Qualified service for the preservation of qualified electronic signatures and seals (QEs)

Service Practice Statement and Preservation Policy

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

Telephone: 932 661 614 (Calls from Spain)

Internactonal +34 933 935 946

Website: www.anf.es

Security Level

Public document

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

Telephone: 932 661 614 (Calls from Spain) International (+34) 933 935 946

Website: www.anf.es

Document control

Name of the document and identification

Name of the document	Qualified service for the preservation of qualified electronic signatures and seals (QEs). Service Practice Statement and Preservation Policy		
Version	1.4.		
OID	1.3.6.1.4.1.18332.56.1.1		
Approval date	14/03/2024	**Publication date**	14/03/2024

Review

Version	Changes	Approval	Publication
1.4.	Annual review. Minor wording changes.	14/03/2024	14/03/2024
1.3.	Annual review and inclusion of the preservation profile, previously outlined in document 1.3.6.1.4.1.18332.61.10	26/02/2023	26/02/2023
1.2.	Profile review with change from WTS to WST	23/04/2021	23/04/2021
1.1.	Ampliation of information of section 3.12	1/04/2021	1/04/2021
1.0.	Initial version. Creation of the document.	15/01/2020	15/01/2020

INDEX

1. Introduction

ANF Certification Authority [ANF AC] is a legal entity established under Organic Law 1/2002 of March 22 and registered with the Ministry of the Interior with the national number 171.443 and VAT number G-63287510.

ANF AC uses OIDs according to the ITU-T Rec. X.660 standard and the ISO / IEC 9834-1: 2005 standard (Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs). ANF AC has been assigned the private company code (SMI Network Management Private Enterprise Codes) 18332 by the international organization IANA -Internet Assigned Numbers Authority-, under the iso.org.dod.internet.private.enterprise branch (1.3.6.1.4.1 -IANA –Registered Private Enterprise-).

The Public Key Infrastructure (PKI) of ANF AC has been designed and is managed in accordance with the legal framework of Regulation [EU] 910/2014[1] of the European Parliament, and with Spanish Law 6/2020. ANF AC's PKI is in compliance with the standards ETSI EN 319 401 *(General Policy Requirements for Trust Service Providers), ETSI EN 319 411-1 (Part 1: General Requirements)*, ETSI EN 319 411-2 *(Part 2: Requirements for Trust Service Providers issuing EU Qualified Certificates)*, ETSI EN 319 412 (Electronic Signatures and Infrastructures (ESI): Certificate Profiles) and RFC 3739 (Internet X.509 Public Key Infrastructure: Qualified Certificates Profile); ETSI EN 319 521 "*Policy and security requirements for Electronic Registered Delivery Service Providers*"; ETSI EN 319 522 "*Electronic Signatures and Infrastructures (ESI) Electronic Registered Delivery Services*"; ETSI TS 119 511 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques "*; ETSI TS 119 512 "*Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services "*.

ANF AC uses the cryptographic techniques indicated in the TS 119 312 standard and the duration of the evidence is determined by the provisions of said standard. In 2FA (Double Factor Authentication) processes, the guidelines of the PCI SSC v3.2 standard are followed regarding the use of Multi-Factor Authentication.

For the purposes of this certification policy, ANF AC is the Provider of the "Qualified Service for the Preservation of Qualified Electronic Signatures" and the "Qualified Service for the Preservation of Qualified Electronic Stamps", provided for in articles 34 and 40 respectively, of the eIDAS Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014, regarding electronic identification and Trust Services for electronic transactions in the internal market.

In addition, ANF AC provides Certified Digitization service through the Legal Snap Scan® solution accredited by the State Tax Administration Agency, in accordance with the Resolution of October 24, 2007 of the State Tax Administration Agency (AEAT), corresponding to software of digitization contemplated in Order EHA / 962/2007, of April 10, 2007. To meet fiscal requirements, the long-term conservation platform subject to this certification policy includes information related to the content of the documents in Metadata and in database.

[1] Any mention in this document of Regulation [EU] 910/2014 includes the Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

This document is the Policy for the Qualified Service for the Preservation of Qualified Electronic Signatures and for the Qualified Service for the Preservation of Qualified Electronic Stamps that ANF AC applies in the development of its responsibility as a Qualified Provider of Trust Services in compliance with the eIDAS Regulation and current national legislation.

This policy is in accordance with the ETSI TS 102 573 standard "Policy requirements for trust service providers signing and / or storing data objects" and RFC 3647 "Certificate Policy and Certification Practices Framework", it defines the procedural and operational requirements to the that the use of the service is subject, and defines the guidelines that ANF AC applies for the provision of the WST profile:

- Preservation and storage of qualified electronic signatures
- Preservation and storage of qualified electronic seals

This document is just one of the various documents that govern the PKI of ANF AC, it details and complements what is defined in the Certification Practice Statement and its addendum. This policy is subordinate to the ANF AC Certification Practice Statement (DPC). ANF AC supervises and supervises that this PC is compatible and consistent with the rest of the documents it has prepared. All documentation is freely available to users and third parties who trust https://www.anf.es

This policy is published in the Spanish and English language versions, in case of discrepancy, the Spanish language version prevails.

This Policy assumes that the reader knows the concepts of PKI, certificate, electronic signature, and long-term storage and conservation; otherwise, the reader is recommended to learn the above concepts before continuing to read this document.

1.1. Service description

Type of service provided, WST profile:

- Preservation and storage of qualified electronic signatures.
- Preservation and storage of qualified electronic seals.

1.1.1. Identifiers of each service modality

In order to identify the qualified preservation services in their different modalities, ANF AC has assigned them the following identifiers (OID) additionally to 0.4.0.19511.1.2. (Qualified service compliant with Annex A of ETSI TS 119 511):

Preservation and temporary storage of qualified electronic signatures	1.3.6.1.4.1.18332.61.5
Preservation and temporary storage of qualified electronic seals	1.3.6.1.4.1.18332.61.6

The same profile will apply throughout the preservation period.

The profile will not change over time, so the profile does not include dynamic aspects outside of the preservation profile.

ANF AC Servicio de conservación			
Subject	CN = ANF AC Servicio de conservación	**Serial number**	995304246984473328978043403
	OI = VATES-G63287510	**Public Key**	RSA (2048 Bits)
	OU = Certificado Cualificado de Sello Electronico		
	O = ANF Autoridad de Certificación	**Signature algorithm**	Sha256RSA
	C = ES L=Barcelona, ST=Cataluña		
Validity period	Valid from 2023-02-01 17:06:59 until 2025-01-31 17:06:59		
x509SKI	MaA+AC7H45Vqfc8OPNA0/muzrDk=		

1.1.2. Electronic evidences

The electronic evidences are generated including metadata in the header of the data files, and signing the data transmitted by the subscriber, using in the elaboration a certificate of Qualified Electronic Seal of ANF AC.

The electronic evidence does not contain explicit information about the preservation service or the applicable Preservation Policy, although the service used in its authentication and the time stamp corresponding to the moment the data was received does include metadata.

