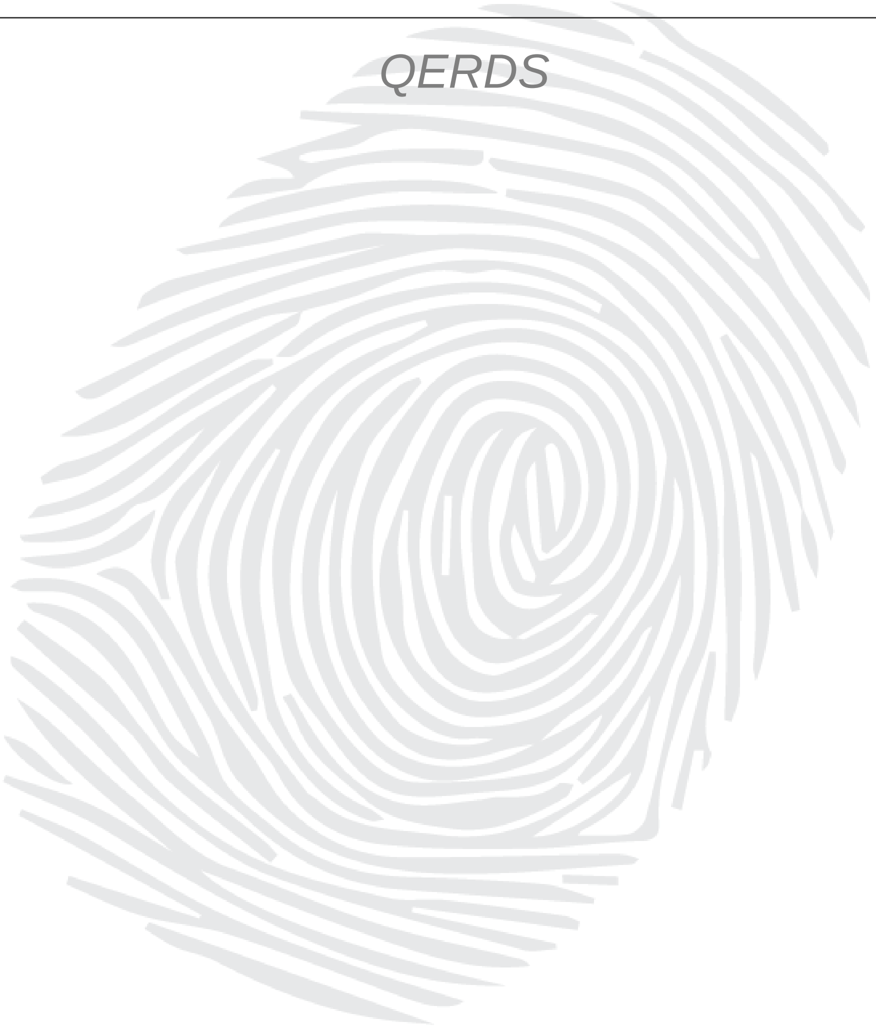
Policy of the Qualified Electronic Registered Delivery Service

QERDS



Registro Nacional de Asociaciones. Número 171.443. CIF G-63287510

Paseo de la Castellana, 79 – 28046 - Madrid (Spain)
Telephone: 932 661 614 (Calls from Spain)
International (+34) 933 935 946
Website: www.anf.es

Security Level

Public Document

Important Notice

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

Website: www.anf.es

INDEX

1 Introduction

ANF Autoridad de Certificación [ANF AC] is a legal entity constituted 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 is a Qualified Trust Services Provider (PCSC) in compliance with eIDAS Regulation and current national legislation.

