Qualified Delivery Service Policy
Certified Electronics

7510

© ANF Certification Authority

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

Telephone: 902 902 172 (calls from Spain)

International (+34) 933 935 946

Web: www.anf.es

Security level

Public

Important announcement

This document is the property of ANF Certification Authority

Its reproduction and dissemination is prohibited without the express authorization of ANF Certification Authority

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 name and identification (*section 1.2)*

Document name	Qualified Certified Electronic Delivery Service Policy QERDS Policy v.1.2.pdf		
file name			
Version	1.1		
OID policy status	Current		
	1.3.6.1.4.1.18332.60		
Approval date	12/04/2020	**Author**	F. Díaz Vilches

The identifier of this Certification Policy will only be changed if there are substantial changes that affect its applicability.

Review and approval		
reviewed by	Pablo Diaz	12/04/2020
Approved by	MariCarmen Mateo	12/04/2020

History of changes			
Version	**Date**	**Description of the cause**	**Responsable**
1.0	01/15/2020	New Policy for the Qualified Certified Electronic Delivery Service.	F. Diaz
1.1	10/01/2020	Inclusion of references to ETSI EN 319 521	F. Diaz
1.2.	12/04/2020	Review after audit.	F. Diaz

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 OID's 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 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)* Y **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 EN 319 531** *“Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Registered Electronic - Mail Service Providers ”;* **ETSI EN 319 532** *“Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Registered Electronic - Mail Service Providers”.*

ANF AC, uses the cryptographic techniques indicated in the TS 119 312 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.

ANF AC is a provider of the “Qualified Certified Electronic Delivery Service” (QeRDS) provided for in article 44 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.

This document is the **Qualified Certified Electronic Delivery Service Policy** 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 document 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 services in any of the

Communication channels available at all times, email or others available that allow ERDS communication:

- Certified electronic delivery service.
- Services related to certified electronic delivery.
  - or Identification of sender and receiver.
  - or Capture of evidences and elaboration of probative document.
  - or Registration and filing of electronic documents.

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 Certification Policy assumes that the reader knows the concepts of PKI, certificate and electronic signature; otherwise, the reader is recommended to learn the above concepts before continuing to read this document.

1.1. Service's description

The Certified Electronic Delivery Service (ERDS) is a service that allows the transmission of data between the sender and the recipients by electronic means, provides evidence regarding the handling of the transmitted data, including proof of sending and receiving the data, and which protects the transmitted data against the risk of loss, theft, damage or any unauthorized alteration.

The communication channel used to make the delivery to the recipient's mailbox can be email (REM) or another, provided that it guarantees the requirements established to be considered ERDS.

For sending and receiving messages, collecting evidence and supporting documents, users have an ERD application / user agent that is available in two modes:

- Web Platform Sign to Sign. API
- Sign to Sign.

Through this application, all users who have a computer terminal or a SmartPhone are compatible to send or receive certified messages in any of its modalities.

The tests consist of the evidences that have been obtained during the service, these evidences and the result of the transaction are collected in a probative document. This document

Evidentiary is a formal statement that includes the intervention of ANF AC as a trusted intermediary party in the receipt of the delivery mandate received from the ordering party and its delivery to the recipient, in this statement the electronic document received and transmitted, identity of the ordering party and of the recipient, as well as all the events that have been generated during the shipping process (evidence of the delivery order by the payer, audit trails of the communication systems, submission of a message, transmission of a message, delivery of a message, rejection of a message, evidence of delivery to the recipient, communication channel used, etc.) specifying the specific moment in which each event occurred and the result obtained.The probative document establishes the modality of service provided and is authenticated by the electronic seal of ANF AC.

Regarding the S&N style functionality in ANF AC's certified delivery platform:

- The service allows the S & N style within its platform, but does not allow it to messages transmitted by another ERDS (REMS).
- The application / user agent has a procedure for the user to accept or reject an incoming S&N message, and help information is provided for its use.
- The application offers the recipient the possibility to establish a specific period for acceptance or rejection of S & N messages, and the recipient is informed of the period.

ANF AC has and offers two types of service:

- ERDS service
- QERDS service

The REMS and QREMS certified email service is part of this service with the only difference being:

- use the SMTP transfer protocol (email),
- offer the option to all users to send and receive messages in MIME format according to RFC 2045 and RFC 5322, and
- receive messages via IMAP or POP. S&F and S&N
- style of operation are supported.

1.1.1. ERDS service

A "Certified Electronic Delivery Service (ERDS hereinafter)" (in English, *Electronic Registered Delivery Service,* ERDS) guarantees the safe and reliable delivery of electronic messages between the parties, which generates evidence of the sending and delivery process for legal purposes.

The level of security in the identification and intervention of the parties is:

Medium / substantial level:

This level corresponds to a configuration of security mechanisms appropriate for most applications. It is suitable for accessing applications classified according to the ENS in the Integrity and Authenticity levels as low or medium risk.