ANF AC, has the necessary capacity to develop at least advanced electronic signatures / seals (Standardized Policy requirements (N)), although the long-term conservation platform has been configured with the ability to use Extended Policy requirements (N +), using qualified certificates, to be able, where appropriate, to prepare qualified electronic signatures.

In order to maximize interoperability, AdES signature formats conforming to,

- **CAdES LT** *(ETSI EN 319 122)*
- **PAdES LT** *(ETSI EN 319 142)*
- **XAdES LT** *(ETSI EN 319 132)*

The algorithms, key lengths and procedures established in the Electronic Signature Policy of ANF AC OID 1.3.6.1.4.1.18332.3.1 are applied.

1.1.3. Certification

ANF AC, in its capacity as Qualified Trust Service Provider and issuer of the qualified electronic signature and seal certificates, is the issuer of the qualified certificates used by the long-term preservation and storage platform.

1.1.4. Validation

ANF AC, in its capacity as Qualified Provider of Qualified Electronic Signature and Seal Validation Services, provides the validation service used by the Long-term Preservation and Storage Platform.

1.1.5. Qualified Time Stamping

ANF AC, in its capacity as a qualified provider of electronic time stamps, provides the validation service used by the long-term preservation and storage platform.

1.2. Name of the document and Identification

Name of the document	Qualified service for the preservation of qualified electronic signatures and seals (QEs). Service Practice Statement and Preservation Policy		
Version	1.4.		
OID	1.3.6.1.4.1.18332.61		
Approval date	14/03/2024	**Publication date**	14/03/2024

The identifier of this policy will only be changed if there are substantial changes that affect its applicability. This policy is published in the Spanish and English language versions, in case of discrepancy, the Spanish language version prevails.

The entry into force of a new version occurs at the time of its publication, the policy is published on the corporate website of ANF AC www.anf.es

1.3. PKI participants

As established in ANF AC CPS.

1.4. Scope of application

1.4.1. Allowed uses

Long-term preservation and temporary storage of data, advanced or qualified electronic signatures and advanced or qualified electronic seals.

1.4.2. Use limitations

In general, as established in the CPS of ANF AC.

1.4.3. Forbidden uses

In general, as established in the CPS of ANF AC.

1.5. Contact information of the entity

As established in ANF AC CPS.

1.6. Definitions and acronyms

In addition to those outlined in the CPS of ANF AC, for the purposes of this service the following definitions and acronyms apply,

1.6.1. Definitions

Time Stamping Authority: ANF AC is the Qualified Provider of Time Stamping of this policy.
Long-term Conservation Authority: ANF AC is the Qualified Provider that provides this service subject to this policy.
Validation Authority: It is the Provider Qualified that provides information about the status of the certificate.
Preservation client: An application or piece of software (API) that interacts with a preservation service through a communications protocol.
Long-term preservation: extension of the validity status of an electronic signature/seal for long periods of time and/or extension of the provision of proof of the existence of data for long periods of time, despite the obsolescence of cryptographic components or the loss of the ability to verify the validity status of the public key certificates used.
Dual control: procedure by which the intervention of two operators is required.
Data: They are real binary objects / octets on which the preservation and storage process is carried out.
Validation Data – Data that is used to validate a digital signature.
Qualified electronic signature creation device: it is a device that meets the requirements listed in Annex II of EU Regulation No. 910/2014 and is certified in this regard.
Electronic document: it is information of any nature in electronic form (eg text of a message, PDF file, images, videos, etc). In providing this service, ANF AC guarantees the accessibility, confidentiality, authenticity, integrity and preservation of the document in the long term.
Duration of the evidence: It is the expected time that the conservation service expects that the evidence can be used to achieve the preservation objective.
Preservation scheme: generic set of procedures and rules relevant to a preservation storage model and one or more conservation objectives (in the case of this policy the WST profile) that describe how preservation evidence is created and validated.
Evidence of conservation: they are the events obtained that have been generated to achieve the preservation of the data.
AdES LT level signature: This format includes TimeStamping , all the certification and revocation information (signed OCSP response) necessary to validate the signature over time.
AdES LTA level signature: To preserve the integrity of the signature in the long term, the AdES LTA format is defined, which includes a time stamp on the entire signature. AdES formats are those that comply with the eIDAS regulation (set of European standards), the most used are: CAdES , PAdES , XAdES.

Advanced electronic signature: is linked to the signer, allows the signer to be identified, has been created using electronic signature creation data that the signer can use, with a high level of confidence, under his or her exclusive control, and is linked to the data signed or sealed in such a way that any subsequent modification of the same is detectable. The advanced electronic signature is always generated using a current qualified electronic certificate and a secure signature creation device.

Qualified electronic signature: it is the electronic signature that meets the requirements established by law, that is, it has been created using a qualified signature creation device and a qualified signature certificate.

Preservation Object Identifier: A unique identifier for a dataset submitted to a preservation service.

Preservation Interface – Component that implements the preservation protocol on the preservation service side.

Long Term – Period of time during which technological changes may be a concern. e.g .*The possible technological changes that cause the obsolescence of cryptographic technology such as: crypto-algorithms, key sizes or hash functions, etc.*

Metadata: It is data encapsulated in other data.

Retention object – A typed data object that is sent, processed, or retrieved from a retention service.

Profile / Conservation model: it is the way in which the service provider implements it. In the case of this policy, the profile is WST (preservation and temporary storage).

Retention period – The length of time during which evidence that is produced asynchronously can be retrieved from the service.

Evidence of Preservation and Temporary Storage Policy: A set of rules that specify the requirements and internal process for generating or how to validate evidence of preservation.

Proof of Existence – Evidence that proves that an object existed at a specific date/time.

Integrity proof: Evidence that the data has not been altered since it was protected.

Re-stamped / Re-sealed: Increase of preservation that is carried out on evidence of conservation in order to demonstrate in the long term the existence of a specific conservation object, thus extending its period of validity. e.g . *Add a new timestamp that protects additional validation data that can be used to validate a signature and/or timestamp, and/or the hash of the data, using a stronger algorithm.*

Portability – Export/import package of information extracted from a preservation service, including submission data object (SubDO), preservation evidence, and preservation-related metadata, allowing another preservation service to import for continue to achieve the preservation objective based on this information.

Provider / Provider of conservation and temporary storage services: In the case of this policy, ANF AC is the service provider.

Notification Protocol – Protocol used by a preservation service to notify the preservation client.

Evidence record: Data unit that allows to prove the existence at a given moment, of a stored data object.

Time Stamp: data in electronic format that links other electronic data to a particular time by establishing proof that this data existed at that time.

Preservation service: Service capable of extending the validity state of a digital signature for long periods of time and/or of providing proof of the existence of data for long periods of time.

Validation service: Service that validates an electronic signature / seal, employee certificates, etc.

Subscriber / Subscriber: is the individual or legal client that hires ANF AC for the long-term conservation service.

1.6.2. Acronyms

2FA: Two Factor Authentication

AdES: Advanced Electronic Signature.

AGO: Augmentation goal.

LT: Long-time.

