Terms and Conditions for eIDAS services

& PKI Disclosure Statement

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

Phone number: +34 932 661 614

Website: www.anf.es

Security Level

Public Document

Important Notice

INDEX

1. Introduction

The purpose of this document is to describe the terms and conditions in which ANF Autoridad de certificación (hereinafter, ANF AC) issues electronic certificates and provides qualified trust services under the eIDAS Regulation.

This document has been created in accordance with the requirements established in:

- **ETSI EN 319 301**, section 6.2. *(eIDAS Services in general)*
- **ETSI EN 319 411-1**, section 6.9.4. *(Electronic Certificates)*
- **ETSI EN 319 411-2**, section 6.9.4. *(Electronic Certificates)*
- **ETSI EN 319 421**, section 6.3. *(TimeStamping)*
- **ETSI TS 119 431-1** (*Management of Qualified Remote Electronic Signature and Seal Creation Devices*)
- **ETSI TS 119 441**, section 6.2. *(Signature/seal validation)*
- **ETSI TS 119 511**, section 6.2. *(Signature/seal preservation)*
- **ETSI EN 319 521**, section 4.2. *(Registered Delivery)*

In no case does it replace the Certification Practice Statement (CPS), nor the Certificate Policies (CP) and services, available at https://www.anf.es/en/repositorio-legal/ .

1.1. Contact information

Name of the provider	ANF Autoridad de Certificación
VAT Number	G63287510
Contact address *(technical and administrative)*	Gran Vía de les Corts Catalanes 996, 4º, 2ª. 08018 Barcelona
Contact telephone	+34 932 661 614
Contact email	info@anf.es

1.1.1. Contact for revocations

Subscribers, trusting third parties, application software providers and other third parties can submit problem reports on certificates issued by ANF AC, detailing the reasonable cause for requesting to revoke a certificate:

- **During office hours**, by calling 932 661 614 or by visiting their premises.
- **Outside office hours,** 24x7x365 service, by calling +34 930 502 397.
- Directly by filling in the web form https://www.anf.es/sat-incumplimiento-uso-indebido/

The revocation request will be processed upon receipt. It must be authenticated in accordance with the requirements established in the corresponding section of the CPS. Once the request has been authenticated and valued, ANF AC may directly revoke the certificate.

It is especially important for ANF AC any information related to an alleged private key compromise, incorrect use of certificates, other types of fraud, misuse, inappropriate conduct or any other matter related to the certificates or the PKI of ANF AC that affect the trust in PKI.

1.2. Document name and identification

Document name	Terms and Conditions for ANF AC eIDAS services		
Version	1.11		
OID	1.3.6.1.4.1.18332.5.1.3		
Approval date	05/02/2026	**Publication date**	05/02/2026

1.2.1. Reviews

Version	Changes	Approval	Publication
1.11	Adaptation of the remote qualified electronic signature service and SLA update	05/02/2026	05/02/2026
1.10	Clarification of log retention time for all services	20/02/2025	20/02/2025
1.9	Annual review and clarification of the Subject figure	27/01/2024	27/01/2024
1.8	Clarification in the classification of incidences of SLA	01/09/2023	01/09/2023
1.7	Clarification on limits of use of certificates	07/08/2023	07/08/2023
1.6.	Annual review and inclusion of PKI Disclosure Statement	20/02/2022	20/02/2022
1.5.	Annual review and update	30/03/2021	30/03/2021
1.4.	General review, modification of the validation services and certified delivery service and inclusion of the qualified service	29/10/2020	29/10/2020
1.3.	General review and inclusion of PSD2 certificates	31/01/2019	31/01/2019
1.2.	Compliance with Regulation (EU) eIDAS	18/04/2017	18/04/2017
1.1.	Links update	15/02/2017	15/02/2017
1.0.	Initial version, creation of the document.	01/06/2016	01/06/2016