Likewise, the risk foreseen by this level corresponds to the low and substantial security levels of the electronic identification systems of the EU regulation 910/2014. The security levels of the eIDAS regulation apply only to electronic identification systems.

ANF AC intervenes as a certified electronic delivery service provider (ERDSP).

1.1.2. QERDS service

The eIDAS Regulation defines the so-called Qualified Electronic Registered Delivery Service (QERDS), which is a special type of ERDS, in which both the service and its provider must meet a series of additional requirements regarding to conventional ERDS and the entities that provide them.

The level of security in the identification and intervention of the parties is:

High level:

This level corresponds to a configuration of security mechanisms appropriate for applications that require additional measures, based on the risk analysis performed. The risk foreseen by this level corresponds to the guarantee level 4 foreseen in IDABC's Basic Authentication Policy. It is suitable for accessing applications classified according to the ENS in the Integrity and Authenticity levels as high risk.

Likewise, the risk foreseen by this level corresponds to the high security level of the electronic identification systems of the EU regulation 910/2014. The security levels of the eIDAS regulation apply only to electronic identification systems.

The security mechanisms acceptable to all parties are qualified electronic signature certificates, and those that offer the required high level of security.

1.1.3. Identifiers for each service mode

In order to identify the certified delivery services, ANF AC has assigned them the following object identifiers (OID).

ERDS	1.3.6.1.4.1.18332.60.1
QERDS	1.3.6.1.4.1.18332.60.2

1.2. Document name and identification

Qualified Certified Electronic Delivery Service Policy

OID 1.3.6.1.4.1.18332.60

1.3. Parties involved

- Certified Electronic Delivery Service Provider (ERDSP): trusted service provider that provides a registered electronic delivery service, in this case ANF AC.
- Subscriber. It is the responsibility of the client who hires the certified delivery service to act as the originator, sender of the communication.
- User. Application or human interacting with a certified delivery customer.
- Trusting third party. Third parties who, without being the subscriber or the user, are generally recipients, although they may also be authors, or legal experts, or Courts of Justice, are authorized to access the sent message.

1.4. Area of application

1.4.1. Permitted uses

The use of the Qualified Certified Electronic Delivery Service provides the following guarantees:

- Non-repudiation of origin and destination

It ensures that the document comes from the originator from whom it claims to proceed, and is addressed to the recipient to whom it should be sent. This characteristic is obtained through the process of

- identification of the payer / subscriber, and
- of the recipient through the procedures established in section 7 “Identification and authentication of this document”. In this way, it guarantees that the document comes from a certain duly identified subject and is addressed to a recipient whose identity has also been validated.

- Integrity

With the use of the qualified Electronic Signature Certificate or the qualified Electronic Seal certificate, it is possible to verify that the document has not been modified. To ensure integrity, the well-known hash functions are used, which are used whenever an electronic signature or seal is made. The use of this system allows to verify that a signed or sealed message has not been altered between sending and receiving.

1.4.2. Limits of use

In general, as established in the CPS of ANF AC, and specifically:

- The communications and documents whose delivery the ordering party requests must be in accordance with current legislation.
- The payer has the legal capacity to establish communication with the recipient.

1.4.3. Prohibited uses

In general, as established in the CPS of ANF AC, and specifically:

- Deliveries made will be carried out only in accordance with the function and purpose established in this Policy for the Qualified Certified Electronic Delivery Service, and in accordance with current regulations.

- The contracting of the service only admits the use of the service in the scope of activity of the client who contracts the service or the entity to which it is linked, in accordance with the purpose of the service. The client may not, except in the specific agreement with ANF AC, make use of the service for commercial purposes. Commercial use of the service is understood to be any action by which the client offers third parties outside the subscriber owner, for consideration or free of charge, the use of this certified electronic delivery service.

1.5. Contact details of the Certification Entity

As defined in the CPS of ANF AC.

2. 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,

Definitions

- **ERD User Agent / Application:** system consisting of software and / or hardware components through which senders and recipients participate in the exchange of data. Within the scope of this ERDS, the application is Sign to Sign Derlivery Services.
- **Addressee:** It is the natural or legal person to whom the content of the sender payer is addressed.
- **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.
- **Evidentiary document:** document that incorporates all the information related to the order of delivery, evidences that have been generated and moment in time in which they have been produced. The document is authenticated by ANF AC using a long-term electronic seal.
- **Evidence:** are the events that have occurred during the provision of the certified delivery service, the intervening party and the moment in which it occurred.
- **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 electronic signature creation data that the signer can use, with a high level of trust, under his exclusive control, and is linked to the signed or sealed data of such that any subsequent modification thereof is detectable. Within the scope of this ERDS, the advanced electronic signature is always generated using a current qualified electronic certificate.

