Qualified signature preservation service and Qualified Electronic Seals (QEs)

Statement of Service Practices and Policy

Conservation

Certification ad
6- Madrid
(Spain) adas
from Spain)
International +34 933 935 946
Web: www.anf.es

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

Conservation Policy and Practice Statement

OID 1.3.6.1.4.1.18332.61

Security level

Public Document

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

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

Web: www.anf.es

Document control

Document name and identification

Document name	Practice Statement of the Qualified Service for the Preservation of Signatures and Qualified Electronic Seals (QEs)		
Version	1.2		
OID	1.3.6.1.4.1.18332.56.1.1		
Approval date	04/23/2021	**Publication date**	04/23/2021

Reviews

Version	Changes	Approval	Publication
1.2.	Profile review with change from WTS to WST	04/23/2021	04/23/2021
1.1.	Annual review	11/28/2020	11/28/2020
1.0.	Initial release. Creation of the document.	01/15/2020	01/15/2020

INDEX

1. Introduction

ANF Certification Authority [ANF AC] is a legal entity established under Organic Law 1/2002 of March 22 and registered in the Ministry of the Interior with national number 171.443 and NIF 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 branch iso.org.dod.internet.private.enterprise (*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 of the European Parliament, and with Spanish Law 59/2003 on Electronic Signature. ANF AC's PKI is in compliance with ETSI EN319 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 digitization software 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 databases.

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 Trust Service Provider 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*", Defines the procedural and operational requirements to which 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 stamps

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 trusthttps://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 stamps.

1.1.1. Identifiers of each service mode

In order to identify the qualified conservation services in their different modalities, ANF AC has assigned them the following identifiers (OID).

Preservation and storage of qualified electronic signatures	1.3.6.1.4.1.18332.61.5
Conservation and storage of Qualified Electronic Stamps	1.3.6.1.4.1.18332.61.6

The same profile will apply throughout the retention period.

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

1.1.2. Electronic evidence

The electronic evidence is generated by including metadata in the header of the data files, and by signing the data transmitted by the subscriber, using an ANF AC Qualified Electronic Seal certificate to prepare:

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

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 conservation and storage platform.

1.1.4. Validation

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

1.1.5. Qualified Electronic Time Stamping

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

1.2. Document name and identification

Document name	Policy for the Qualified Service for the preservation of qualified electronic signatures and for the Qualified Service for the preservation of qualified electronic stamps		
Version	1.0		
OID policy status	APPROVED and CURRENT		
	1.3.6.1.4.1.18332.61		
Approval date	01/15/2020	**Publication date**	01/15/2020

The identifier of this Certification 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. Parts of the PKI

As defined in the CPS of ANF AC.

1.4. Area of application

1.4.1. Permitted uses

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

1.4.2. Limits of use

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

1.4.3. Prohibited uses

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

1.5. Contact details of the Certification Entity

As defined in the CPS of ANF AC.

1.6. Definitions and acronyms

In addition to those outlined in the CPS of ANF AC, for the purposes of this service the following terms and abbreviations 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 Qualified Provider that provides information on the status of the certificate.
- **Conservation Client:** 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 evidence of the existence of data for long periods of time, despite the obsolescence of cryptographic components or loss of the ability to verify the validity status of the public key certificates used.
- **Dual control:** procedure that requires the intervention of two operators.
- **Data:** they are actual binary / octet objects on which the preservation and storage process is performed.
- **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 long-term preservation of the document.
- **Duration of evidence:** is the expected time that the preservation service expects the evidence to 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.
- **Conservation evidence:** are the events obtained that have been generated to achieve the preservation of the data.
- **AdES signature level LT:** This format includes TimeStamping, all the certification and revocation information (signed OCSP response) necessary to validate the signature over time.
- **Signature AdES LTA level:** 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 identification of the signer, has been created using data from the creation of the electronic signature that the signer can use, with a high