ANF AC is a provider of the "Qualified Electronic RegisteredDelivery Service" (QERDS) provided for in article 44 of 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 (hereinafter eIDAS Regulation), provided in accordance with:

- **Ley 6/2020,** de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza,
- **ETSI EN 319 401** *(General Policy Requirements for Trust Service Providers).*
- **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".*

This document is the **Policy of the Qualified Electronic Registered Delivery Service**, that defines the procedural and operational requirements to which the use of the service is subject, and defines the practices that ANF AC applies for the provision of services in any of the communication channels available at any time, email or other available that enable ERDS communication:

- Electronic registered delivery service.
- Services related to electronic registered delivery service.
  - Sender and recipient identification.
  - Capture of evidences and preparation of probative document.
  - 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 Practices Statement and its addendum. This policy is subordinate to the Certification Practices Statement (CPS) of ANF AC. All documentation is freely available to users and third parties https://anf.es/en/legal-repository/

This Policy assumes that the reader knows the concepts of PKI, electronic certificate and electronic signature; otherwise, it is recommended the reader to be trained in the knowledge of the previous concepts before continuing with the reading of this document.

1.2. Name of the document and identification

Document name	Policy of the Qualified Electronic Registered Delivery Service		
Version	1.3.		
OID	1.3.6.1.4.1.18332.60		
Approval date	15/10/2021	**Publication date**	15/10/2021

1.2.1. Reviews

The revision process of this policy has a minimum annual periodicity, and whenever there is something new that requires its revision and is justified from the technical and legal point of view. The version will only be changed if there are substantial changes that affect its applicability.

The members of the Governing Board of the PKI are competent to agree on the approval of this policy, guaranteeing that the changes meet the requirements that are intended to be covered, that they are in harmony with the CPS and the ANF AC addendum. Prior to the publication of updates, the implications on the relying parties will be assessed, and the need to notify said modifications by registered email to each of the users, the CAB and the Supervisory Body is anticipated.

Version	Changes	Approval	Publication
1.3.	Clarification of the delivery order rejection method, and S&N vs. S&F models. The ERDS service does not transmit to other ERDS.	15/10/2021	15/10/2021
1.2.	Review after audit.	04/12/2020	04/12/2020
1.1.	Inclusion of references to ETSI EN 319 521	01/10/2020	01/10/2020
1.0.	New Policy for the Qualified Electronic Registered Delivery Service.	15/01/2020	15/01/2020

1.3. Definitions and Acronyms

In this policy, the definitions specified in the CPS of ANF AC apply, in addition to the following:

English	Spanish	Acronym	Definition
Sender	*Ordenante*		Natural or legal person who orders the delivery of user content and establishes the requirements for delivery. The sender may intervene in his own name and on his behalf, in which case he assumes the role of subscriber of the service (sender), or may intervene on behalf of a third party.
Recipient	*Destinatario*		Natural or legal person to whom the user content is addressed.
user content	*Contenido de usuario*		original data produced by the sender that must be delivered to the recipient

consignment	*Consignación*		act of making user content available to the recipient, within the limits of the electronic registered delivery service.
handover	*Transferencia*		the act of causing user content to successfully cross the recipient's electronic registered delivery service boundary into the recipient's ERD-UA.
Electronic Registered Delivery Service	*Servicio de Entrega Electrónica Certificada*	ERDS	Electronic service that allows the transmission of data between the originator and the recipients by electronic means and provides evidence related to the handling of the transmitted data, including proof of sending and receiving the data, and that protects the transmitted data against the risk of unauthorized loss, theft, damage or alteration
Qualified Electronic Registered Delivery Service	*Servicio Cualificado de Entrega Electrónica Certificada*	QERDS	As specified in the eIDAS Regulation.
Electronic Registered Delivery Service Provider	*Prestador de Servicio de Entrega Electrónica Certificada*	ERDSP	Trusted service provider that provides an electronic registered delivery service.
Qualified Electronic Registered Delivery Service Provider	*Prestador Cualificado de Servicio de Entrega Electrónica Certificada*	QERDSP	Trusted service provider providing a qualified electronic registered delivery service.
ERD user agent/application	*Aplicación/Agente usuario ERD*	ERD-UA	System consisting of software and/or hardware components through which originators and recipients participate in the exchange of data with the ERDSP. Within the scope of this ERDS, the application is Sign to Sign Delivery Services.
ERDS evidence	*Evidencia ERDS o Trazas de auditoría*		Data generated within the ERDS, which aims to demonstrate that a certain event has occurred at a certain time.
Probative document	*Documento probatorio*		Document that incorporates all the information related to the transaction, evidence that has been generated and the moment in time in which it has been produced. The document is authenticated by ANF AC by means of an electronic seal.