- **Delivery order:** are the original data that the Originator communicates to the ERDSP to request the provision of the service.
- **Originator:** It is the natural person who orders the certified electronic delivery to the service provider and establishes the requirements for making the delivery. The payer may intervene in his own name and representation, in which case he assumes the role of subscriber holder of the service (sender), or he may intervene on behalf of a third party.
- **Certified Electronic Delivery Service Provider:** is the Certified Electronic Delivery Service Provider (ERDSP). In some usage scenarios, ERDSPs can cooperate

in the transfer of data from a sender to a recipient when they are subscribed to different ERDSPs. See 4-corner and extended models in clauses 4.3 and 4.4 of ETSI EN 319 522-1 [i.6].

- **Qualified Provider of Certified Electronic Delivery Services:** is the QERDSP provider that is qualified, as specified in Regulation (EU) No. 910/2014, for the provision of qualified certified electronic delivery services (QERDS). In the context of this policy, ANF AC assumes this role.

- **Subscriber:** is the natural or legal person who is the sender of the certified electronic delivery (ERD).

- **Transfer:** act of causing the payer's electronic document to successfully cross the border of the recipient's registered electronic delivery.
- **Audit trails:** They are evidences generated by the automated systems that intervene during the provision of the service, they determine the system that has intervened and the moment in which it intervened.

- **Addressee:** Natural or legal person to whom the communication of the payer is directed through the certified delivery service.

Acronyms

- **2FA:** Double Factor Authentication (multifactor)
- **SCA:** Strong customer authentication (*Strong Customer Authentication).*
- **ERD:** Certified electronic delivery.
- **ERDS:** Certified electronic delivery service.
- **ERDSP:** Certified electronic delivery service provider.
- **QERDS:** Qualified certified electronic delivery service.
- **QERDSP:** Qualified provider of certified electronic delivery service.
- **REM:** Registered email.
- **REMS:** Registered email service.
- **QREMS:** Qualified registered email service.
- **QREMSP:** Registered email service provider.
- **OTP:** One-Time-Password
- **PKI:** Public key infrastructure.
- **SSL:** Secure ports layer. They are cryptographic protocols that provide secure communications over a network and authenticate the server that provides service.
- **S&F:** Store and forward
- **S&N:** Store and notify
- **SMTP:** Simple mail transfer protocol
- **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.

- **QTSP:** Qualified Trust Services Provider.

3. Repositories and publication of information

3.1. Repositories

As defined in the CPS of ANF AC.

3.2. Publication of the information

As defined in the CPS of ANF AC.

3.3. Frequency of updates

As defined in the CPS of ANF AC.

3.4. Access controls to repositories

As defined in the CPS of ANF AC.

4. Operational requirements

ANF AC, guarantees that,

- It uses an Information Security Management System (ISMS) certified in the ISO / IEC 27001: 2013 standard, thus ensuring compliance with the security controls in the transmission against risks of loss, theft, damage or any unauthorized modification .
- This policy is defined for the Qualified Certified Electronic Delivery Service, as determined by Regulation (EU) 910/2014 [2].
- This policy is in accordance with the ETSI EN 319 521 standard "*Policy and security requirements for Electronic Registered Delivery Service Providers*", And ETSI EN 319 522"*Electronic Signatures and Infrastructures (ESI) Electronic Registered Delivery Services*".

5. Roles of trust, physical security controls, facilities, management and operations

5.1. Physical and environmental security controls

As defined in the CPS of ANF AC.

5.2. Operational controls

As defined in the CPS of ANF AC.

5.3. Personnel controls

As defined in the CPS of ANF AC, and specifically for the ERDS:

The people who participate in the services provided by ANF AC are personnel under the direction of the organization, and are selected following ANF AC's personnel policy.

Exclusive functions of highly trusted personnel of the senior management of ANF AC:

- **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 originator and recipient, in accordance with the provisions of this policy and in the CPS of ANF AC.
- **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:
  - or They do not have access to the CA keys.
  - or They do not have access to the CA logs. It will be avoided by user properties of the CA software.
  - or They authenticate via smartcard or USB token with the CA software and this software will not support any alternative 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 in a QSCD device on a 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 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 logs of ANF AC systems.
  You will see the logs through the web interface offered by the CA. Electronic signature certificate is used for access control.
  Only this Role will have access to the logs. The
  auditor should be responsible for:
  - or Check incident and event tracking
  - or Check the protection of the systems (exploitation of vulnerabilities, access logs, users, etc.).
  - or 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:
  - or Verify the existence of all the required and listed documentation
  - or Check the coherence of the documentation with the procedures, inventoried assets, etc.

ANF AC maintains the following criteria in relation to the information available for audits and analysis of incidents that may exist with the certificates.

- **Incident Detection and Control**

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
-
- By 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.