level of trust, under its exclusive control, and is linked to the signed or sealed data of such that any subsequent modification thereof is detectable. The advanced electronic signature is always generated using a valid 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 - Unique identifier of a set of data submitted to a preservation service.
- **Conservation interface:** component that implements the preservation protocol on the conservation 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:** They are data encapsulated in other data.
- **Conservation object:** typed data object that is sent, processed, or retrieved from a retention service.
- **Conservation Profile / Model:** It is the way in which the service provider implements it, in the case of this policy the profile is WST (*conservation and storage).*
- **Retention period:** the period of time during which evidence that occurs asynchronously can be retrieved from the service.
- **Conservation and storage evidence policy:** set of rules that specify the requirements and the internal process to generate or how to validate a preservation evidence.
- **Proof of existence:** evidence that proves that an object existed at a specific date / time.
- **Integrity test:** evidence that the data has not been altered since it was protected.
- **Re-stamping / Re-sealing:** Preservation enhancement that is carried out on a conservation evidence 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 pulled from one preservation service, including submission data object (SubDO), preservation evidence, and preservation-related metadata, allowing another preservation service to import to continue to achieve the preservation objective based on this information.
- **Provider / Provider of conservation and 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.

- **Test log:** Data unit that allows to prove the existence at a given moment, of a stored data object.
- **Time Stamp:** data in electronic form that links other electronic data to a particular time by establishing evidence that this data existed at that time.
- **Conservation service:** Service capable of extending the validity status of a digital signature for long periods of time and / or of providing evidence of the existence of data for long periods of time.
- **Validation service:** Service that validates an electronic signature / seal, certificates used, etc.
- **Subscriber / Subscriber:** It is the natural or legal person that contracts the long-term conservation service from ANF AC.

1.6.2. Acronyms

- **2FA:** Double Factor Authentication (multifactor).
- **AdES:** Advanced Electronic Signature.
- **AUG:** Magnification target.
- **LT:** Long-time. Long term.
- **LTA:** Long-time archive. Long-term archive.
- **OCSP:** On-line Certificate Status Protocol.
- **OTP:** One-Time-Password.
- **PC:** Certification Policies.
- **PCSC:** Qualified Trust Service Provider, in the context of this policy ANF AC is the PCSC of reference.
- **PKI:** Public key infrastructure.
- **POC:** Preservation object container.
- **PRP:** Conservation service protocol.
- **PSP:** Conservation service provider.
- **SCA:** Strong customer authentication (*Strong Customer Authentication)*.
- **SigS:** Electronic signature / stamp creation service.
- **ISMS:** Information Security Management System.
- **SSL:** Secure ports layer. They are cryptographic protocols, which provide secure communications over a network and authenticate the server that provides service.
- **SubDO:** Shipping data object.

- **TLS:** Transport layer security. They are cryptographic protocols, which provide secure communications over a network and authenticate the parties involved in the communication.
- **TSP:** Trust Service Provider.
- **Waltz:** Validation Service.
- **WST:** Conservation service profile with storage.

2. Repositories and publication of information

2.1. Repositories

As defined in the CPS of ANF AC.

2.2. Publication of the 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, supports signature, object storage identifies additional targets and controls that specifically comply with the potential risks associated with signing and / or storing additional relevant objects that specifically meet 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 (RGPD) and the Organic Law on Data Protection and Guarantee of Digital Rights, having prepared a Data Protection Impact Assessment (EIPD) with a low risk level result. What's more,

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 responsibilities are established.

ANF AC, manages:

or Risk Management Plan, OID 1.3.6.1.4.1.18333.13.2.1; or Risk Assessment, OID 1.3.6.1.4.1.18332.101.80.6.3; or Risk Matrix, OID 1.3.6.1.4.1.18333.101.80.6.1;
or Disaster Recovery and Continuity Plan, OID 1.3.6.1.4.1.18332.13.1.1;

or Plan of cessation of activity, 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 they may cause, and the safeguards applied by the organization.

Private signature keys are classified as sensitive data that must be protected by special measures.

The data objects are classified as confidential 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 is managed in the long-term conservation and storage platform.

The provisions of the Policy for the reporting and treatment of OID security incidents apply. 1.3.6.1.4.1.18332.101.45.30

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 person in one of the offices of the Recognized Registration Authorities.
- By person in the ANF AC offices.

ANF AC has an Incident Registry in which all incidents that have occurred are registered with the certificates issued, and the evidence obtained. These incidents are recorded, analyzed and solved according to the procedures of the Information Security Management System of ANF AC.

The Security Officer determines the severity of the incident and appoints a manager and, in the event of relevant security incidents, reports to the PKI Governing Board.

ANF AC has a Physical and Environmental Security Policy OID 1.3.6.1.4.1.18332.101.45.14 that, among other issues, establishes requirements for physical access to the organization's facilities and use of assets.