ERDS practice statement	*Declaración de Prácticas ERDS*		Statement of the practices that an ERDSP employs to provide its services.
Store and Forward	*Almacenamiento y Reenvío*	S&F	Style of operation of a REMS in which the user content provided by the sender is transmitted to the recipient by value, and no explicit acceptance of the recipient is required.
Store and Notify	*Almacenamiento y notificación*	S&N	Style of operation of a REMS in which a reference to the user content is first transmitted to the recipient, and the recipient's acceptance is required before sending the user content itself.
Registered electronic mail	*Correo electrónico certificado*	REM	It is a specific type of electronic registered delivery, which is based on the formats, protocols and mechanisms used in ordinary email messaging.

1.4. ERDSP contact details

As defined in the CPS of ANF AC.

Department	PKI Governing Board
Email	juntapki@anf.es
Address	Paseo de la Castellana, 79. 28046, Madrid.
Administrative Address	Gran Vía de les Corts Catalanes, 996 piso 3 y 4 08018, Barcelona.
Telephone number	932 661 614 (calls from Spain) International (+34) 933 935 946

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

Website	https://reportarproblema.anf.es
Email	info@anf.es
Appearance in ANF AC administrative offices	Gran Vía de les Corts Catalanes, 996 piso 3 y 4 08018, Barcelona.
Telephone number	932 661 614 (calls from Spain) International (+34) 933 935 946

2 Description of the services

2.1. Type of service according to qualification

2.1.1. ERDS Service

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

This service has been designed and is managed in accordance with ETSI standards:

- **EN 319 521**: *"Policy and security requirements for Electronic Registered Delivery Service Providers";*
- **EN 319 531**: *"Policy and security requirements for Registered Electronic - Mail Service Providers";*

Data sent and received through the ERDS service has legal effects and should not be denied admissibility as evidence in legal proceedings solely because it is in electronic format or does not meet the requirements of the QERDS service (section 2.1.2.).

In order to identify the ERDS registered delivery services, ANF AC has assigned the following **OID 1.3.6.1.4.1.18332.60.1.**

2.1.2. QERDS Service

The eIDAS Regulation establishes a series of additional requirements that both the provider and the service must meet with respect to conventional ERDS and the entities that provide them. This QERDS service is the ERDS service (section 2.1.1.) that applies the additional requirements established in article 44 of the eIDAS Regulation. This service has been designed and is managed in accordance with:

- **Article 44** of eIDAS Regulation.
- **EN 319 521**: *"Policy and security requirements for Electronic Registered Delivery Service Providers";*
- **EN 319 531**: *"Policy and security requirements for Registered Electronic - Mail Service Providers";*

The data sent and received through the QERDS service enjoy the presumption of data integrity, the sending of these data by the identified sender, its reception by the identified recipient and the accuracy of the date and time of sending and receiving indicated by the service.

In order to identify QERDS qualified electronic registered delivery services, ANF AC has assigned the following **OID 1.3.6.1.4.1.18332.60.2.**

Sign to Sign Delivery Services			
Subject	CN = Sign to Sign Delivery Services	**Serial number**	996187871247079129227164297

	OI = VATES-G63287510	**Public Key**	RSA (2048 Bits)
	OU = Certificado Cualificado de Sello Electronico		
	O = ANF Autoridad de Certificación	**Signature algorithm**	Sha256RSA
	C = ES L=Barcelona, ST=Cataluña		
Validity period	Valid from 2020-12-02 13:52:56 until 2022-12-02 13:52:56		
x509SKI	ebLudB3q/eytq7utl/KmzdRLXfl=		

The communication channel used to make the delivery to the recipient's mailbox can be electronic mail (REM) or another, as long as it guarantees the requirements established to be considered ERDS.