- **Incident Record**
  ANF AC has an Incident Registry in which all incidents that have occurred with the certificates issued, and the evidence obtained, are registered. These incidents are recorded,

They analyze and solve 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.

5.4. Network security

As defined in the CPS of ANF AC.

6. End users

The end users of the service are the natural or legal persons who have the capacity to request and obtain the provision of the service under the conditions established in this policy.

For the purposes of this policy, the following are end users:

- Payer
- Subscriber
- Addressee
- Trusted third parties

6.1. Payer

It is the natural person who, in his own name or on behalf of a third party, and after identification, requests the provision of the service. In the case of an ordering party who intervenes on behalf of a third party, they must prove their legal capacity to represent them.

6.2. Subscriber

It is the natural or legal person client of ANF AC who is considered a subscriber, and whose name and responsibility the service is provided as the sender of the communication.

6.3. Addressee

It is the natural or legal person to whom the payer requests that an electronic document be delivered.

6.4. Trusted third party

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 CPS of ANF AC.

7. Identification and authentication

All the requirements established in this section apply to the REM service, any reference to ERD, ERDS, or ERDSP, shall be understood as extended to REM, REMS and REMSP respectively.

7.1. Initial identification

In the QERDS service, the identity of the originator and the recipient will be verified by one of the means of identification of substantial security level or high security level (*Art. 8.2 b) and c) of the eIDAS Regulation)* following:

- Physical presence in one of ANF AC's face-to-face or AR verification offices, 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.

In the ERDS service, the identity of the payer and the recipient will be verified by one of the means of identification with a low security level (*Art. 8.2.a) of the eIDAS Regulation).*

In the event that the originator or the recipient has not linked their identity to a means of authentication, the identity verification will be carried out each time content is sent or delivered.

In the case of SMS delivery, low security level (ERDS), Spanish law obliges Telecommunications Operators to carry out a strong and complete identification of the owner of the telephone and / or data line, in accordance with the following regulations :

- Law 9/2014, of May 9, General Telecommunications *(https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950)*
- Law 25/2007, of October 18, on data conservation regarding electronic communications and public communications networks. *(https://www.boe.es/buscar/act.php?id=BOE-A- 2007-18243)*

ANF AC is based on the identification made by the telephone operator. The Identification Manager may request the documentation that he considers appropriate to validate that identification (*e.g., line contract, invoices, Telecommunications Operator's certificate, etc.)*

In addition, the Originator, according to clause 2 of the service subscription contract (*"S2S Contract"),* Previously, you must have identified the recipient of the certified delivery operations, due to a pre-existing relationship between the two, formalizing in writing a document that collects the recipient's consent on the communications and assignment of the means used, with express mention of the recipient's trusted mailboxes, which he maintains under his exclusive control, be they mobile phone numbers, email addresses or others.

7.2. Authentication

In all the modalities of the Qualified Service of Certified Electronic Delivery, a qualified certificate of signature or electronic seal may be used.

Additionally, 2FA authentication mechanisms based on one-time session passwords or OTP (One-Time Password) may be used.

The authentication process using 2FA mechanisms consists of:

- Sending a one-time session password using one of the channels corresponding to the interested party's mailbox: SMS, WhatsApp, Instant Messaging, etc.
- Registration of the session password in a multi-factor authentication application.
- Access to the service platform through username and password, and the multi-factor authentication application used.

The authentication process using OTP mechanisms consists of:

- Sending a QR code by email to the email id.
- Registration of the QR code in a multi-factor authentication application.
- Access to the service platform through username and password, and the multi-factor authentication application used.

The payer establishes the identification and authentication requirements that must be contemplated by the ERDS, the requirements determine the ERDS or QERDS modality.

8. Events, evidence and probative document

ANF AC will keep a record of service events through logs and audit trails that can be consulted directly from the application.

All the requirements established in this section apply to the REM service, any reference to ERD, ERDS, or ERDSP, shall be understood as extended to REM, REMS and REMSP respectively.

Each ERDS service has a unique identifier.

All the evidence produced by the service can be downloaded in PDF format. Each evidence has a unique evidence identifier, includes an ERDS identifier, and details information on the identity of the originator and the recipient, automated systems that have intervened, information related to events, when they occurred and audit trails that have been obtained.

Each evidence is authenticated by ANF AC electronic seal that includes OCSP verification and qualified electronic time stamp that meets the XAdES, ETSI TS 10317, v.2.1.1 standards, (LT and LTA level) in accordance with the Implementation Decision (EU) 2015/1506 of the Commission of September 8, 2015, which establishes specifications for advanced electronic signature formats and advanced electronic seals of Regulation (EU) No. 910/2014.

The set of evidence generated in each certified electronic delivery service is compiled in a single PDF document called “Evidence Document”. This document has a unique evidence identifier, includes an ERDS identifier, which includes the service modality, the final result of the service performed, and details information on all the evidence generated.