LTA: Long-time archive.

OCSP: On-line Certificate Status Protocol.

OTP: One-Time-Password.

PC: Certification Policies.

QTSP: Qualified Trust Service Provider, in the context of this policy ANF AC is the reference QTSP.

PKI: Infraestructura de clave pública.

POC: Preservation object container.

PRP: Conservation Service Protocol.

PSP: Conservation Service Provider.

SCA: Strong Client Authentication.

SigS: Electronic signature / seal creation service.

ISMS: Information Security Management System.

SSL: Secure Ports Layer. They are cryptographic protocols that provide secure communications over a network and authenticate the server that provides the service.

SubDO: Submission data object.

TLS: Transport Layer Security. Cryptographic protocols that provide secure communications over a network and authenticate the parties involved in the communication.

TSP: Trust Service Provider.

ValS: Validation Service.

WST: with Storage.

2. Repositories and publication of information

2.1. Repositories

As defined in the CPS of ANF AC.

2.2. Publication of information

As defined in the CPS of ANF AC.

2.3. Frequency of updates

As defined in the CPS of ANF AC.

2.4. Access controls to repositories

As defined in the CPS of ANF AC.

3. Operational Requirements

3.1. Information Management Systems Security (ISMS)

ANF AC uses an Information Security Management System (ISMS) that has been certified in accordance with the ISO/IEC 27001:2013 standard, thus ensuring compliance with security controls in transmission against risks of loss, theft, damage or any unauthorized modification.

ANF AC's ISMS has been developed in accordance with ISO/IEC 27002 and as indicated in Annex A of ISO/IEC 27001:2013, it supports the signature, the storage of objects identifies objectives and additional controls that specifically comply with the potential risks associated with signing and/or storing relevant objects additional that specifically comply with the potential risks associated with signing and/or storing relevant objects.

The information security policy complies with applicable laws and regulations, especially the risk controls established in ETSI EN 319 401 and, in particular, the General Data Protection Regulation (GDPR) and the Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, having prepared a Data Protection Impact Assessment (EIPD) with a low risk level result. In addition,

- ANF AC has an Information Security Policy OID 1.3.6.1.4.1.18332.101.80.1
- Policies for the relationship with external service providers that support ANF AC in the provision of its certification services, having signed a formal contract in which duties and responsibilities are established.
- ANF AC, manages:
    - Risk Management Plan, OID 1.3.6.1.4.1.18333.13.2.1;
    - Risk Assessment, OID 1.3.6.1.4.1.18332.101.80.6.3;
    - Risk Matrix, OID 1.3.6.1.4.1.18333.101.80.6.1;
    - Continuity and disaster recovery plan, OID 1.3.6.1.4.1.18332.13.1.1;
    - Activity cessation plan, OID 1.3.6.1.4.1.18332.1.9.1.11.
- Assets and vulnerabilities are identified, risks are evaluated, the probability that they will occur, the degree of impact that they can cause and the safeguards applied by the organization.
- Private signature keys are classified as sensitive data that must be protected by special measures.
- Data objects are classified as sensitive data of the subscriber/subscriber who is responsible for them. This information is only disclosed to persons authorized by the subscriber.

ANF AC maintains criteria in relation to the information available for audits, and analysis of incidents that may occur.
Periodically, at least once a year, internal and external audits are carried out in accordance with an Audit Plan of the organization, audits against international norms and standards on the matter.
Control and detection of incidents are managed on the long-term temporary storage and conservation platform.
The provisions of the Policy for the reporting and treatment of security incidents OID 1.3.6.1.4.1.18332.101.45.30 apply

Any interested party can communicate their complaints or suggestions through the following means:

- By phone: 902 902 172 (calls from Spain) International (+34) 933 935 946
- By email: info@anf.es
- Filling in the electronic form available on the website https://www.anf.es
- By in person at one of the offices of the Recognized Registration Authorities.
- By in person at the ANF AC offices.

- ANF AC has an Incident Registry in which any incident that has occurred with the certificates issued, and the evidence obtained, is recorded. These incidents are recorded, analyzed and solved according to the procedures of the ANF AC Information Security Management System.
- The Security Manager determines the severity of the incident and appoints a manager and, in the event of relevant security incidents, informs the PKI Governing Board.
- ANF AC has a Physical and Environmental Security Policy OID 1.3.6.1.4.1.18332.101.45.14 which, among other issues, establishes requirements for physical access to the organization's facilities and use of assets.
- The organization's computer systems have controls in place to protect against attacks and malicious software. There is a version control procedure, project control and all processes and technology are documented and classified.
- Periodically, port scanning and verification of server configurations and study of logs are carried out in order to detect suspicious actions of unauthorized access attempts or data processing.
- The systems are regularly updated to the latest versions classified as stable and for exploitation.
- The servers have advanced technology to control unauthorized access, antivirus system, firewall, etc. Periodic LOG checks are carried out to detect attempts at aggression.
- All staff submit to a commitment to confidentiality and carry out Continuous Training.
- In teleworking, an SSL connection and identification by means of a qualified electronic signature certificate are required.
- ANF AC, the Contingency and Disaster Recovery Plan, is periodically tested.

3.2. Use of the private key

Subscribers who have a qualified electronic signature certificate can send their documents signed. Otherwise, at least the subscriber must use an ANF AC application for the secure download of documents that generates a hash of the data object in his terminal and includes the SSL communications protocol for sending it to the storage platform.

ANF AC signs the electronic documents with its own password on behalf of the subscribers.

The private signature key is stored at least in a secure EAL 4+ Common Criteria certified signature creation device, although the device used may also be certified in QSCD compliance in accordance with the eIDAS Regulation, in which case the electronic signatures are qualified signatures.

The electronic signatures / seals produced on the temporary storage and conservation platform are long-term signatures LT / (in accordance with Baseline standards).

3.3. Signature maintenance during the storage period

In order to ensure that electronic signatures/seals are maintained in such a way that their validity can be verified for the entire storage period. ANF AC has implemented technical procedures and organizational measures, as a minimum:

a) Technical Measures
All signatures include information that enables validation of the signature *(for example, the certificate path of a known trust point, for example, root CA and revocation information)* and a trust indicator *(for example, timestamp)* from the moment that signature existed and the certificate used was valid. The information is stored at the same time as the signed data object, in such a way that the integrity of this set of information is guaranteed.

For data transmission, the platform has:
- Web application for personal users,
- API for cross-system automation.

Both systems require credentials from the parties and a communication protocol that guarantees the confidentiality of the data (SSL) is used.

All received data objects that are signed are subjected to validation control, only those whose validation is in compliance are accepted.

The data objects received and whose conservation and temporary storage have been accepted, are electronically signed AdES LT by ANF AC. The subscriber is delivered a record of acceptance of conservation and temporary storage OID 1.3.6.1.4.1.18332.62.4

The duration of the evidence is determined by the provisions of ETSI TS 119 312. In order to guarantee the preservation of authenticated information, for a time greater than the lifetime of the cryptographic algorithms and key lengths used, when necessary re-timestamping process is applied through the use of archival time stamps, in accordance with ETSI standards for AdES signature formats, applying cryptographic components in accordance with ETSI TS 119 312.