2.2. ERD-UA

For sending and receiving communications, collecting evidence and generating supporting documents, users have an application (ERD-UA) that is available in two modalities:

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

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

ANF AC does not make changes to the content provided by the sender, nor does it even modify the format of the electronic document.

2.3. Participants in the service

- **Electronic Registered Delivery Service Provider (ERDSP):** trusted service provider that provides a registered electronic delivery service, in this case ANF AC.
- **Sender**: Is the natural person who, in their own name or on behalf of a third party, and after identification, requests the provision of the service. In the case of a sender intervening on behalf of a third party, they must prove their legal capacity to represent them.
- **Subscriber**: Is the natural or legal person who is a client of ANF AC and who is considered a subscriber, and in whose name and responsibility the service is provided as the sender of the communication.
- **Recipient:** Is the natural or legal person to whom the sender requests that an electronic document be delivered.
- **Trusted third party:** Third parties who, without being the subscriber or the user, generally recipients, although they may also be authors, or judicial experts, or Courts of Justice, are authorized to access the message sent.

2.4. ERDS logic model

The ERDS logic model applied is the black-box model, with ANF AC as the only ERDSP.

2.5. Style of operation

2.5.1. Store and Forward (S&F)

Sending content directly to the recipient's platform without requiring an action from the recipient is allowed.

The REMS and QREMS registered email service is part of this service with the only difference that:

- use the SMTP (email) transfer protocol,
- offer the option to all users to send and receive messages in MIME format according to RFC 2045 and RFC 5322

Does not support interconnection with other REMS.

2.5.2. Store and Notify (S&N)

Both QERDS and ERDS allow for the S&N style, in which a reference to user content is sent to the recipient and the recipient is required to actively respond on the platform by accepting or rejecting the incoming message, prior to commit. Commitment of user content only occurs if the response was positive.

The service does not allow the S&N style for messages transmitted by another ERDS (REMS).

Sign to sign offers the sender the possibility of establishing a specific validity period and expiration date for acceptance or rejection of communications sent following the S&N style, and the recipient is informed of said period.

2.6. Identification and authentication

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

2.6.1. Initial Identity verification of the sender

The identity of the sender will be verified before the start of the service by the Identity Verification Manager through one of the following means of identification with a substantial security level or a high security level (Art. 8.2 b) and c) of the eIDAS Regulation):

- Physical presence in one of ANF AC's face-to-face verification offices or AR, or through a third party in accordance with national law.
- Through a certificate of a qualified electronic signature or a 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 security level of this identification for the QERDS service is High Level, corresponding to level 4 of guarantee foreseen in the IDABC Basic Authentication Policy.

The security level of this identification for the ERDS service is Medium/Substantial Level.

This verified identity will be linked to the user of said sender, and to a means of authentication.

2.6.2. Recipient Identification

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

In the QERDS service, the identity of the recipient will be verified before each delivery 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 verification offices or AR, or through a third party in accordance with national law.
- Through 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 recipient will be verified by one of the means of identification with a low security level (Art. 8.2.a) of the eIDAS Regulation).

ANF AC can link the previously verified identity of the recipient to a means of authentication indicated in the requirement REQ-QERDS-5.2.2-03 of the ETSI EN 319 521.

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

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950)
- Ley 25/2007, de 18 de octubre, de conservación de datos relativa a las comunicaciones electrónicas ya las redes públicas de comunicaciones. (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 Person Responsible for Identification may request the documentation that he deems appropriate to validate that identification (eg, line contract, invoices, certificate from the Telecommunications Operator, etc.)

In addition, the Originator, as stated in clause 2 of the service subscription contract ("S2S Contract"), must have previously identified the recipient of the registered delivery operations, due to a pre-existing relationship between the two, formalizing in writing a document that collects the consent of the recipient 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, whether they are mobile phone numbers, email addresses or others.

2.6.3. Authentication

In all the modalities of the Electronic Registered Delivery Qualified Service, a qualified certificate for electronic signature or 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 by username and password, and the multifactor authentication application used.

