TSA Certificate change

Controls are established to guarantee the renewal of the keys before the expiration of their validity.

The TSA certificate can be exchanged at any time for another TSA certificate, prior approval of the PKI Governing Board of ANF AC.

In the event of a certificate change, the associated keys will be destroyed so that they cannot be recovered, in accordance with the instructions of the manufacturer of the HSM that generates and houses them.

The TSA certificate will have a maximum useful life of 5 years. The duration of the TSU certificate is limited by:

- The validity period of the CA certificate.
- The validity period established in the certificate itself.
- If an algorithm or key length is compromised, it is no longer adequate; the TSA will cease using the affected certificates, proceeding to issue new certificates with secure algorithms and lengths.
- Cessation of activity. The provisions of the TSA Termination and Termination Plan section of this document will apply.

6.6.5. 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.

6.6.1. End of TSU's key life cycle

After the expiration of the private keys, they are destroyed in such a way that they cannot be recovered following the procedure established by the manufacturer of the cryptographic module that stores them.

6.7. Time-stamping

ANF AC TSA only issues qualified electronic time stamps, and does not issue unqualified electronic time stamps.

The TSU does not issue a time stamp before its signature verification (public key). When the certificate is uploaded to the TSU, the TSA verifies that this certificate has been signed correctly (including verification of the certificate chain from a trusted certificate authority).

6.7.1. Time-stamp issuer

ANF AC TSA offers time-stamping services using RFC 3161 "Time Stamp Protocol (TSP)", which is profiled in ETSI EN 319 422. 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 time stamp requests, accepts SHA256, SHA384, SHA512 hashing algorithms and, to sign the TST, the minimum cryptographic hash function of SHA-256 is used.

The TSU keys are RSA keys with a minimum length of 2048 bits. The key is used only for signing the TST. The TSA records all issued TSTs, which are stored indefinitely.

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.

ANF AC TSA manages a hash chaining service relative to all the TSTs issued by each TSU, without including information that can determine the identity of the requestor. And, therefore, you can prove the existence of a specific TST, and its correct chronological correspondence with respect to the set of TSTs issued by a specific TSU. In addition, it makes a notarial deposit of the general summary minutes of the incoming-current-outgoing hashes associated with the issued TSTs. ANF AC TSA may ask the trusting third party to cover the costs of verification of the existence of hash, in case of request for evidence.

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

6.7.2. Clock synchronization with UTC

ANF AC TSA 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

6.7.3. Time Stamp Reques

ANF AC TSA provides the Electronic Time Stamping service to its clients. The service is provided in two ways:

- Using an ANF AC TST client,
- Direct consultation of the TSU server, for this the stamp requests will comply with the syntax of the "RFC 3161 Time Stamp Protocol (TSP)" specification and will need to pass the corresponding access authentication control.

ANF AC TSA provides technical support in any of the cases.

6.7.4. Time Stamp Response Format

Responses do not include extensions, the TSA is not included when including the TSU certificate in the response, and the TSP is sent in the following format:

Content type: application / timestamp-reply

Method: POST

Content-length: required

<< Contains the ASN.1 timestamp response (in your case specify the error code), encoded in DER >>

Field	Treatment
Time-stamp policy	1.3.6.1.4.1.18332.15.1
Ordering	False
Nonce	If the request contains it, the same value is returned, otherwise a new one is created
Attached certificates	<TSA Certificate> <Subordinate CA Certificate>
Accuracy	Corresponding, not allowed TST greater than 1

If the request could be processed, TimeStampToken Sequence. Signed structure of the CMSSignedData type that includes the time stamp and the electronic stamp of the same. It includes the TSU certificate that signs it:

TSTInfo ::= SEQUENCE {
version INTEGER { v1(1) },
messageImprint MessageImprint,
-- OID del algoritmo hash y el valor hash de los datos sellados---
reqPolicy TSAPolicyId OPTIONAL,
certReq BOOLEAN DEFAULT FALSE,
nonce INTEGER OPTIONAL,
extensions [0] IMPLICIT Extensions OPTIONAL
}

The reqPolicy field corresponds to the OID of the TSAPolicyId. The accepted OIDs are OID 1.3.6.1.4.1.18332.15.1 corresponding to the CPS of ANF AC TSA, and OID 0.4.0.2023.1.1 corresponding to best-practices-ts-policy defined in the European standard ETSI EN 319 421.