A LOG system is managed that records all access events and services required and provided.

b) Organizational Measures
The storage platform is maintained by ANF AC, using CPDs from multinationals of recognized prestige and guarantees. All servers are under its exclusive administration and control, installed in the territory of a member country of the Union.

ANF AC manages equipment and systems that guarantee the processing and storage capacity required by its subscribers. Service is guaranteed with an SLA level greater than 99%.

3.4. Access to information, publication and traceability

The information is permanently accessible and access controls have been implemented to ensure that only authorized personnel can access it.

All persons authorized to access the information will be provided with credentials based on qualified electronic signature certificates.

Access to information is done electronically remotely. The privacy of communications is guaranteed through the use of the SSL / TLS communications protocol, in accordance with current legislation.

The authorized operators, prior to accessing the information, sign a document detailing the request and actions carried out.

The systems have procedures for performing a data search and its publication.

3.5. Authenticity and integrity

In order to guarantee the authenticity of the origin and the integrity of a set of data objects, and also in order to avoid the loss or surreptitious addition, access to the information is only possible to consult or obtain an authenticated copy of the same.

ANF AC guarantees:

- Prior to the publication of the information, the validity of the signature that authenticates and guarantees its integrity is checked. Through this procedure, any breach of integrity is detected.
- All information stored is authenticated at least with a long-term advanced electronic signature in AdES LT format.
- The necessary techniques are applied (if necessary, re-stamping using a strong cryptographic procedure) to guarantee the maintenance of the signature during the entire storage period.

3.6. Signature

What is defined in the Signature Policy of ANF AC OID 1.3.6.1.4.1.18332.27.1.1 applies

3.7. Signature validation

What is defined in the Qualified Validation Policy of ANF AC OID 1.3.6.1.4.1.18332.56.1.1 is applied

For the validation of the evidence of preservation, qualified validation mechanisms must be used. ANF AC makes publicly available a validation mechanism that allows the validation of electronic evidence, including:

- Electronic signatures
- Electronic time-stamps
- Certificates (full certification chain)

3.8. Electronic Time stamp

What is defined in the Qualified Electronic Time Stamp Policy of ANF AC OID 1.3.6.1.4.1.18332.15.1 is applied

3.9. Readability

The ANF AC long-term storage platform only accepts electronic documents in PDF, JPG, JEPG, PNG formats. The service does not include the conversion process from an analog object to a digital/electronic format.

In order to ensure that the data objects remain human- or machine-readable during the storage period, technical and organizational means are applied:

a) Technical measures

- The retention platform is configured to reject all data objects whose format is not accepted according to a specification published on the same platform.
- The long-term temporary storage and conservation platform includes a document display system and electronic signatures.
- When there is a risk that a specific display system will become obsolete, all affected data will be reliably backed up while maintaining its semantics and without content changes. to a new data file in current format. An independent reliable statement will be produced that attests to the correspondence of the content and semantics of the new data object with the old one.

b) Organizational measures

ANF AC has a Quality Plan that determines the procedure and operators that assume the responsibility of verifying the quality of electronic documents, prior to their delivery to the long-term conservation platform. This Quality Plan, in addition to contemplating legibility control, includes metadata control that facilitates the search for electronic documents.

3.10. Information security

In order to ensure that the means where the data objects are stored can withstand the passage of time, such as the deterioration of the support that stores them or even hacker attacks or fortuitous corruption of the information and, especially, the obsolescence of the cryptographic components used for its conservation, it has:

- S3 storage system, using buckets technology. This technology automatically generates online backup copies of 100% of the data objects. These copies are located on servers installed in a different geographical area than the data being used.
- Privacy. All stored information is cryptographically protected to prevent manipulation. Using SSE-S3 technology, each object is encrypted with a unique key. As an added security measure, it encrypts the key itself with a periodically rotating master key. The symmetric cryptographic algorithm used is Advanced 256-bit Encryption Standard (AES-256).
- Upon receipt of the information, prior to its acceptance, an antivirus is used to check that the data object does not contain known malicious code.
- At the time of receipt of the information, prior to its acceptance, we proceed to check if the data is signed and, where appropriate, we proceed to validate the signature. In case of non- conformity, conservation is rejected.
- In case of acceptance of conservation, the long-term electronic seal of ANF AC is stamped, the cryptographic components used are recorded in order to carry out an obsolescence control and, where appropriate, re-stamp those that are necessary, and issues certificate of acceptance.

When data objects are stored, whose format may include changes in the presentation or any modification not detectable by integrity controls, the preservation platform notifies the user, prior to publication, that the data objects are in an unreliable format.

3.11. Separation and confidentiality requirements

In order to ensure the confidentiality of the information, the electronic data objects related to different owner organizations are stored and archived in such a way that their access to unauthorized third parties is impossible. Each data object has a unique identifier of its owner (subscriber code) and access to the data is restricted based on its owner.

3.12. Preservation Protocol

The service has been developed by the ANF AC R&D department and has its own conservation protocol. It works with XML. It is protected against unauthorized use.

Specifically, the operations indicated by ETSI TS 119 512:

- RetrieveInfo
- PreservePO
- RetrievePO
- DeletePO
- UpdatePOC
- RetrieveTrace
- ValidateEvidence
- Search

Traces of all operations related to a specific preservation object identifier can be obtained, as defined in the *RetrieveTrace* operation according to ETSI TS 119 512

It is possible to search for preservation objects including filters and retrieve them as defined in the *Search* operation according to ETSI TS 119 512

In the event that the subscriber requests the removal of a conservation order before the end of the conservation period, it will be required that the request be made by a person authorized by the subscriber and that they provide the corresponding receipt.

The deletion has a scope to the data objects and the preservation tests of the SubDO.

The deletion does not necessarily entail the destruction of the information, the service subscription contract will establish whether the scope of a deletion is destruction or blocking of the data.

In case of data blocking, the information will be deleted from the conservation service repository and a copy will be stored in a security repository, applying a limitation of use in order to make it inaccessible. The information with limitation of use, has the sole objective of proving the correct provision of the service by ANF AC, or complying with an order from a Court of Justice.

3.13. Notification protocol

For each data object delivery made by the subscriber, the Conservation service generates a record specifying whether the service has been accepted or rejected and, where appropriate, validation of the signature/seal or generation of the ANF AC electronic seal. In case of rejection, the reason is specified.

On-demand subscriber can download data object, evidence of preservation or minutes indicated above through the service console. Only accessible to persons authorized by the subscriber.

Notification is not planned.

3.14. Reports and exchanges with the authorities

The owner is the subscriber to the service of stored electronic documents, therefore, except in case of court order, access and publication of the data to the authorities must be authorized by the owner of the data.