2.7. Scope of application

2.7.1. Usage limits

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

- The communications and documents whose delivery are requested by the sender must be in accordance with current legislation.
- The sender has the legal capacity to establish communication with the recipient

2.7.2. Prohibited usages

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

- The deliveries made will be executed only in accordance with the function and purpose established in this Policy of the Qualified Electronic Registered Delivery, and in accordance with current regulations.
- The contracting of the service admits only the use of the service in the field of activity of the client that contracts the service or of the entity to which it is linked, in accordance with the purpose of the service. The client may not, unless specifically agreed with ANF AC, make use of the service for its commercial purposes.
- Commercial use of the service is understood as any action through which the client offers third parties other than the subscriber, for consideration or free of charge, the use of this electronic registered delivery service.

2.8. Terms and conditions of the service

See the Terms and Conditions document published at https://anf.es/en/legal-repository-terms-and-conditions/

3. Events, evidence and probative document

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

3.1. Evidence registered by the service

3.1.1. Identity evidences

The information recorded is, at a minimum:

- Proof of initial verification of the sender's identity;
- Identification data of the sender;
- Authentication data of the sender;
- Records of the operation of the ERDS, identity verification of the originator and recipient and communication;
- Proof of verification of the identity of the recipient before sending / delivery of the user content;

3.1.2. Evidence of user content

- Means to demonstrate that user content has not been modified during transmission and storage. The electronic documents of the user content are electronically sealed, which allows verifying that they have not been modified between sending and receiving
- Reference or a summary of the complete content of the submitted user;

3.1.3. Evidence on the audit trails of the delivery order

Timestamp tokens corresponding to the date and time of submission, commit and delivery of user content.

Events Related to the sending	
Acceptance of registered delivery order *(Submission Acceptance)*	The sender, duly authenticated in the service, has transmitted to the ERDS (ANF AC – Sign to sign), at the time indicated in the evidence, a communication request with user content and a specification of the delivery requirements. ANF AC, has verified the request and has accepted the order of registered delivery to the recipient and to the indicated mailbox.
Denial of provision of service *(Submission Rejection)*	The registered electronic delivery requested by the sender was not accepted by the ERDS (ANF AC – Sign to sign). The service provider may reject a request whenever it deems it appropriate, whether for political, commercial, formal or technical reasons. The ERDS, prior to the transmission of the electronic document, performs an integrity check in order to detect any modification of the content. If the validation is negative, the transmission is not carried out.

	The evidence related to the denial of service attests that the provision of the service to the sender has been rejected, and the moment in which the rejection occurs.
Events related to the notification of delivery by the recipient	
Notification For Acceptance	The ERDS (ANF AC – Sign to Sign) notifies the recipient that a communication/delivery is available (without necessarily disclosing the originator, content, etc.) and allows him to access the delivery platform to accept, reject or ignore it. This notification may also indicate that an explicit action will be requested that proves the recipient's compliance with the content of the electronic document delivered. The related evidence attests that the recipient received and opened the notification in the indicated mailbox, at a specific time as indicated by the evidence. The evidence does not attest that this notification was read by the recipient.
Notification For Acceptance Failure	The notification could not be delivered to the recipient within a given time period 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. Related evidence attests that a delivery available notification could not be delivered to the specified recipient after a certain number of attempts or a certain timeout.
Events related to the consignment to the recipient	
Consignment Acceptance	The recipient performed an explicit action (eg 2FA) indicating to the ERDS the acceptance to receive the user content. The evidence attests that the recipient, after proper identification and authentication, at the time indicated by the evidence, carried out an explicit action through which they agree to receive the electronic document consigned by the sender.
Content Consignment	ANF AC – Sign to sign, confirms that the user content has been made available to the recipient within the limits of the application. The related evidence attests that the User Content, at a specific time indicated by the evidence, was made available to the recipient.
Consignment Rejection	The recipient, after proper identification and authentication, performed an explicit action indicating that he refuses to receive the content consigned by the sender. The related evidence attests that the recipient, with proper identification and authentication, at the time indicated by the evidence, refuses to receive the content that the sender consigned.