The probative document is authenticated by ANF AC electronic seal that includes OCSP verification and qualified electronic time stamp that complies with the XAdES, ETSI TS 10317, v.2.1.1 standards, (LT and LTA level) in accordance with the Implementation Decision (EU) 2015/1506 of the Commission of September 8, 2015, which establishes specifications for advanced formats of electronic signatures and advanced electronic seals of Regulation (EU) No. 910/2014.

To obtain evidence related to the transmitted data, the ERD application has a system that allows obtaining an authenticated copy of the evidence and a document proving the transmission made. The ERD application requires, prior to access, user identification, which will at least have a substantial security level. Likewise, ANF AC offers the possibility of requesting an authenticated copy by any of the following procedures:

- Person in the administrative offices of ANF AC,

  Gran Vía de les Corts Catalanes, 996 3rd and 4th floor

08018 - Barcelona - Spain

Proving identity by means of a legal document (DNI, Passport, residence card), in case of third-party representation by notarial power of attorney.

- Postal mail sent to the administrative offices of ANF AC, will include proof of identity.

Related tests of transmitted data are only accessible:

- To the payer.
- To the sender holder subscriber.
- To the recipient provided that the certified electronic delivery had been made effectively. By court order.
-

If the identification of the recipient is based on an advanced or qualified electronic signature, and the signature validation is in compliance, the recipient will be notified without other authentication control requirements.

8.1. Processing frequency

Audit logs are periodically reviewed for unusual or suspicious activity.

8.2. Retention period

ANF AC custody during the applicable national legal period after the date of shipment, all the relevant evidence. At least it keeps online all the records of the information transmitted for a minimum period of 6 months, and for a period of up to 15 years in backup.

The information preserved will be, as a minimum:

a) user identification data;

b) user authentication data;

c) proof of initial verification of the identity of the sender;

d) ERDS operation records, sender and recipient identity verification and communication;

e) proof of the verification of the identity of the recipient before sending / delivering the user content;

f) means of demonstrating that user content has not been modified during transmission;

g) a reference or a summary of the complete content of the submitted user; Y

h) timestamp sheets corresponding to the date and time of shipment, consignment and delivery and modification of the user's content, as appropriate.

8.3. Limitations to the validity period

ANF AC will guarantee the validity of the evidences and supporting documents during the entire retention period.

8.4. 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.

The signing keys are kept and used on a QSCD device. 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).

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

The payer signs the notification, guaranteeing the authenticity of the origin and the integrity of the content. The ERDS, prior to accepting the notification, performs signature verification, and prior to transmission to the recipient, it proceeds to verify the signatures that authenticate the notification.

The entire identification process is carried out in a safe and controlled environment in accordance with the physical and logical security measures established in the CPS and addendum of ANF AC. ANF AC guarantees the confidentiality, integrity and availability of the records.

8.5. Events logged by the service

8.5.1. Origin ERDS events

8.5.1.1 Acceptance of the certified delivery order

The payer has identified himself, intervening on his behalf as the subscriber owner or on behalf of a third party, and has transmitted to the certified delivery service a request for communication specifying the delivery requirements.

ANF AC, has verified the request and has accepted the order for certified delivery.

The evidence attests to the identity of the payer and the subscriber, who, duly authenticated in accordance with the details indicated in the evidence, has successfully transmitted, at the time indicated in the evidence itself, the identity of one or more recipients, the channel of communication to be used to carry out the certified delivery, a content to be made available to the recipient, requirements that the payer establishes to make the delivery effective (eg electronic signature certificate, 2FA and / or reading confirmation), and acceptance by part of ANF AC of the delivery order and moment in which the order is accepted.

8.5.1.2 Denial of the provision of the service

The certified electronic delivery requested by the payer was not accepted by the ERDS. The service provider can reject a request whenever it deems it appropriate, whether for political, commercial, formal or technical reasons.

The evidence related to the denial of service attests that the provision of the service to the payer has been rejected, and the moment in which the rejection occurs.

8.5.2. Re-transmission events between ERDS

8.5.2.1 Acceptance of the re-transmission

An ERD message sent by the relay ERDS and successfully received by the relayed ERDS was accepted by the latter.

Related evidence attests that, in situations where multiple ERDS are cooperating to jointly offer ERD service, an intermediate or recipient ERDS has accepted an ERD message sent by the previous ERDS in the aforementioned chain.

8.5.2.2 Re-transmission rejection

An ERD message sent by the ERDS relay, and successfully received by the ERDS relay, was rejected by the latter due to political, formal, or technical reasons.

The related evidence attests that, in situations where several ERDS are cooperating to jointly offer the ERD service, an intermediate or recipient ERDS, at the time specified by the evidence, has rejected an ERD message issued by the earlier ERDS in the aforementioned case. previously.