In order to ensure that the data objects are reported and exchanged with the authorities authorized by the owner, in such a way that the integrity and security of the data source is guaranteed, ANF AC guarantees:

- The representative of the authority must identify themselves in accordance with the provisions of this certification policy and will be provided with access credentials, the use of which must be adapted to this policy, to the CPD of ANF AC.
- A secure channel is used to send data objects to the Authorities, so that the remote user and the server are authenticated, the integrity and confidentiality of communications are protected against network vulnerabilities (for example, user credentials and SSL communications protocol).
- Access to information is remote, available 24x7x365.
- The publication platform offers the possibility of reading and obtaining authentic copies of the electronic documents of interest.
- Prior to publication, the conservation evidence is validated.

4. Trusted roles

All personnel involved in the management and administration of the conservation platform have been clearly informed in writing of their duties and responsibilities, these personnel have accepted the responsibilities and obligations in writing.

In addition, ANF AC personnel have signed the corresponding confidentiality commitment, a commitment that lasts even after their departure from the organization.

Periodically, ANF AC carries out internal audits of processes and of the activity carried out by its staff in order to reduce the risk of theft, fraud or misuse of the organization's assets.

All ANF AC staff have received credentials based on a qualified electronic signature certificate, and specific training on the ANF AC campus for the proper performance of their duties.

ANF AC has and applies HR policies:

- Roles and Responsibilities Policy OID 1.3.6.1.4.1.18332.38.1,
- Internal Regulation OID 1.3.6.1.4.1.18332.101.80.5
- Training plan OID 1.3.6.1.4.1.18332.100.20.1.2

4.1. Personnel controls

As defined in the CPS of ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1, HR Policies and specifically:

The people who participate in the services provided by ANF AC, are personnel who are under the direction of the organization, and are selected according to objective criteria of training and availability.

Exclusive functions have been established for highly trusted personnel of ANF AC senior management:

Responsible for identity verification

It is personnel assigned to the RDE area of ANF AC. It assumes the responsibility of ensuring compliance with the processes established for the verification of the initial identity of the subscriber and operators authorized to access on their behalf.

Systems administrator

They are personnel assigned to the technical area of ANF AC. It assumes the responsibility of ensuring the full operation of the systems, carrying out installation, configuration and maintenance tasks for the management of services. Requirements specific:

- They do not have access to the CA keys.
- They do not have access to the CA logs. It will be prevented by CA software user properties.
- They authenticate via SmartCard or USB token with the CA software and this software will not support any alternative authentication method.

Responsible for QSCD access codes

They are in charge of activating the ERDS signature keys, each manager has a SmartCard or a USB Token that allows managing the signature keys stored in a QSCD device on the remote signature server. The number of persons responsible for access codes is three people, and the system requires dual intervention.

These trusted personnel are the only ones authorized and enabled to carry out backup, conservation and recovery operations on the signature key. Always under dual control and in a physically secure environment.

Systems operator

Personnel authorized to use the terminals with access to the certified delivery systems and who carry out general tasks of management and daily attention to the service. This role is not incompatible with that of system administrator.

System auditor

Authorized to view files and audit logs of ANF AC systems.

You will see the logs through the web interface offered by the CA. Authentication through SmartCard or token.

Only this Role will have access to the logs.

The auditor must be in charge of:

- Check the tracking of incidents and events
- Check the protection of the systems (exploitation of vulnerabilities, access LOGs , users, etc.).
- Check alarms and physical security elements

Security Manager

In accordance with what is defined in the Security Policy of ANF AC. In addition, it will be responsible for :

- Verify the existence of all the required and listed documentation
- Check the consistency of the documentation with the procedures, inventoried assets, etc.

4.2. Suppliers and external collaborators

ANF AC has drawn up a Relationship Policy with suppliers and external collaborators that requires an evaluation analysis to determine its suitability for the role required by the organization.

Member and Provider Code of Conduct OID 1.3.6.1.4.1.18332.101.45.

The relationship with these entities is always contractually formalized. The contracts, among other clauses, include a commitment to confidentiality and, once the relationship has ended, a demand for the return of the organization's assets and withdrawal of the access credentials that could have been granted.

Subscribers / Clients

Individuals or legal entities that contract this long-term temporary storage and conservation service.

Relying third parties

All those people who, voluntarily, trust the services provided by ANF AC accepting the terms and conditions of the service, as well as the limitations of use, Policies and DPC of ANF AC.

5. Identification and authentication

5.1. Initial identification

The identity of the subscriber/subscriber and their authorized operators, as well as that of the ANF AC operators in charge of managing the platform, will be verified by one of the means of identification with a substantial security level or a high security level (1) following:

- Physical presence in one of ANF AC's Face-to-Face Verification Offices or AR, or through a third party in accordance with national law.
- Through a certificate of a qualified electronic signature or a current qualified electronic seal.
- Using any of the procedures established in art. 24 of the eIDAS Regulation.
- Through a 2FA means in which one of the factors is based on a procedure qualified by the Court of Justice or legally recognized nationally as a means that allows the identification of a natural person.

The identity of the trusting third parties (auditors, AEAT inspectors, and operators expressly authorized by the subscriber) can be done through one of the low security level identification means (2).

(1) *Article 8.2. of the Regulation eIDAS*

5.2. Authentication

The authentication process will be carried out by means of a Qualified Electronic Signature Certificate.

6. Functional procedure

The service applies the methods of identification, electronic signature or seal, OCSP verification and qualified electronic time stamp provided for in the eIDAS Regulation, subjecting electronic documents to permanent audits in order to guarantee the integrity, authenticity and legibility of the files stored throughout over time.

This service is provided during the period of time contracted by the client subscriber, once the contract is finished the information is blocked or permanently destroyed (see section 3.12).

The conservation service guarantees permanent access, the full recovery of the documents, and the management of the evidence that allows the integrity of the documents in custody to be demonstrated.

6.1. Data object download

The long-term storage platform has two procedures for subscribers to transfer data objects:

a) End user console on Web server.
b) API to establish communication between the subscriber's automated system and the ANF AC conservation platform.

One or more submission data objects (SubDO) are allowed to be preserved under a specific preservation profile (client code).

6.2. Initial protection

In order to guarantee integrity and adequate control of the audit process, the platform, upon receipt of the electronic document, performs:

- Subscriber identity verification. Only subscribers to the service can send data.
- Data object format validity check. Only formats accepted by the platform can be accepted.
- If the electronic document is signed, the electronic signature or seal that authenticates it will be validated. In this process, a qualified validation system for electronic signatures and seals is used.
- In the event that the electronic document is transmitted associated with a hash, the correspondence of the hash with the data object will be verified.
- Evidence of the conformity or failure of the signature or hash validation process carried out in the previous steps is obtained. In case of non-compliance, a denial of service is made.
- Document metadata is recorded.
- The platform applies an LTA signature/seal to the electronic document in order to ensure integrity, long-term validity, and unify permanent audit process.
- The signature applied as a minimum is an advanced electronic signature prepared with a qualified certificate, and in accordance with the ETSI AdES standards.

- It includes a qualified electronic time stamp in accordance with eIDAS, and verification of status at origin by OCSP consultation, both issued by ANF AC as PCSC.
- The document and evidence obtained from the previous processes is stored in a specific folder individualized for that subscriber.
- The information is stored in the exploitation area and replicated in the recovery area, backup server located in a different geographical location.