Content Consignment Failure	User Content could not be made 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 given period. This event can be triggered for different reasons, for example: • The system was unable to commit the user content to the recipient. • The 2FA system was unable to successfully transmit the verification or QR code to the recipient. • Corrupt encrypted document • Electronic document integrity failure • Detection of illicit content The related evidence attests that the content could not be made available to the recipient within a period of time given a technical failure of the ERDS application.
Acceptance/ Rejection Expiry	ANF AC – Sign to sign sent a notification to the recipient, but did not respond to said notification with an acceptance/rejection after a certain period of time. This period of time can be determined by legislation, ERDS policy rules, or parameters given by the sender. By default, an expiration period of 2 months will be established. The related evidence attests that the delivery order notice expired at the time indicated by the evidence, following the recipient's lack of response.
Events related to the download of the content by the recipient	
Content Handover	The electronic document was delivered and downloaded by the recipient. The related evidence testifies that the electronic document consigned by the sender, at a specific time, was transmitted in its entirety to the recipient.
Content Handover 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 specified waiting time.
Other specific events of the ERDS ANF AC Sign to sign	
Adherence to an electronic document	The recipient carried out an explicit action (e.g. electronic signature, graphometric 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, in the event of As a requirement of the transaction, the recipient makes a mandate to ANF AC so that, as agent, it signs on its behalf the conformity of acceptance of the content of the electronic document.
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 originator.

	The related evidence attests that the recipient, with the appropriate identification and authentication, at the time indicated by the evidence, refuses to adhere to the terms contained in the document consigned by the sender.
Expiration of adherence / rejection	The ERDS sent a notification to the recipient, but did not respond to the notification with an opt-in/reject. The related evidence attests that the recipient, at the time indicated by the evidence, did not react to the accession/refusal 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 sender.

3.2. Probative document

The evidence of the set of events produced in each electronic registered delivery order of the service is compiled in a single PDF document called "Probative Document". This document is identified with a unique code and authenticated by the qualified electronic stamp of ANF AC, including OCSP verification and qualified electronic time stamp.

This evidentiary document is a formal statement stating the intervention of ANF AC as a trusted intermediary in the reception of the delivery order received from the sender and its delivery to the recipient.

It consists of a general record that contains information on the electronic content received and transmitted, the identity of the sender and the recipient, as well as all the events that have been generated during the sending process (delivery order by the sender, audit trails of the communications systems, remission 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 they occurred and the result obtained . A specific minute with detailed information is also included for each specific event.

The supporting document establishes the type of service provided according to qualification.

For obtaining evidentiary documents, the following methods are provided:

- Through the ERD-UA: it has a system that allows obtaining an authenticated copy of the evidence and supporting document of the transmission made. The ERD application requires, prior to access, user identification that will at least have a substantial security level.
- Appearance at the administrative offices (section 1.4.) of ANF AC: proving identity by means of a legal document (DNI, Passport, residence card), in case of representation by a third party by power of attorney.
- Postal mail sent to the administrative offices of ANF AC, identity proof will be included.

Only accessible to:

- The sender
- The recipient provided that the registered electronic delivery had been carried out effectively.
- By court order

3.3. Service logs

ANF AC keeps a record of the logs related to:

- All the events identified in point 3.1.
- Changes related to security policy
- System startup and shutdown
- System crashes and hardware failures
- Firewall and router activities
- Access attempts to the PKI system.

Each piece of evidence is authenticated by the ANF AC electronic seal that includes OCSP verification and a qualified electronic time stamp.

3.3.1. Processing frequency

Audit logs are periodically examined for suspicious or unusual activity.

3.3.2. Retention period

ANF AC custody during the applicable national legal period after the date of shipment, all relevant evidence. At a minimum, it keeps all the records of the transmitted information online for a minimum period of 2 years and for a period of up to 15 years in backup.

3.3.3. Limitations to the period of validity

ANF AC will guarantee the validity of the evidence and supporting documents throughout the retention period.