Periodically, at least once a year and whenever substantial changes occur, this document is reviewed and updated. The latest version is published on the website,

https://www.anf.es

1.3. Definitions and acronyms

1.3.1. Definitions

- Authentication. Electronic process that enables the electronic identification of a natural or legal person, or of the origin and integrity of data in electronic format.
- Registration Authority. Unless it has been carried out by an OVP, it is the entity that carries out the identification tasks of the applicants, subscribers and those responsible for the certificates, verifies that the documentation provided by the applicant is original, current and obtains a certified copy of it . In all cases, it checks the supporting documentation the circumstances that appear in the certificates, inform and evaluate the applicant's capacity, adequacy of the certificate or requested service, process the issuance, revocation and renewal of the certificates before ANF AC.
- Charges. Monthly charges for the use of the Services.
- Certificate. Digital data that allows creating digital signatures, verification of digital identity, device identification, secure transmission of data, code signing and / or data encryption and where the public key is linked to the natural or legal person who owns the certificate.

- Qualified electronic signature certificate. An electronic signature certificate that has been issued by a qualified trust service provider and that meets the requirements established in Annex I of the eIDAS Regulation.
- Qualified Certificate of Centralized Electronic Signature. It is an electronic signature certificate created remotely in an electronic signature creation environment managed by ANF AC on behalf of the signer.
- Contract. Subscription Contract ratified between ANF AC and the Subscriber for the use of electronic certificates issued by ANF AC. The Subscription Agreement includes the Terms and Conditions.
- Policy Disclosure Statement. A set of statements of a CA's policies and practices regarding the operation of its PKI.
- eIDAS Regulation. Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 /EC
- Advanced electronic signature. The electronic signature that meets the requirements contemplated in article 26 of the eIDAS Regulation. It has been prepared with a qualified electronic signature certificate.
- Qualified electronic signature. An advanced electronic signature that is created by a qualified electronic signature creation device and that is based on a qualified electronic signature certificate (Art. 3.12 eIDAS).
- Electronic identification. The process of using the identification data of a person in electronic format that uniquely represents a natural or legal person or a natural person representing a legal person.
- Public Key Infrastructure. Set of people, policies, procedures and computer systems necessary to provide authentication, encryption, integrity and non-repudiation services, through the use of public and private key cryptography and electronic certificates
- Electronic identification means. A tangible and / or intangible unit that contains a person's identification data and is used for authentication in online services.
- Identity Verification Office. Entity that performs the identification tasks of the applicants, subscribers and those responsible for the certificates, verifies that the documentation provided by the applicant is original, current and obtains a certified copy of it.
- Qualified Trust Services Provider. For the purposes of this document, ANF AC is the trust service provider that, in accordance with Regulation (EU) 910/2014, provides one or more qualified trust services and to which the supervisory body has granted the qualification by registering it in the eIDAS trusted lists,

  (https://sede.serviciosmin.gob.es/Prestadores/TSL/TSL.pdf)
- Subscriber. Natural person requesting the certificate.
- Subject. Natural or legal person for whom the certificate will be issued, the certificate holder, who may or may not coincide with the subscriber.

  When the subscriber is the representative of the subject, he acts and commits himself both as subscriber and as subject.

  When there is no such relationship of representation between the subscriber and the subject, for example in corporate profile certificates for employees, in which it is the company that requests the certificate but the subject (holder) is the employee, both, subscriber and subject must be informed and commit themselves with their signature.
- Responsible for the certificate. Natural person expressly authorized by the subscriber to safeguard and activate the signature creation data.
- Service. Service contracted by the Subscriber and provided by ANF AC.

- Qualified Trust Service. A trust service that meets the applicable requirements established in eIDAS and which is provided by a Qualified Trust Service Provider.
- Website. For the purposes of this document Https://www.anf.es/
- Relying Party. All those natural or legal persons, or Public Administrations that, voluntarily, trust the electronic certificates, the electronic signatures and seals they generate.
- Terms and Conditions. This document describes the rights, obligations and responsibilities of the Subscriber, legal representative, responsible for the certificate, and Trusted Third Party while they use or trust the electronic certificate issued and / or ANF AC Services. The Terms and Conditions are part of the Contract.
- Certificate users.
    - Subject requesting the certificate, every certificate must be requested by a natural person, in their own name or as the legal representative of a legal entity.
    - Subscriber of the certificate, holder, natural or legal person identified in the certificate.
    - Signatory, the signatory is the person who owns a signature creation device and who acts on his own behalf or on behalf of a legal person whom he represents. In accordance with Art. 3.9) of the eIDAS Regulation: "signer: a natural person who creates an electronic signature."