6.3. Access to information, traceability

The long-term temporary storage and conservation platform manages a metadata service that facilitates its search and location. Metadata includes information relative to the system that generates the evidence. In addition, a procedure is managed that manages the traceability of the data: operators who have accessed, actions carried out and the moment in which each event occurred.

Each operator must sign an access certificate, thus assuming its responsibility in the transaction carried out. The platform has a search and publication system, from a private web environment and available 24x7x365.

6.4. File

The platform allows you to associate documents by means of a unique identifier, in this way you can access all the documents corresponding to the same file in a simple and efficient way.

6.5. Augmentation

Online audit: prior to the publication of a document, a signature validation is carried out, in case of compliance, access is given to the subscriber. In case of failure, a copy of the backup is restored once its integrity has been verified.

Periodically, an integrity audit of all stored documents is carried out.

Re-stamping : the evolution of the state of the art and the security of the algorithms and cryptographic procedures used in its authentication are monitored. In case of risk, the evidence is re-sealed by applying a qualified seal electronic time stamp using cryptographic components qualified as secure in accordance with ETSI TS 119 312.

6.6. Protection

The signing keys are physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing content and/or user evidence.

Signature keys are maintained and used, at a minimum, in a secure signature creation device, or a qualified signature creation device (QSCD). The backup copies of the signature keys are stored in a bank bunker.

Security measures are applied during the transport and storage of the cryptographic devices used by the ERDS service, carrying out the necessary tests that guarantee their correct operation prior to their use.

The registry files are protected from unauthorized reading, modification, deletion or any other type of manipulation using logical and physical access controls. Evidence stored in S3 storage systems, using buckets technology.

Full backup copies of the audit log are generated, cryptographically protected to prevent tampering. Using SSE-S3 technology, each object is encrypted with a unique key. As an additional security measure, it encrypts the key itself with a periodically rotating master key, the symmetric cryptographic algorithm used is Advanced 256-bit Encryption Standard (AES-256).

Communications with the systems are always carried out using the SSL encrypted communications protocol between users and ANF AC systems, and TLS between computer systems.

6.7. Portability - Import

The subscriber can request the portability of the data stored in the conservation platform, or the importation of data. The information will be delivered or received in a standardized format (always based on an open format), or in one of the formats defined in BSI Annex TR-ESOR-F of the BSI 03125 Technical Guide for the preservation of cryptographic evidence, published in ,

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03125/PrevVersion-1_2/BSI_TR_03125_TR-ESOR-F_V1_2_EN.html

The portability or import of data is not automated. A prior budget will be made, the cost of which will depend on the volume and complexity of the information. The provision of the service will require its acceptance by the subscriber.

Application process:

- It must be requested by the legal representative of the subscriber:
  - The request must be sent by email to soporte@anf.es and will be electronically signed.
  - It will indicate the type of format in which you want to receive or send the data.
  - Indicate the person or persons authorized to download or send the information.
  - Will pay the fees previously accepted by budget issued by ANF AC.

The imported or ported data package will be transmitted encrypted through ANF AC's Security Transfer services.

Exported data packages will only be delivered to the person authorized by the service subscriber.

A record of all ported data packages will be managed, whether exported or imported, specifying:

1) The date of the event.
2) The criteria that have been used to select the set of preservation objects that will be included in the export-import.

6.8. End of conservation period

The provision of the service establishes a WTS [preservation and temporary storage] profile. The duration period corresponds to the period contracted by the subscriber.

Once the term has expired and the contractual relationship with the subscriber has concluded in the event of non-renewal of the service, the subscriber is informed that the data will be destroyed and portability (data export) is made available to them for a period of 60 days.

7. Preservation profile

This preservation profile is uniquely identified with the OID 1.3.6.1.4.1.18332.61.10.

The Retention Policy that applies in this Retention Profile at the time of its publication is, OID 1.3.6.1.4.1.18332.61 version 1.3

The Validation Policy applied in this Conservation Profile at the time of its publication is, OID 1.3.6.1.4.1.18332.56.1.1 version 2.7

The version of the aforementioned policies may change over time and they are publicly accessible at http://www.anf.es (latest and historical version). The version that corresponds to the moment of generating the conservation evidence will be applied.

7.1. Preservation goals

ANF AC's preservation platform is designed and developed to achieve the following goals:

- **Preservation of General Data (PGD):** Provides proof of existence for long periods of time of the submission data object (SubDO) sent to the preservation service. It reaches both signed and unsigned data.
    - http://uri.etsi.org/19512/goal/pgd
- **Preservation of digital signatures (PDS):** extends over long periods of time the ability to validate an electronic signature / seal, maintain its validity status and obtain proof of the existence of the associated signed data.
    - http://uri.etsi.org/19512/goal/pds
- **Augmented Preservation (AUG):** indicates that the preservation service admits the increase in the conservation evidence sent (re-stamped).
    - http://uri.etsi.org/19512/goal/aug

7.2. Storage model

The ANF AC conservation platform stores the data objects that are sent to it by subscribers (SubDO), as well as the preservation evidence that is produced by the conservation service. In this model, the conservation service supports the portability and import of preservation objects and evidence produced by the platform itself or by third-party providers, as the case may be.

ANF AC preservation service contemplates a single storage model, WST.

ANF AC storage model is WST storage, in accordance with clause 4.3 ETSI TS 119 512. The data to be preserved is stored and delivered at the client's request, along with the evidence.

The client sends the complete data object to the preservation service.

This storage model is addressed by the WithStorage (WST) value within the PreservationStorageModelType.

```
<simpleType name = " PreservationStorageModelType " >
        < base de restricción = " cadena " >
                <enumeration value = " WithStorage " />
```

```
        </restriction>
</simpleType>
```

The same retention profile will be applied throughout the retention period to the data object and to the retention evidence.

7.3. Identifier

The ANF AC storage model is addressed by the WithStorage (WST) value within the PreservationStorageModelType. In accordance with

- http://uri.etsi.org/19512/scheme/pds+pgd+aug+wst+ers

7.4. Supported operations

The ANF AC platform supports:

- Preservation,
- Recovery,
- Erased,
- Validation,
- Search.

7.5. Generation and validation of evidence of preservation

ANF AC platform supports two types of SubDO:

- SubDO with one or more digital signatures (SubDOwithDS)
    - SubDOwithDS, the conservation service will carry out a signature validation in accordance with the ANF AC validation policy, and collect and store the validation reports in the repository for this purpose.
- SubDO without digital signatures (SubDOwoDS)
    - Evidence of conservation prepared by electronic seal AdES LT from ANF AC is obtained.

In any case, the evidence of conservation produced will be a file format of an AdES signature.

7.6. Augmentation of preservation evidence

The provisions of ETSI TS 119 312 are followed for cryptographic security purposes.

The ANF AC re-stamping service makes qualified electronic time stamps to increase cryptographic security if necessary.