The organization's IT systems have controls to protect against attacks and malicious software. There is a versioning control procedure, project control and all processes and technology are documented and classified.

Periodically, port scans are carried out and server configurations are checked and the logs are studied in order to detect suspicious actions of access attempts or unauthorized data processing.

The systems are regularly updated to the latest versions classified as stable and for exploitation.

The servers have advanced technology to control improper access, antivirus system, firewall, etc. Periodic LOG checks are carried out to detect attempted aggression.

All personnel submit to a confidentiality commitment and carry out Continuous Training.

In teleworking, an SSL connection and identification through a qualified electronic signature certificate are required.

ANF AC, the Contingency and Disaster Recovery Plan, is periodically tested.

3.2. Using the private key

Subscribers who have a qualified electronic signature certificate can send the signed documents. Otherwise, at least the subscriber must use an ANF AC application for the

secure download of documents that generates hash of the data object in its terminal and includes SSL communications for sending to the conservation 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 accordance with QSCD in accordance with the eIDAS Regulation, in which case the electronic signatures are qualified signatures. .

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

3.3. Maintenance of the signature during the storage period

In order to ensure that electronic signatures / seals are maintained so that their validity can be verified for the entire storage period. ANF AC has implemented technical procedures and organizational measures, at least:

a) Technical measures

All signatures include information that allows the validation of the signature (*for example, the certificate path of a known trust point, for example, root CA and revocation information)* and a confidence indicator (*e.g. timestamp)* from the moment when 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 the transmission of data, the platform has the following conservation clients:

- Web application for personal users, API
- for automation between systems.
-

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

All data objects received 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 storage have been accepted, are electronically signed AdES LT by ANF AC. A certificate of acceptance of conservation and storage OID 1.3.6.1.4.1.18332.62.4 is delivered to the subscriber

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 process is applied

re-stamping using archival timestamps, in accordance with standards ETSI 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 data centers 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. The service is guaranteed with an SLA level higher than 99%.

3.4. Access to information, publication and traceability

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 endowed with credentials based on qualified electronic signature certificates.

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

The authorized operators, prior to accessing the information, sign an act that details the request and the actions carried out.

The systems have procedures to perform 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 for consultation or obtaining 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 integrity breach is detected.

All the information stored is authenticated at least with an advanced electronic signature of long term in AdES LT format.

The necessary techniques are applied (if necessary, re-stamped using strong cryptographic procedure) to guarantee the maintenance of the signature throughout the storage period.

3.6. Firm

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

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

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

3.8. Electronic time stamping

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

3.9. Readability

The long-term conservation platform of ANF AC only accepts electronic documents in PDF formats. The service does not include the process of converting the analog object to digital / electronic format.

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

a) Technical measures

- The conservation platform is configured to reject all data objects whose format is not accepted according to the specification published on the same platform.

- Long-term storage and preservation platform includes display system of documents and electronic signatures.
- When there is a risk that a specific display system will become obsolete, all affected data was reliably copied 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.
- If data is accepted in XML format, acceptable style sheets will be referenced and included in the signature, or standard syntax with fully defined semantics (eg XBRL) will be used.

b) Organizational measures

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

3.10. Security of the information

In order to ensure that the media where data objects are stored can withstand the passage of time, such as deterioration of the medium that stores them or even hacker attacks or fortuitous corruption of information and, especially, the obsolescence of the cryptographic components used for their preservation, there are:

- S3 storage system, using bucket technology. This technology automatically generates online, support copies of 100% of the data objects. These copies are located on servers installed in a different geographical area from the data in operation. 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 master key that rotates periodically. The symmetric cryptographic algorithm used is 256-bit Advanced Encryption Standard (AES-256). When the
- information is received, prior to its acceptance, an antivirus is used to verify 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 are signed and, where appropriate, the signature is validated. In case of non-conformity, the conservation is rejected.
- In case of acceptance of conservation, the long-term electronic seal of ANF AC is stamped, the cryptographic components used are registered in order to carry out an obsolescence control and, where appropriate, re-stamp those that are necessary, and issues acceptance certificate.
- When data objects are stored whose format may include changes in the presentation or any modification not detectable by integrity checks (*E.g. Word documents that allow the inclusion of macros, scripts or hidden code capable of modifying the presentation of the data object),*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 guarantee the confidentiality of information, 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. Conservation protocol

The service has been developed by ANF AC's 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

You can get the traces of all operations related to a specific preservation identifier, as defined in the operation *RetrieveTrace* according to ETSI TS 119 512

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

In the event that the subscriber requests the elimination of a conservation order before the end of the conservation period, the request will be made by a person authorized by the subscriber and that they provide the corresponding supporting document.