1.3.2. Acronyms

- ANF AC. ANF Autoridad de Certificación Asociación ANF AC, con domicilio social en Paseo de la Castellana, 79, inscrita en el Registro Nacional de Asociaciones, Grupo 1, Sección 1, Número Nacional 171443 y NIF G-63287510.
- RA. Registration Authority.
- CA. Certification Authority (Qualified Trust Services Provider).
- CPS. Certification Practices Statement of ANF Autoridad de Certificación.
- LRDASEC. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- IVO. Identity Verification Office.
- CP. Certification Policy.
- QTSP. Qualified Trust Services Provider.
- IRM. Issuance Reports Manager.

2. General terms for eIDAS services

2.1. eIDAS Services provided by ANF AC

ANF AC is accredited to provide the qualified trust services outlined in this section. These services comply with the eIDAS Regulation and the LRDASEC.

Each service provided by ANF AC and its different categories is regulated by a specific policy which is published at ANF AC website.

eIDAS Service	ANF AC policy specific to the service	Applicable section of this document
Qualified certificates for electronic signature	OID 1.3.6.1.4.1.18332.3.1.	2, 3, 4.
Qualified certificates for electronic seal	OID 1.3.6.1.4.1.18332.25.1.1	2, 3, 4.
Qualified webiste authentication certificates (SSL/TLS)	OID 1.3.6.1.4.1.18332.55.1.1	2, 3, 5.
Qualified TimeStamping service	OID 1.3.6.1.4.1.18332.15.1	2, 6.
Qualified electronic signature/seal validation service	OID 1.3.6.1.4.1.18332.56.1.1	2, 7.
Qualified electronic signature/seal preservation service	OID 1.3.6.1.4.1.18332.61	2, 8.
Qualified electronic registered delivery service	OID 1.3.6.1.4.1.18332.60	2, 9.

2.2. Scope of the Terms and Conditions

This Terms and Conditions describe the main commitments assumed by ANF AC in the provision of the services and the main obligations that the Subscriber assumes when contracting them. The Certification Policy, the CPS and its addendum provide detailed information on the conditions of use of the qualified services, and are binding on the Subscriber.

The Subscriber and ANF AC formalize their relationship through a Subscription Contract for products and services. This "Terms and Conditions" document is part of it, and in the event of a conflict between the Subscription Contract and these Terms and Conditions, the provisions of the Subscription Contract shall prevail. Likewise, this document has been translated into different languages, in case of conflict the document whose content is in Spanish will prevail.

Once the Subscription Contract is ratified, ANF AC will grant the Subscriber access to the products and/or services contracted.

ANF AC will provide the products and / or services, and the Subscriber agrees to use the Services in accordance with the terms defined herein. The Subscriber agrees to review and comply with the conditions of use, principles and technical specifications of the Services.

ANF AC reserves the right to modify the Terms and Conditions at any time if, at its discretion, there is a justified need to do so. The publication date of this document is the effective date of the document.

2.3. Qualified Trust Services Provider, EU Trust Mark and Audits

ANF AC is a Qualified Trust Service Provider, therefore, you can make use of the eIDAS Trust Label following the indications of the Commission Implementing Regulation (EU) 2015/806 of May 22, 2015 by which specifications are established regarding the form of the 'EU' trust label for qualified trust services.

The certifications in conformity and official accreditations obtained by ANF AC can be verified on the website,

https://www.anf.es/acreditaciones/

ANF AC, with the periodicity established by the norms and standards on the matter, is audited by an accredited conformity assessment body in accordance with eIDAS, and against ETSI standards. ANF AC has achieved the certification under these technical specifications of all the services detailed in this document, as publicly stated on the website of the competent supervisory body and on the Spanish trust list (TSL).

https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

2.4. Scheduled and unscheduled outages

ANF AC will notify the Subscriber at least fifteen (15) days in advance of the scheduled interruption of the Service, by email and / or publication on the Website, including the reasons and the estimated time of restoration of the Service.