7.7. Profile scheme

ANF AC service has been designed and developed in accordance with the following WST profile scheme "Preservation and storage".

- *ProfileIdentifier*: The service profile is uniquely identified, it is WST.
- Operation: The compatible operations are reported (3.2), the system contemplates the elements:
    - Input / Format / FormatID corresponding to the PreservePO operation contains the URI http://uri.etsi.org/19512/format/DigestList, and
    - Input / Format / Parameter / Format / FormatID elements specify the set of supported digest algorithms.
- *Policy*: The evidence conservation policy can be found in the document OID 1.3.6.1.4.1.18332.61.11. The signature validation policy is found in the document OID 1.3.6.1.4.1.18332.56.1.1.
- *ProfileValidityPeriod*: the point in time from which the preservation profile has been activated is the moment the data object is accepted and the ANF AC electronic seal is applied. The retention period ends and is deactivated at the time of concluding the contractual obligation with the customer.
- *PreservationStorageModel*: Equals WithStorage .
- *PreservationGoal*: In accordance with what is specified in Section 7.1 of this document.
- *EvidenceFormat*: Signature AdES LT.
- *Specification*: Not required.
- *Description*: Not required.
- *SchemeIdentifier*: Not required.
- *PreservationEvidenceRetentionPeriod*: Duration of the contract signed with the subscriber, plus 60 days to perform portability if required by the subscriber.
- *Extension*: Not required.

8. Obligations and responsibilities

8.1. Obligations of the service provider

ANF AC, in its capacity as Qualified Provider of Trusted Services, fully assumes the provision of all QTSP services necessary for the provision of the long-term conservation service. It is obliged to:

- Respect the provisions of this Policy.
- Implements ETSI TS 119312 monitoring controls
- A control of the state of the cryptographic technique and its advances is carried out.
- Safeguard your private keys.
- Issue qualified electronic time stamps whose minimum content is that defined by current regulations.
- Process and issue qualified electronic signature certificates.
- Process and issue qualified electronic seal certificates.
- Process and issue electronic time stamp certificates.
- Process and issue OCSP certificates.
- Remote service of qualified electronic signature.
- Obtain OCSP responses signed by the issuing PCSC whose minimum content is that defined by current regulations.
- Proceed with the validation of electronic signatures and seals through a qualified validation service in accordance with current regulations.
- Publish this Policy on the corporate website.
- Inform client subscribers about the modifications of the Policy.
- Establish the mechanisms for the generation and custody of relevant information in the activities described, protecting them against loss, destruction or falsification.
- Respond for non-compliance with the provisions of this policy and, where applicable.
- All the people involved in the management and administration of the service are obliged to keep secret all the information managed by ANF AC, having signed the corresponding confidentiality agreement.
- Guarantee the confidentiality of communications and electronic documents in custody, using strong encryption techniques when applicable.
- Information regarding the services provided to third parties will not be provided, except in compliance with a court order.

8.1.1. Financial liability

It is applied within the limits established in the current Electronic Signature Law.

8.1.2. Disclaimer

ANF AC will not be responsible in any case when faced with any of these circumstances:

- Damages caused by external attacks on them, provided that they have applied due diligence according to the state of the art at all times, and have acted in accordance with the provisions of this policy and current legislation, where applicable.
- State of War, natural disasters, defective operation of electrical services, telematic and/or telephone networks or computer equipment used by the client subscriber or by Third Parties, or any other case of force majeure.
- For improper or fraudulent use of the service.
- For the improper use of the information contained in the Certificate or in the CRL.
- For the content of the messages or documents used.
- In relation to actions or omissions of the Client.
- Lack of veracity of the information provided for the provision of the service.
- Negligence in the conservation of your access data to the service, in the assurance of its confidentiality and in the protection of all access or disclosure.
- Exceeding the use of the service, as provided in current regulations and in this policy.

ANF AC does not review the contents of the electronic documents received for their preservation, it intervenes as a mere service provider, therefore, the intervention of ANF AC cannot presuppose adherence or responsibility for its content.

8.2. Subscriber obligations

- Respect the provisions of this Policy, Terms and Conditions, and commitments assumed in the Contract for the Provision of Services.
- Protect the credentials that allow access to the ANF AC conservation platform.
- Respect the provisions of the contractual documents signed with ANF AC.
- Report any security incident as soon as it is identified.
- Transfer electronic documents that meet the technical and organizational requirements established by ANF AC. Especially, when you transfer data authenticated by electronic signature, applying valid electronic signatures.
- Reverse engineering and troubleshooting of system logic is prohibited.
- The objects must meet the format requirements established in control SS.3.5 of annex A of ETSI TS 102 573
- Send the objects accurately and completely, in accordance with the requirements established in the Information Security Policy of ANF AC.

8.3. Relying third party obligations

It is the obligation of third parties who trust to comply with the provisions of current regulations and, in addition:

- Prior to placing your trust, proceed to the qualified validation of the signatures and seals that authenticate the evidence and probative documents, using a qualified service of electronic signatures and seals.
- Take into account the limitations on the use of the service, as indicated in this Certification Policy.
- Report any security incident as soon as it is identified.
- Consider other precautions described in agreements or other sites.

9. Service termination

ANF AC has a Termination Plan OID 1.3.6.1.4.1.18332.1.9.1.11

9.1. Actions prior to cessation of activity

In the event of cessation of its activity as a Trust Service Provider, ANF AC will carry out the following actions with a minimum of two months in advance, or in as short a period of time as possible in case of compromise, loss or suspicion of password compromise private security used to authenticate evidence and probative documents, as well as stamping of qualified electronic time stamps and OCSP validation responses.

9.1.1. Communication to interested parties

Inform all customers and other entities with whom there are agreements or other forms of established relationships of the termination, including trusted service providers and relevant authorities such as supervisory bodies. In addition, this information will be made available to other trusted parties.

9.1.2. Notifications to the Supervisory Body

Notify the Supervisory Body competent in matters of eIDAS qualified services, the cessation of its activity, as well as any other relevant circumstance related to the cessation of activity.

Make available to the competent Supervisory Body, information on events and logs so that it takes charge of their custody during the rest of the committed period.

By virtue of the agreement established with the Association of Qualified Trust Service Providers of Spain, deposit information on events and logs for it to take care of their custody for the rest of the committed and/or legally established period.

9.1.3. Transfer of obligations

Transfer the obligations to a trusted party to keep all the information necessary to provide evidence of operation for a reasonable period, unless it can be shown that ANF AC does not have this information.

ANF AC will compile all the information referred to, and will transfer it to a trusted party with whom there is an agreement to execute the Cessation Plan in case of bankruptcy.

When a cessation of activity occurs without implying a bankruptcy situation, all the registered information will be stored without the need to transfer it to a trusted party.

9.1.4. Management of service signature keys

Destroy both the private keys and the backup copies of the signature certificates and electronic seals used by ANF AC to provide the service, so that they cannot be recovered. This operation will be executed following the procedure established in the corresponding policy.