4. Obligations and responsibilities

4.1. ERDSP obligations (ANF AC)

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

- Respect the provisions of this Policy of the Qualified Electronic Registered Delivery Service.
- Respond for non-compliance with the provisions of this Qualified Electronic Registered Delivery Service Policy and, where applicable.
- Publish and update this Policy of the Qualified Electronic Registered Delivery Service.
- Inform about the modifications of the Policy of the Qualified Electronic Registered Delivery Service to clients and third parties that trust in the services.
- Use a qualified certificate for electronic seal that identifies the electronic registered delivery service and allocate it for that sole purpose.
- Protect its private keys securely.
- Provide the Qualified Electronic Registered Delivery Service according to the information sent by the sender and free of data entry errors.
- Proceed to the validation of electronic signatures and seals through a qualified validation service in accordance with current regulations.
- Establish mechanisms for the generation and custody of relevant information in the activities described, protecting it against loss, destruction or falsification.
- Custody of the evidence issued for clients who contract the Qualified Electronic Registered Delivery Service.
- All persons involved in the management and administration of the electronic registered delivery service are required to keep secret all the information managed by ANF AC, having signed the corresponding confidentiality commitment.
- Guarantee the confidentiality of communications, using strong encryption techniques when applicable.
- Information regarding the services provided to third parties will not be provided, except in compliance with a court order.

4.1.1. Finantial liability

The provisions of the CPS of ANF AC are applied. In terms of compensation to third parties who rely on the service, ANF AC has sufficient financial resources to face the risk of liability for damages to users of its services and to third parties, however, its responsibility in the exercise of the activity of QTSP as defined in ETSI EN 319 401 art. 7.1.1.c, is guaranteed by Professional Civil Liability Insurance with coverage of,

FIVE MILLION EUROS (€5,000,000)

4.1.2. Disclaimer of liability

ANF AC limits its liability by restricting the electronic registered delivery service provided.

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 may be used. NF AC is not responsible for any transaction losses.

ANF AC, will not be responsible in any case when it is 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, malfunctioning 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.
- Due to improper or fraudulent use of the service.
- 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 as user content for the provision of the service.
- Negligence of the user in the conservation of his access data to the service, in the assurance of its confidentiality and in the protection of all access or disclosure.
- Excessive use of the service, in accordance with the provisions of current regulations and this QERDS Policy.
- Damages caused to the recipient or bona fide third parties if the recipient of 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 depositing trust without carrying out the required qualified validations, using a qualified electronic signature and seal validation service.
- The intervention of ANF AC cannot presuppose adherence to the content of the message, nor is ANF AC responsible for it. ANF AC does not review the content of the communications, notwithstanding the foregoing, if it comes to notice by any means that the content to be transmitted is illegal, it will proceed to deny the service ANF AC does not review the content of the communications of the sender, it intervenes as a mere communications service provider.
- ANF AC does not act as fiduciary agent or representative in any way of subscribers or third parties that rely on the provision of their trusted services.

4.2. Obligations of the sender and recipient

- Respect the provisions of this Policy of the Qualified Electronic Registered Delivery Service.
- Safely protect your access credentials and qualified electronic certificate.
- 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.
- Do not apply reverse engineering and fault finding in the system logic, which is prohibited.
- Guarantee that delivery orders are due to a legal relationship with the recipients and that they are not unwanted communications by them, except when the delivery is protected by the provisions of a law.

4.3. Relying Third Party Obligations

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

- Before placing their trust, proceed to the qualified validation of the signatures and seals that authenticate the evidence and probative documents, using a qualified service of electronic signatures and seals.
- Take into account the limitations in the use of the service, as indicated by the Qualified Electronic Registered Delivery Service Policy.
- Report any security incident as soon as it is identified.
- Take into account other precautions described in agreements or other sites.

4.4. Obligations of external organisations

ANF AC ensures that the storage service provider (AWS) has the measures in place to guarantee the confidentiality and availability of the information.

4.5. Conflict resolution

- **Out-of-court conflict resolution:**

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

- **Competent jurisdiction:**

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

5. Management and operation of the QERDSP

5.1. Physical and environmental security controls

As defined in the CPS of ANF AC.

5.2. Operational controls

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

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

Full backup 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 256-bit Advanced Encryption Standard (AES-256).