ANF AC will ensure that the **scheduled** interruptions of the Service:

- Do not exceed 2 times per calendar month;
- Do not exceed 12 times a year;
- Occur between 23:00 pm to 06:00 a.m .;
- are up to 3 hours at a time and up to 6 hours a month.

In case of **unscheduled** interruptions, ANF AC will notify Subscribers as soon as possible, by email and/or publication on the Website, and will ensure that the duration of unscheduled interruptions of the Service does not exceed:

- 45 minutes at a time during Business Hours and 90 minutes total per calendar month;
- 3 hours at a time outside of Business Hours and 6 hours in total per month.

It is not considered an uscheduled interruption if the number of failed requests during one of the periods described above is less than 10% of the total requests for the service.

2.5. Suspension of services

ANF AC will notify the Subscriber of any need to suspend the Service within a reasonable period of time. The Services will be suspended after the Subscriber does not rectify the communicated reasons within 7 days or within the period of time established by ANF AC.

Once the suspension has occurred, the service may be resumed if the Subscriber rectifies the communicated reasons for suspension within the period conferred for this purpose, which shall not be less than another 7 calendar days.

ANF AC has the right to suspend Subscriber Services without prior notice in the following cases:

- The Subscriber breaches the Terms and Conditions and/or the Contract.
- The Subscriber has a delay of ten (10) calendar days in the payment of an issued invoice;
- The Subscriber's actions pose a risk to the operation of the Services and their availability to other Subscribers.
- The Subscriber's actions pose a risk to the operation of the structure or the prestige of ANF AC.

ANF AC, in accordance with the rules that regulate its activity, has a Cessation Plan, to cover scenarios of termination of the service due to cessation of activity and guarantee its continuity.

2.6. Payment of services and billing

1. ANF AC, has the right to payment by the Subscriber for the services and products requested and effectively provided by ANF AC, or any of the entities that are part of the ANF AC Cluster. The price to be applied will be, except for specific agreement between the Parties, the price list published on the Website. The Subscriber in the

process of requesting his certificate, receives detailed information on the services and products that he can consume and the prices applicable to each one of them. The Price List can be freely modified by ANF AC.

2. ANF AC issues invoices to Subscribers for the services provided and products supplied. The direct debit of the receipt against the Subscriber's bank account is established as a form of payment. Non-payment of this receipt entitles ANF AC to suspend the Service, revoke the Certificates issued, and initiate the corresponding claim actions for the amount invoiced, as well as for the expenses and interest incurred.

3. The Subscriber must pay the invoice for its Services to ANF AC within ten (10) business days from the date of issuance of the invoice.

4. ANF AC has the right to collect the expenses and interests caused by the non-payment by the Subscriber.

5. The price of certain products or services offered by ANF AC or, by entities belonging to the ANF AC Cluster, may be associated with an escalation by consumption. In this case, the price to be applied will be calculated based on the requests made by the Subscriber, within the period established by each escalation. Charges are calculated based on the minimum number of requests set in the Price List.

6. Requests made through the middleware provided by ANF AC are classified as Services and are priced in accordance with the Price List. ANF AC may charge an additional fee for the middleware use license.

7. The prices of the products and services do not include audit records, or the issuance of expert reports, or the statement of our experts before the Courts. In each case, and according to its complexity, rates will be applied according to the anticipated budget and accepted by the Subscriber or Relying Parties.

2.7. Refund Policy

ANF AC handles reimbursement requests on a case-by-case basisg.

2.8. Modification of the contract

1. ANF AC has the right to make unilateral modifications to the Contract by making a one (1) month advance notice to the Subscriber, but in no case may it exercise this clause more than three (3) times a year. The Subscriber will be notified in accordance with the provisions of this document..

2. If the Subscriber does not agree with the unilateral modification made by ANF AC to the Contract, the Subscriber will have the right to terminate the Contract.

3. The Subscriber does not have the right to assign the Contract, nor the corresponding rights and obligations to third parties without the written consent of ANF AC. Any transfer of the acquired rights and the obligations assumed in the Contract to third parties by the Subscriber without the consent of ANF AC will be null.