8.5.2.3 Re-transmission failure

It was not possible to retransmit an ERD message to the destination ERDS within a specified period of time due to technical errors or other problems. For example: failure to identify the destination ERDS, the destination ERDS is unreachable, or the destination ERDS rejected communication without providing a reason.

The related evidence attests that, at the time specified in the evidence, it was impossible to send an ERD message within a given period of time to an intermediate ERDS provider or to the recipient's ERDS provider due to technical errors and / or other issues.

8.5.3. Acceptance / rejection events by the recipient

8.5.3.1 Notification for acceptance

The system that manages the recipient's account confirms that an ERDS communication has been deposited in the recipient's account, notifying the recipient of the availability of a message (without necessarily disclosing its sender, content, etc.) and requesting the recipient's willingness to accept it. (eg notification to the recipient that an electronic document has been sent and can collect it by accessing the certified delivery platform)

The related evidence attests that a notification requesting acceptance of a message has been sent to a recipient at a specific time as indicated by the evidence. The evidence attests to the delivery notice sent to the system that manages the recipient's account.

8.5.3.2 Failure to notify for acceptance

The recipient could not be notified within a given period of time due to technical errors and / or other reasons, or there is no proof of notification from the system managing the recipient's account within a given period.

The time limit is set by legal or contractual regulations, or is determined by ERDS policy, or has been predefined by the payer.

Related evidence attests that a notification requesting acceptance of a message could not be delivered to the specified recipient after a certain number of attempts or a timeout as specified in applicable policies.

8.5.3.3 Notification of content modification

The EDRS does not make changes to the content provided by the payer, nor does it even modify the format of the electronic document.

The ERDS, prior to the transmission of the electronic document, performs an integrity check in order to detect any modification of the content. In the event that the validation is negative, the transmission is not made.

The related evidence attests that a notification requesting the acceptance of a message could not be sent to the specified recipient due to modification of the original notification delivered by the originator.

8.5.3.4 Acceptance of the consignment

The recipient performed an explicit action (eg 2FA) indicating to the ERDS that it issued the notification of acceptance to receive an electronic document.

The evidence attests that the recipient, with the appropriate identification and authentication, at the time indicated by the evidence, carried out an explicit action by means of which he accepts to receive the electronic document consigned by the originator.

8.5.3.5 Rejection of the consignment

The recipient, after proper identification and authentication, performed an explicit action indicating that the recipient refused to receive the document consigned by the originator.

The related evidence attests that the recipient, with the appropriate identification and authentication, at the time indicated by the evidence, refuses to receive the content that the payer consigned.

8.5.3.6 Expiration of acceptance / rejection

The ERDS sent a notification to the recipient, but did not respond to the notification with an accept / reject.

The related evidence attests that the recipient, at the time indicated by the evidence, did not react to the request to accept / reject to receive any content consigned by the originator within a defined period of time.

This period of time can be determined by legislation, ERDS policy rules, or parameters given by the payer.

8.5.4. Acceptance / rejection events by the recipient

8.5.4.1 Content consignment

The system that manages the recipient's account confirms that the communication transmitted by the ERDS has been deposited in his account.

The related evidence attests that the ERD message, at a specific time indicated by the evidence, was made available to the recipient.

8.5.4.2 Content Consignment Failure

The content consigned by the originator may not be available to the recipient within a given period of time due to technical errors and / or other reasons or there is no proof of delivery within a specified period.

Related evidence attests that the ERD message could not be made available to the recipient within a given period of time. The issuance of this evidence can be triggered by different events, by way of illustration, not limitative:

- The system that manages the recipient's account could not send the communication to the recipient's account.

- A relay ERDS did not receive, within a given time period, evidence of successful forwarding from the transmitted ERDS. In this case, it is the relay ERDS that creates the evidence with the appropriate reason code.

- The 2FA system was unable to successfully transmit the verification or QR code to the recipient.
- Technical failure of the ERDS publishing platform.

8.5.4.3 Notice of consignment

A notification was sent to the recipient about the availability of the consigned message.

The related evidence attests that a notification about the availability of the consigned message has been sent to a recipient at a specific time as indicated by the evidence.

8.5.4.4 Consignment Notification Failure

An attempt to notify the recipient of the availability of user content failed.

The related evidence attests that a notification regarding the availability of the content of the consigned user could not be transmitted.

8.5.5. Recipient delivery events

8.5.5.1 Content delivery

The electronic document was delivered to the recipient.

The related evidence attests that the electronic document consigned by the originator, at a specific moment, was transmitted in its entirety to the recipient.

8.5.5.2 Content delivery failure

The electronic document was not delivered to the recipient.

The related evidence attests that the electronic document consigned by the originator was not delivered to the recipient after a certain number of attempts or a waiting time specified by the applicable policies.