Communications with the systems are always carried out using the SSL/TLS encrypted communications protocol between users and ERDS systems, and between computer systems. The database managers are in the same internal network as the rest of the ERDS subsystems, so they do not require a secure connection, since they are not accessible outside said network.

The sender signs the notification, guaranteeing authenticity of origin and integrity of content. The ERDS, prior to accepting the notification, performs signature verification, and prior to transmission to the recipient, the signatures that authenticate the notification are verified.

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

5.3. Cryptographic controls

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 the electronic sealing of the content and/or evidentiary document.

The signing keys are kept and used in 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 before they are put into operation.

5.4. 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 who are under the direction of the organization, and are selected following the personnel policy of ANF AC.

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

- **Responsible for identity verification**
  They are personnel assigned to the IRM area of ANF AC. It assumes the responsibility of ensuring compliance with the processes established for the verification of the initial identity of the sender and recipient, in accordance with the provisions of this policy and the CPS of ANF AC.
- **System administrator:** staff assigned to the technical area of ANF AC. Assumes the responsibility of ensuring the full operability of the systems, carrying out installation, configuration and maintenance tasks for the management of services.
- **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 them to manage the signature keys stored in a QSCD device on a remote signature server. The number of people responsible for access codes is three people, and the system requires dual intervention.
  These trusted personnel are the only one authorized and empowered to carry out backup, preservation and recovery operations on the signature key. Always under dual control and in a physically secure environment.
- **System operator:** Personnel authorized to use the terminals with access to the registered delivery systems and who carry out general tasks of management and daily attention to the service. This role is not incompatible with the system administrator.
- **System auditor**: Authorized to view files and audit logs of ANF AC systems. The logs will be accessible to them 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 must be responsible for:
  - Check the tracking of incidents and events
  - Check system protection (exploitation of vulnerabilities, access logs, users, etc.).
  - Check alarms and physical security elements
- **Security Responsible:** In accordance with what is defined in the Security Policy of ANF AC. In addition, it will be responsible for:
  - Verify the existence of all the required and listed documentation
  - Check the consistency of the documentation with the procedures, inventoried assets, etc..

5.5. Incident management

ANF AC has an Incident Registry in which all incidents that have occurred with the services, and the evidence obtained, are recorded. These incidents are recorded, analysed and resolved according to the procedures of the Information Security Management System of ANF AC.

The Security Officer determines the seriousness of the incident and appoints a person in charge and, in case of significant security incidents, informs the PKI Governing Board.

5.6. Network Security

As defined in the CPS of ANF AC.

5.7. 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.

6. QERDS Termination

In case of cessation of the Qualified Electronic Registered Delivery Service, the following actions must be applied:

6.1. Actions prior to activity termination

In the event of cessation of its activity as a Trust Service Provider, ANF AC will carry out the following actions at least two months in advance, or in the shortest period of time possible in the event of key compromise, loss or suspected compromise used to authenticate evidence and probative documents, as well as stamping of qualified electronic time stamps and OCSP validation responses.

6.1.1. Communication to interested parties

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

6.1.2. Notifications to the Supervisory Body

- Notify the competent Supervisory Body in matters of qualified eIDAS services, the cessation of its activity, as well as any other relevant circumstance related to the cessation of activity.
- Make information on events and logs available to the competent Supervisory Body so that it can take charge of their custody during the rest of the committed period.
- Pursuant to the agreement established with the Association of Qualified Trust Service Providers of Spain, deposit information on events and logs so that it is in charge of their custody during the rest of the committed period.

6.1.3. 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 shown 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 there is an execution agreement of the Termination Plan in case of bankruptcy.
- When there is a cessation of activity without implying a bankruptcy situation, all registered information will be stored without the need to transfer it to a trusted party.

6.1.4. 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 to provide the service, so that they cannot be recovered. This operation will be executed following the procedure established in the corresponding policy.

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

6.1.5. Service management transfer

The transfer of service management is not contemplated.

6.2. Obligations after the termination of the activity

The following shall 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 publishing them on the website: https://www.anf.es

if there is a termination 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 (APCSCE).