4. Modifications and additions to the Contract will be documented in writing unless agreed by the Parties..

5. If the modification of the data of the Contract requires changes in the configurations of the Services, ANF AC must implement them within the following ten (10) business days.

2.9. Duration and termination

The Contract is concluded for an indefinite period, unless the Parties define otherwise in the Contract, and will enter into force at the time of its ratification, unless agreed by the Parties.

If the Subscriber is a natural person, the Contract will terminate upon his death. If the Subscriber is a legal entity, the Contract will be terminated with its dissolution / presentation of the contest request. The Contract will also be terminated after the dissolution, or cessation of activity, or loss of official accreditation of ANF AC, or prior agreement of the Parties, or unilateral termination for reasons established in the Contract.

ANF AC has the right to unilaterally resolve in the following cases:

- The Services have ceased to be provided by ANF AC, giving the Subscriber two (2) months' notice;
- The Subscriber uses the Services for purposes for which they were not provided, to carry out an illegal activity, or in a way that may cause substantial damage, whether material or in the good name and prestige of ANF AC or third parties. The termination will be immediate without prior notice;
- The Subscriber has not rectified the reasons for the suspension within one (1) month from the suspension of the Service.
- The Subscriber does not comply with his obligations, especially: payment of invoices, keeping his information updated and accurate, not communicating a risk situation in which the certificates that have been supplied may be found.

The termination of the Subscription Contract will not release the Subscriber from his obligation to pay the bills for the Services, until the expiration date specified in the Contract.

The termination / rescission of the Contract will not have any impact on the execution or settlement of the financial credits that arise before the termination / rescission of the Contract.

2.10. Privacy policy, data use and confidentiality

The Parties undertake to safeguard the confidentiality of the other Party's information, that of its clients, business partners, and employees. Special reserve will be given to personal data, documents that have been communicated for the provision of services, as well as consumption made, the financial situation and the transactions that are disclosed due to the celebration, execution, modification and / or termination of the contract. and All parties agree not to disclose such information to third parties without the consent of the other party, except in compliance with a judicial or tax mandate. This clause has an unlimited duration, it persists even after the termination of the Contract.

When the Services are provided to third parties, the Parties have the right to refer to the existence of the Contract, if it is expressly established in said document, but not to the details regarding its substance or technical data, or economic information such as prices, escalations or any other agreed commercial conditions.

All information that has become known while providing services and is not intended for publication is confidential. The Subscriber has the right to obtain information from ANF AC about him / her, except that which affects the intellectual or industrial property of ANF AC. Non-personalized statistical data on ANF AC products and services is considered private intellectual property information of ANF AC. ANF AC may publish statistical data that does not include the identity of the Subscriber, nor is it identifiable.

ANF AC protects the confidential information and data transmitted by the Subscriber, Subject, and, where appropriate, the Responsible for the Certificate. This information has security measures that guarantee integrity, availability and access control, all data transmission is carried out using the SSL / TLS communication protocol.

ANF AC, in order to maintain a low risk level, has developed different Security Policies and implemented technical safeguards and procedures that have been audited in accordance with ISO 27001, Information Security Management Systems. Assuming that there is no configuration that guarantees 100% security of the assets, there is a Business Continuity and Disaster Recovery Plan that has been audited accordingly. In addition, a Cyber Insurance Policy is available to cover assets that may be damaged by hacker or cracker attacks.

ANF AC, in order to comply with the Principle of Proactive Responsibility (Accountability) established by the General Data Protection Regulation (EU) 679/2016 (RGPD), as well as with the guidelines approved by the European Data Protection Commission and the Spanish Control Body (AEPD), has carried out a Data Protection Impact Assessment (EIPD) of each of the products and services with a low risk level result.

In addition, ANF AC has a Privacy Policy published at

https://www.anf.es/politica-de-privacidad/

The obligation of confidentiality will not extend to the disclosures that ANF AC makes to its auditors, to organizations that exercise supervision in accordance with the law, legal advisors and, in compliance with a court order.