8.5.5.3 Failure due to inability to access content

The electronic document is not accessible to the recipient due to technical reasons (eg corrupt encrypted document, electronic document integrity failure, detection of illegal content, etc.).

The related evidence attests that the electronic document consigned by the originator is not accessible to the recipient for technical or formal reasons detailed in the evidence.

8.5.6. Connection events with non-ERDS systems

8.5.6.1 Forwarding to a non-ERDS system

A particular message was successfully sent to a system that does not provide acknowledgment.

The related evidence attests that a certain ERD message was successfully forwarded to the system that manages the recipient's account at the time indicated in the evidence, but the system does not issue confirmation of receipt.

8.5.6.2 Forwarding to a non-ERDS system failed

The attempt to relay a message to a non-ERDS system failed due to technical errors and / or other reasons.

Related evidence attests that a certain ERD message could not be forwarded to a non-ERDS system at the time indicated in the evidence.

8.5.6.3 Receiving from a non-ERDS system

A certain message was received from a non-ERDS system, therefore all information related to its shipment, such as sender identifier and delivery time, cannot be trusted.

Related evidence attests that a certain message was received from an external non-ERDS system, therefore all information about the origin of the message is not reliable.

8.5.7. Adherence of the addressee to the content of the electronic document

8.5.7.1 Notification for accession

The ERDS notifies the recipient that the payer requests an explicit action that certifies the recipient's compliance with the content of the electronic document delivered, and the procedure to follow.

The related evidence attests that a notification requesting acceptance and adherence to the terms expressed in the electronic document delivered by the ERDS has been requested from the recipient at a specific time and the procedure that the recipient must carry out in case of compliance.

8.5.7.2 Failure to notify for accession

The recipient could not be notified within a given period of time due to technical errors and / or other reasons, or there is no proof of notification from the system managing the recipient's account within a given period.

The time limit is set by legal or contractual regulations, or is determined by ERDS policy, or has been predefined by the payer.

The related evidence attests that the adhesion notification could not be delivered to the specified recipient after a certain number of attempts or a time-out as specified in the applicable policies.

8.5.7.3 Adherence to the electronic document

The recipient carried out an explicit action (eg electronic signature, metric signature, 2FA, etc.) as an expression of their will and consent to accept and adhere to the terms expressed in the electronic document delivered by the ERDS and, if applicable At the request of the transaction, the recipient makes a mandate to the ERDS provider so that, as agent, he signs the agreement of acceptance of the content of the electronic document.

The evidence attests that the recipient, with the appropriate identification and authentication, at the time indicated by the evidence carried out an explicit action by which he accepts and adheres to the content of the electronic document consigned by the originator and, where appropriate, so that the ERDS provider in capacity of agent of the addressee (principal), sign on his behalf the acceptance of the document electronic.

8.5.7.4 Refusal to adhere to the electronic document

The recipient, after proper identification and authentication, performed an explicit action indicating that the recipient refused to adhere to the terms contained in the document consigned by the payer.

The related evidence attests that the recipient, with adequate identification and authentication, at the time indicated by the evidence, refuses to adhere to the terms contained in the document consigned by the originator.

8.5.7.5 Expiration of accession / rejection

The ERDS sent a notification to the recipient, but did not respond to the notification with an adherence / rejection.

The related evidence attests that the recipient, at the time indicated by the evidence, did not react to the adhesion / rejection request to accept the content of the electronic document.

This period of time can be determined by legislation, ERDS policy rules, or parameters given by the payer.

9. Obligations and responsibilities

9.1. Obligations of the service provider

ANF AC, in its capacity as Qualified Trust Service Provider, fully assumes the provision of all QTSP services necessary for the provision of the QERDS. It is forced to:

- Respect the provisions of this Policy for the Qualified Certified Electronic Delivery Service.

- Protect your private keys safely.
- Provide the Qualified Certified Electronic Delivery Service according to the information sent by the payer and free of data entry errors.
- 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 of the Qualified Certified Electronic Delivery Service.
- Inform about the modifications of the Policy of the Qualified Service of Certified Electronic Delivery to clients and third parties who trust the services.
- Establish the mechanisms for the generation and custody of the relevant information in the activities described, protecting them against loss, destruction or falsification.
- Custody of the evidence issued for clients who contract the Qualified Certified Electronic Delivery Service.
- Respond for non-compliance with the provisions of this Policy of the Qualified Certified Electronic Delivery Service and, where applicable.
- Use the electronic seal certificate that identifies the certified electronic delivery service and use it for that sole purpose.
- All persons involved in the management and administration of the certified electronic delivery service are obliged to keep all the information managed by ANF AC secret, having signed the corresponding confidentiality commitment.

- Protect the confidentiality of the identity of the sender and recipient, or between distributed components of the ERDS system.
- Guarantee the confidentiality of communications, 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.