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

The elimination does not necessarily entail the destruction of the information, the service subscription contract will establish whether the scope of the elimination is destruction or the 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 limited use, has the sole objective of proving the correct provision of the service by ANF AC, or to attend an order from a Court of Justice.

3.13. Notification protocol

For each delivery of the data object made by the subscriber, the Conservation service generates an act in which it is specified whether the service has been accepted or rejected and, where appropriate, validation of the signature / seal or generation of the ANF electronic seal. AC. In case of rejection, the cause is specified.

The subscriber on demand can download data objects, preservation evidence or minutes indicated above through the service console. Only accessible to persons authorized by the subscriber.

Notification is not foreseen.

3.14. Reports and exchanges with the authorities

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

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

The representative of the authority must identify himself 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 CPS of ANF AC.

A secure channel is used to send data objects to the Authorities, so that the user remote and the server is authenticated, the integrity and confidentiality of the communications are protected against vulnerabilities of the networks. (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. Roles of trust

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 staff have signed the corresponding confidentiality commitment, a commitment that lasts even after they leave the organization.

Periodically ANF AC conducts an internal audit 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 personnel 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:

Policy of Roles and Responsibilities OID
1.3.6.1.4.1.18332.38.1, Disciplinary Sanctions Policy OID
1.3.6.1.4.1.18332.39.14.2 Internal Regulations OID
1.3.6.1.4.1.18332.101.80.5
OID training plan 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 of highly trusted personnel of ANF AC's senior management have been established:

Head of identity verification

They are 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

It is personnel assigned to the technical area of ANF AC. It assumes the responsibility of ensuring the full operability of the systems, carrying out installation, configuration and maintenance tasks for the management of services. Specific requirements:

They do not have access to the CA keys.
They do not have access to the LOGs of the CA. It will be avoided by user properties of the CA software.

They are authenticated via SmartCard or USB token with CA software and this software will not support other alternate authentication method.

Responsible for access codes to the QSCD

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

These trusted personnel are the only ones authorized and authorized to perform backup, preservation and recovery operations on the signature key. Always under dual control and in a physically safe environment.

Systems operator

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

System auditor

Authorized to view files and audit the 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 should be responsible for:

Check incident and event tracking

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 ANF AC Security Policy. In addition, it will take care of:

Verify the existence of all the required and numbered documentation
Check the coherence 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 their suitability for the role required by the organization.

Code of conduct for members and suppliers OID 1.3.6.1.4.1.18332.101.45.1

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

5. Roles of trust

Subscribers / Subscribers

Natural or legal persons who contract this long-term conservation and storage service.

Trusting 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 Practices of ANF AC.

6. Identification and authentication

6.1. Initial identification

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

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.
By means of a certificate of a qualified electronic signature or a valid qualified electronic seal.
Using any of the procedures established in art. 24 of the eIDAS Regulation.

By means of 2FA in which one of the factors is based on a procedure qualified by the Court of Justice or legally recognized at national level 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) may be carried out using one of the means of identification with a low security level (2).

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

6.2. Authentication

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

7. 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 the electronic documents to permanent audits in order to guarantee the integrity, authenticity and legibility of the files guarded as required. over time.

This service is provided during the period of time contracted by the client subscriber, after contracting the information is permanently destroyed.

The conservation service guarantees permanent access, the full recovery of the documents, and the management of the evidences that allow to demonstrate the integrity of the documents in custody.

7.1. Data object download

The conservation platform has two procedures so that subscribers can transmit the data objects. The conservation clients available are:

a) End user console on Web server.

b) API to establish communication between the subscriber's automated system and the ANF AC conservation platform.

In any of the cases, SSL / TLS communication protocol is used to guarantee data privacy and the subscriber uses credentials to authenticate before the conservation platform.

One or more Shipment Data Objects (SubDO) are allowed to be preserved under a specific preservation profile.

7.2. Initial protection

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

Verification of identity of the subscriber. Only subscribers of the service can send data.
Data object format validity check. Only formats accepted by the platform can be accepted.