Signing keys will always be destroyed upon removal of the cryptographic device that contains them. This destruction does not necessarily affect all physical copies of the private key. Only the physical copy of the key stored in the cryptographic device in question will be destroyed.

9.1.5. Transfer of service management

The transfer of service management is not contemplated.

9.2. Obligations after termination

ANF AC shall proceed to:

- Notify the affected entities; and
- transfer of obligations to other parties

ANF AC will keep your public key available to trusted parties for a period of no less than fifteen years.

These obligations will be carried out by publishing on the website https://www.anf.es

if a cessation of activity occurs without implying a bankruptcy situation. In the event of bankruptcy, these obligations will be assumed by a trusted party by virtue of the agreement established with the Association of Qualified Trust Service Providers of Spain.

10. Responsibility limitations

10.1. Warranties and warranty limitations

ANF AC may limit its liability by including limits on the use of the service, and limits on the value of the transactions for which the service can be used.

10.2. Responsibilities disclaimer

ANF AC does not assume any responsibility in case of loss or damage:

- Damages caused by external attacks on them, provided that they have applied due diligence according to the state of the art at all times, and have acted in accordance with the provisions of this policy and current legislation, where applicable.
- State of War, natural disasters, defective operation of electrical services, telematic and/or telephone networks or computer equipment used by the client subscriber or by Third Parties, or any other case of force majeure.
- For improper or fraudulent use of the service.
- For the improper use of the information contained in the Certificate or in the CRL.
- For the content of the messages or documents used.
- In relation to actions or omissions of the subscriber.
- Lack of veracity of the information provided for the provision of the service.
- Negligence in the conservation of your access data to the service, in the assurance of its confidentiality and in the protection of all access or disclosure.
- Caused by the recipient or bona fide third parties if the recipient of the documents delivered electronically does not check or take into account the restrictions that appear in the service regarding their possible uses.
- Caused by the use of the service that exceeds the limits established in the certificate used by ANF AC for the provision of the service or by this policy.
- Caused by placing trust without carrying out the required qualified validations, using a qualified service for validating electronic signatures and seals.

11. Terms and conditions

ANF AC makes this policy available to subscribers to the service and to all parties who trust it, which includes the terms and conditions under which the conservation service is provided. This document is permanently published in PDF format and can be downloaded at,
https://www.anf.es/repositorio-legal/

11.1. Contracting the service

The service is only provided to subscribers who have formally signed the corresponding contract accepting these terms and conditions, and this certification policy in its entirety.

The service modality provided corresponds to the WTS profile defined in ETSI TS 119 511 for long-term conservation and temporary storage. The duration of the conservation and storage is for the duration of the contract signed between ANF AC and the subscriber of the service.

11.2. Constitution of the preservation deposit

This service offers a platform for the safe preservation and storage of data and long-term evidence. The solution guarantees permanent access and full recovery of the stored documents, manages the evidence that allows to demonstrate the integrity of the stored documents.

In the event that the subscriber assumes the commitment to participate in the preservation process, they must provide an AdES LTV (long-term validation) form.

In the event that the subscriber delivers data that has been previously authenticated by electronic signature or seal, whether it is a basic level BES, or LT, or LTV, prior to its acceptance, the conservation service will proceed to its validation. If the result of the validation is INDETERMINATE or TOTAL FAILURE, the deposit will not be accepted and the data object received will be destroyed.

In the event that it is not possible to collect and verify all validation data, the retention request will be cancelled and the received data object will be destroyed.

The preservation service does not analyze the content of data objects submitted by the subscriber for preservation. In the event that the data object is only a hash, it is not possible to verify the correspondence of that hash, not even if it corresponds to a hash, nor if the calculation carried out to obtain it has been correct. ANF AC is not responsible for guaranteeing the association of a hash with any document.

ANF AC advises its subscribers that a hash allows proof of the existence of a data object, but only while the algorithm used to obtain it is secure.

11.3. Availability of electronic documents

Once the delivery is constituted, the WTS conservation platform maintains custody of the document and assumes control of access to it and the long term of preservation, availability is permanent electronically.

11.4. Portability - Import

As specified in section 6.7 “Portability – Import” of this document.

11.5. Service availability

The platform will be available 24 hours a day, 7 days a week, understanding availability as the ability to access the service by the authorized user who requests it, regardless of the speed or pace at which it is subsequently provided, and always prior identification with conformity.

This availability, measured in a period of one month, in no case may be less than 99.9%.

The terms and conditions of the service level agreement are detailed in the SLA document (Service level Agreement).

11.6. Information Security Management System

ANF AC guarantees authenticity, integrity of the information, exclusive access control to duly authorized persons, and its confidentiality.

11.7. Legal terms

The relationship between ANF AC and the service subscriber is governed exclusively by Spanish law.

The following standards are explicitly assumed to apply:

- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) and by Repealing Directive 1999/93/EC.
- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
- Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which Directive 95/46/CE (General Data Protection Regulation) is repealed.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.
- Ley 6/2020 reguladora de determinados aspectos de los servicios electrónicos de confianza.

11.8. Conflict resolution

Any controversy derived from this contract or legal act, as well as those that derive from it or are related to it -including any question related to its existence, validity, termination, interpretation or execution- will be definitively resolved through arbitration of Law, administered by the Arbitration Court of the Distribution Business Council (TACED), in accordance with its Arbitration Regulations in force on the date of submission of the arbitration request. The Arbitral Tribunal designated for this purpose will be made up of a single arbitrator and the seat of arbitration and substantive law applicable to the solution of the dispute, will be those corresponding to the domicile of TACED, http://www.taced.es

12. Review procedure and modifications

The review process of this policy has a minimum annual frequency, and whenever something new occurs that requires its review.

A modification of this document will be made whenever it is justified from a technical and legal point of view. A version control of the document is applied, specifying the date of approval and publication, being valid from the moment of its publication.

A control of modifications is established, to guarantee, in any case, that the resulting specifications meet the requirements that are intended to be covered, that caused the change, and that they are in harmony with the CPS and ANF AC addendum.

The implications that the change of specifications has on the parties that rely on it are established, and the need to notify them of said modifications is foreseen.

12.1. Publication and notification procedure

This policy, the ANF AC certification practices statement and addendum, is published and permanently updated, along with its revision history, on the website,

https://www.anf.es/repositorio-legal/

12.2. Policy approval procedure

The members of the Governing Board of the PKI are competent to approve the approval of this policy.

13. Financial capability

13.1. Compensation to third parties who rely on the service

ANF AC has sufficient financial resources to face the risk of liability for damages to the users of its services and to third parties, however, its liability in the exercise of PCSC activity as defined in ETSI EN 319 401 art. 7.1.1.c, is guaranteed by Professional Civil Liability Insurance with a coverage of,

FIVE MILLION EUROS (€5,000,000)

13.2. Trust relations

ANF AC does not act as a fiduciary agent or representative in any way of subscribers or third parties who trust in the provision of their trust services.

13.3. Audits

ANF AC guarantees the performance of periodic audits of the established processes and procedures. These audits will be carried out both internally and by independent auditors officially accredited to carry out eIDAS compliance audits.