9.1.1. Financial responsibility

It is applied within the limits established in the current Electronic Signature Law. ANF AC is not responsible in case of transaction losses.

9.1.2. Liability exemption

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

- Damages caused by external attacks, 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 these QERDS Policies 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 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 QERDS Policy.

ANF AC does not review the contents of the payer's communications, it intervenes as a mere provider of the communications service, therefore, the intervention of ANF AC cannot presuppose adherence to the content of the message, nor is ANF AC responsible for it.

9.2. Obligations of the sender and receiver

- Respect the provisions of this Policy for the Qualified Certified Electronic Delivery Service. Protect your
- private keys safely.
- Respect the provisions of the contractual documents signed with ANF AC. Report any
- security incident as soon as it is identified.
- Do not use the ERDS service for communications that are prohibited by current legislation. Use the technical
- resources of the ERDS, in accordance with the indications established by ANF AC. Reverse engineering and
- troubleshooting of system logic is prohibited. Guarantee that the shipping orders obey a legal relationship with
- the recipients and that they are not unwanted communications by them, except when the shipment is covered by the provisions of a law.

9.3. 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 seals that authenticate the evidences and probative documents, using a qualified service of electronic signatures and seals.

- Take into account the limitations in the use of the service, as indicated by the Policy of the Qualified Service of Certified Electronic Delivery.
- Report any security incident as soon as it is identified. Take into consideration other
- precautions described in agreements or other sites.

10. Termination of the QERDS service

In the event of termination of the Qualified Certified Electronic Delivery Service, the following actions must be applied:

10.1. 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.

10.1.1. Communication to interested parties and third parties

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

10.1.2. 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 can take charge of their custody during the rest of the committed period.

10.1.3. 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.

10.1.4. 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.

10.1.5. Transfer of service management

The transfer of service management is not contemplated.

10.2. Obligations after the cessation of activity

Will be performed:

- notification to affected entities; and 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.

11. Limitations of liability

11.1. Warranties and Warranty Limitations

ANF AC limits its liability by restricting the service to the certified electronic delivery supplied.

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.

11.2. Disclaimer of responsibilities

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

- Damages caused by external attacks, 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 these QERDS Policies 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 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 QERDS Policy.

- Damages 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.

12. Terms and conditions

ANF AC, makes this policy that includes the terms and conditions in which the ERDS 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/

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.

Constitution of the delivery

The Qualified Certified Electronic Delivery Service provides the safe and reliable delivery of electronic messages between the parties, producing evidence of the delivery process for legal liability.

In accordance with article 28 of Law 34/2002, of July 11, on information society services, the ERDS considers delivery to have been made when the systems that manage the recipient's account confirm receipt.

The delivery will generate evidence that will be stored associated with the message on the platform and will be made available to the orderor of the service.

The ERDS considers the document to be accessed by the recipient when it performs an explicit collection compliance action.

The recipient's access to the document will generate evidence that will be stored associated with the message on the platform and will be made available to the service provider.

The evidence is prepared as a statement from the Certified Electronic Delivery Service Provider that a specific event, rigorously detailed, related to the delivery process occurred at a specific time. The evidence can be delivered immediately to the payer or can be stored in a repository for later access by interested parties.

The evidence is encoded with a unique identifier and authenticated by the long-term electronic seal of ANF AC, thus stating the responsibility assumed and guaranteeing its integrity.

All the evidences associated with a certified electronic delivery are compiled in an evidentiary document.

The probative document is encoded with a unique identifier and authenticated by an electronic long-term seal of ANF AC, thus stating the responsibility assumed and guaranteeing its integrity.

Availability of delivery data

Once the delivery is constituted, the recipient will have a maximum period established by the ordering party to confirm receipt of the data, which in no case will be longer than six months. Once this threshold is exceeded, the delivery data will no longer be available for receipt by the recipient.

Service availability

The Qualified Service of Certified Electronic Delivery will be available 24 hours a day, 7 days a week, understanding by availability the ability to access the service by whoever requests it, regardless of the speed or pace at which it subsequently be borrowed.

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 document SLA (Service Level Agreement).

Information Management System Security

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

Legal terms

The relationship between ANF AC and the user of the service is governed exclusively by Spanish legislation.

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 transactions electronic devices in the internal market (eIDAS Regulation) and repealing Directive 1999/93 / EC.

- 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).
- Organic Law 3/2018, of December 5, on Protection of Personal Data and guarantee of digital rights.
- Law 34/2002, of July 11, on services of the information society and electronic commerce.
- Law 59/2003 of electronic signature.

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

13. 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.

13.1. 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/

13.2. Policy approval procedure

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

14. Financial capacity

14.1. 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)

14.2. 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.

14.3. 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.

15. Conflict resolution

15.1. Extrajudicial conflict resolution

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

15.2. Competent jurisdiction

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