In the event that the electronic document is signed, the signature or electronic seal that authenticates it will be validated. In this process, a qualified system of validation of signatures and electronic stamps is used.
If the electronic document is transmitted associated with a hash, the correspondence of the hash with the data object will be checked.
Evidence is obtained of the conformity or failure of the signature or hash validation process carried out in the previous steps. 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 to unify permanent audit process.
The signature applied at least is an advanced electronic signature prepared with a qualified certificate, and in accordance with 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 different geographical location

7.3. Access to information, traceability.

The long-term conservation and storage platform manages a metadata service that facilitates its search and location. The metadata includes information related 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 their responsibility in the transaction carried out. The platform has a search and publication system, from a private web environment and available 24x7x365.

7.4. Proceedings

The platform allows associating 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.

7.5. Document audit, re-stamped (*augmentation)*

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

An integrity audit of all stored documents is carried out periodically.

Re-ringing: The evolution of the state of the art and the security of the algorithms and cryptographic procedures used in their authentication is monitored, in case of entry into risk, the evidence is re-sealed by applying a qualified electronic time stamp that use cryptographic components qualified as secure in accordance with ETSI TS 119 312.

7.6. Protection

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

Signing keys are kept and used at a minimum, on 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 putting them into operation.

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

Full support copies of the audit trail 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 master key that rotates periodically, the symmetric cryptographic algorithm used is Advanced Encryption Standard 256 bits (AES-256).

Event logs (LOGs) are generated that allow the necessary information to be established for audit tests.

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

7.7. 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 any of the formats defined in Annex TR-ESOR-F of BSI of the Technical Guide BSI 03125 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 preliminary budget will be made, the cost of which will depend on the volume and complexity of the information, the provision of service will require its acceptance by the subscriber.

Application procedure:

It must be requested by the legal representative of the subscriber:

or The request must be sent by email to support@anf.esand it will be signed electronically.

or It will indicate the type of format in which you want to receive or send the data.

or It will indicate the person or persons authorized to download or send the information.

or You will pay the rates that you have previously accepted by budget issued by ANF AC.

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

The 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 to be included in the export-import.

7.8. End of the conservation period

The provision of the service establishes a WST profile [*conservation and storage]*. The term of duration corresponds to the period contracted by the subscriber.

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

8. Obligations and responsibilities

8.1. Obligations of the service provider

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

Respect the provisions of this Policy.
Implements ETSI TS 119 312 monitoring controls
A control is carried out on the state of the cryptographic technique and its advances.
Protect your private keys safely.
Issue qualified electronic time stamps whose minimum content is 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.
Qualified electronic signature remote service.
Obtain OCSP responses signed by the issuing PCSC whose minimum content is 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 customer subscribers about changes to the Policy.
Establish the mechanisms for the generation and custody of the 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 all the information managed by ANF AC secret, having signed the corresponding confidentiality commitment.
Guarantee the confidentiality of communications and electronic documents in custody, using strong encryption techniques when applicable.
No information will be provided regarding the services provided to third parties, except in compliance with a court order.

8.1.1. Financial responsibility

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

8.1.2. Liability exemption

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 due diligence has been applied according to the state of the art at all times, and has acted in accordance with the provisions of this policy and current legislation, where applicable.
State of War, natural disasters, malfunction 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 the 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.
Excess use of the service, in accordance with current regulations and this policy.

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

8.2. Subscriber obligations

Respect the provisions of this Policy, Terms and Conditions, and commitments assumed in the Service Provision Agreement.
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. In particular, 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. Obligations of trusting third parties

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

Before placing your trust, proceed to the qualified validation of the signatures and stamps that they authenticate the evidences and supporting documents, using a qualified service of electronic signatures and seals.

Take into account the limitations in the use of the service, as indicated in this Certification Policy.

Report any security incident as soon as it is identified.

Take into consideration other precautions described in agreements or other sites.

9. Termination of service

ANF AC has a Dismissal Plan OID 1.3.6.1.4.1.18332.1.9.1.11

9.1. Actions prior to the cessation of activity

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

9.1.1. Communication to interested parties

Report the termination to all clients and other entities with which there are agreements or other forms of relationships established, including trust 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 competent Supervisory Body 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 can take 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 so that it takes charge of their custody during the rest of the committed and / or legally established period.

9.1.3. Transfer of obligations

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

ANF AC will collect all the information referred to, and will transfer it to a trusted party with which it has an agreement to execute the Dismissal Plan in the event of bankruptcy.