If the request cannot be processed, a response is returned indicating an error code when it cannot respond with a time-stamp. The following describes the error codes in the PKIFailureInfo field, which are included when generating a failed response for each type of possible error:

1. badRequest: When the request policy does not match the TSA policy.
2. badAlg: When the messageImprint algorithm is not supported or is invalid.
3. badTime: When the accuracy is greater than or equal to one second or 1000 milliseconds.
4. timeNotAvailable: When the current date is not valid because it is not higher than the last date registered in the database.
5. systemFailure: When the old chain is wrong, or the new chain cannot be obtained. It is also included in the response produced by an exception or error that does not allow further processing of the request.

6.7.5. Time Stamp Validation

To validate a qualified electronic time stamp, relying parties will verify the TST using a qualified signature and seal service and electronic stamps that has TST verification. ANF AC makes this service available to the public and free of charge.

The TST verification service makes use of the “messageImprint” field described in the previous section, as well as the validity status of the TSU Certificate through the ANF AC certificate status validation service (OCSP protocol). The access point to the OCSP service is included in the TSU certificate.

Time stamp verification includes the following operations:

- **Operation I Verification of the time stamp issuer:** The issuer is ANF AC TSA, a Time Stamping Authority registered in the TSL of Spain in accordance with the eIDAS Regulation, which uses the appropriate electronic certificates to issue the qualified time stamps electronic. The public keys of the certificates used are included in the TSU and CA certificates, and are published to allow a verification that the time stamp has been correctly signed by the TSA. Certificates can be found at: www.anf.es
- **Operation II Verification of the revocation status of the TSU certificate:** An OCSP service that complies with IETF RFC 6960, is available in order to check the revocation status of the certificates used in the time stamp. The address to access the OCSP responding service is included in the certificate used to sign the time stamp.

- **Operation III Verification of the integrity of the timestamp:** The cryptographic integrity of the timestamp, for example, the ASN.1 structure is correct, and the data (the data that has been dated) belongs to the request. This can be verified by means of qualified validation devices available publicly at: www.anf.es

The validation service will be able to determine the association of the TST with the sealed electronic data by obtaining the hash of the sealed electronic data, verifying its correspondence with the hash that has been sealed by the TSA.

In addition, the existence and impossibility of manipulation of the electronic time stamp by the TSA can be verified, checking:

- the existence of the hash of the TSP in the chaining records, and
- its correct correspondence of the date and time stamped, with respect to the chronological relation of the set of TSTs issued by the TSU of interest.

The general list of hash chaining records are protocolized through the intervention of a public notary.

6.8. 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.

6.9. 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.
h) The correct calibration of the clock of your TSU is monitored. In case of detecting a deviation greater than 1 second, the TSA service will stop automatically.

6.10. 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.

6.11. 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.

6.12. 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).

6.13. 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 5.7.1 of this document.

6.14. 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.

6.15. Compliance

ANF AC TSA ensures compliance with applicable law at all times. Specifically, it is compliant to:

- Regulation (EU) 910/2014 (eIDAS), article 42.
- Spanish Law 6/2020, of november 11th, regulating certain aspects of electronic trust services.
- ETSI EN 319 421: *"Policy and Security Requirements for Trust Service Providers issuing Time-Stamps."*
- ETSI EN 319 422: *"Time-stamping protocol and time-stamp token profiles."*
- ETSI EN 319 401: *"Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"*
- ETSI TS 119 312: *"Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"*

- IETF RFC 3628: *"Policy Requirements for Time-Stamping Authorities (TSAs)"*
- IETF RFC 3161 *"Internet X.509 Public Key Infrastructure Time-stamp Protocol"*

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