When there is a cessation of activity 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 signing keys

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

The signing keys will always be destroyed when removing 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 on 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 the cessation of activity

Will be performed:

notification to affected entities; Y
transfer of obligations to other parties

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

These obligations will be carried out by posting on the website

https://www.anf.es

if there is a cessation of activity without implying a bankruptcy situation. In the event of a 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. Liability 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. Disclaimer of responsibilities

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

- Damages caused by external attacks on them, provided that due diligence has been applied according to the state of the art at all times, and has acted in accordance with the provisions of this policy and current legislation, where applicable.
- State of War, natural disasters, malfunction 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 the 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 to the recipient or third parties in good faith 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 performing the required qualified validations, using a qualified service for the validation of signatures and electronic seals.
-

eleven. Terms and Conditions

ANF AC, makes this policy that includes the terms and conditions in which the conservation service is provided to the subscribers of the service and to all the parties that trust. 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 WST profile defined in ETSI TS 119 511 for conservation and long-term storage. The duration of 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 conservation deposit

This service offers a platform for the preservation and secure storage of data and evidence in the long term. The solution guarantees permanent access and comprehensive retrieval of stored documents, manages the evidences that allow to demonstrate the integrity of the stored documents.

In the event that the subscriber undertakes 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 means of an electronic signature or seal, be it 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 UNDETERMINED or TOTAL FAILURE, the deposit will not be accepted and the received data object will be destroyed.

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

The preservation service does not analyze the content of data objects sent by the subscriber for preservation. In the case that the data object is only a hash, it is not possible to check the correspondence of that hash, not even if it corresponds to a hash, or 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 warns its subscribers that a hash allows to prove 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 WST conservation platform maintains custody of the document and assumes control of access to it and the long term of preservation, the availability is permanent via electronic means.

11.4. Portability - Import

As specified in section 7.7 "Portability - Import" of this document.

11.5. Service availability

The platform will be available 24 hours a day, 7 days a week, understanding by availability, 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 after identification with conformity.

This availability, measured in a period of one month, may in no case 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 Management System Security

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 subscriber of the service is governed exclusively by Spanish law.

The following rules are explicitly assumed to apply:

- 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 (eIDAS Regulation) and by which Directive 1999/93 / EC is repealed.
- 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 repeals Directive 95/46 / EC (General Data Protection Regulation).
- Law 34/2002, of July 11, on services of the information society and electronic commerce.

- Law 59/2003 of electronic signature.

11.8. Conflict resolution

Any controversy derived from this contract or legal act, as well as those that derive from or are related to it -including any question regarding its existence, validity, termination, interpretation or execution- will be definitively resolved through arbitration of Law, administered by 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 appointed for this purpose will be composed of a single arbitrator and the seat of the arbitration and substantive law applicable to the solution of the dispute, will be those corresponding to the domicile of the TACED,http://www.taced.es

12. Review and modification procedure

The review process of this policy has a minimum annual periodicity, and whenever there is something new 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 addendum of ANF AC.

The implications that the change in specifications have on relying parties are established, and the need to notify such modifications is foreseen.

12.1. Publication and notification procedure

This policy, the declaration of certification practices and addendum of ANF AC, is published and permanently updated, together 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 agree to the approval of this politics.

13. Financial capability

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

13.1. Indemnification to third parties who trust 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 responsibility in the exercise of the activity of PCSC as defined in ETSI EN 319 401 art. 7.1.1.c, is guaranteed by a Professional Civil Liability Insurance with a coverage of,

FIVE MILLION EUROS (€ 5,000,000)

13.2. Fiduciary relationships

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.

14. Conflict resolution

14.1. Extrajudicial conflict resolution

ANF AC formally submits in its declaration of Terms and Conditions to an institutional arbitration procedure, of the TACED Arbitration Court.

Any controversy derived from this contract or legal act, as well as those that derive from or are related to it -including any question regarding its existence, validity, termination, interpretation or execution- will be definitively resolved through arbitration of Law, administered by 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 appointed for this purpose will be composed of a single arbitrator and the seat of the arbitration and substantive law applicable to the solution of the dispute, will be those corresponding to the domicile of the TACED,http://www.taced.es

14.2. Competent jurisdiction

The relationship between ANF AC and the relying parties is governed exclusively by Spanish law.