2.11. Notification Obligation and Document Format

The Subscriber agrees to immediately notify ANF AC of any change in personal affiliation, especially the representation data of a third party for which he has intervened, professional qualification data, or data that is contained in the Contract, or that provided by filling in any form, or in response to requests from AR, OVP or RDE. The reliability and accuracy of the new information must be accredited by the subject of interest directly or by means of verification in the official registry.

Unless its modification is communicated, the contact information provided by the Parties will be understood to be current and their personal trusted mailboxes. In particular, the email address and mobile phone number provided by the Parties are considered as communication channels accepted by them to issue and receive notifications.

The Subscriber is responsible for the consequences related to the proper custody and use of the email address and / or mobile phone number that they have provided to ANF AC. As well as the credentials that you have identified with ANF AC as belonging to operators that are under your direction, follow your instructions, they are trusted and, therefore, the work orders and accesses that these operators carry out, will be considered as carried out by the own subscriber. The Subscriber has the responsibility to safeguard their trusted mailboxes (eMAIL and Mobile) and to properly supervise and instruct their operators, therefore, cases in which the Subscriber alleges that a third party has fraudulently used or misused the account. of mail, terminal in which the SIM of the mobile number is installed, or even, credentials of its authorized operators, will not be cause for repudiation of the transaction. This responsibility will end at the moment in which the Subscriber communicates to ANF AC the revocation of these accounts or credentials.

The Subscriber and the Subject consent to the storage of data related to the certificate and the retention period of the information that is legally applicable.

Any notification that ANF AC makes to the Subscriber will be made electronically to any of the trust mailboxes indicated by the Subscriber himself, including notifications regarding changes in the Subscription Contract, or in these Terms and Conditions.

2.12. Responsibility of the parties

Relying Parties are responsible for direct material damage caused to the other Party, to a third party due to non-compliance or improper compliance with the obligations assumed by the Subscription Contract or for violation of applicable legislation.

In the case of the certificate validation service, OCSP Responses or CRL Listings, ANF AC is responsible for ensuring that the most recent validity information related to the certificates it issues is used to issue the OCSP Response and is included in the corresponding CRL List.

ANF AC is not responsible for the breach of the obligations of the Subscriber, Subject and, where appropriate, the Certificate Responsible stipulated in this document.

2.13. Major force

Causes of force majeure releases the Parties from liability in the event that the fulfillment of the obligations derived from the Contract is hindered. Force majeure are circumstances independent of the intention of the Parties, which are unpredictable, and prevent the obligations arising from the Contract from being carried out.

A Party shall notify the other Party of the force majeure circumstance as soon as possible.

Force majeure will not release the Parties from the obligation to adopt as soon as possible all the measures that are reasonably possible to prevent or mitigate the damages derived from the breach or non-compliance of the Contract.

In the event that the force majeure circumstance applies for a duration of more than 30 (thirty) days, either Party shall have the right to unilaterally terminate the Contract by written notification to the other Party..

2.14. Service Level Agreement (SLA)

2.14.1. Scope of the Service

This Service Level Agreement (SLA) aims to define the conditions, service levels, and procedures applicable to the technical support and service operations provided by ANF AC to its CLIENT, in accordance with the main service agreement.

2.14.2. Declaración de responsabilidad

ANF AC, está comprometida con la calidad de sus servicios, ofreciendo garantías de respuesta a peticiones, de continuidad del servicio y de asistencia técnica:

a) Guarantee of Response to Requests.

The service measures the time elapsed between the registration of the request in its systems until the start of its treatment, also controlling the workload of each server. Docker technology is used to ensure that the response time, regardless of concurrency and peaks, is always within optimal parameters. In addition, all services are permanently monitored to determine any risk of lack of resources or incidence.

b) Service continuity guarantee.

ANF AC guarantees a 95 % service level, except in cases of:

- Lack of programmed availability, with seven (7) days' prior notice to final users and clients. Except in an emergency (such as a security risk or critical error or risk of critical error), ANF AC is committed to devoting its best efforts to schedule inactivity time during weekends and early mornings.
- Lack of availability stemming from unforeseen circumstances beyond ANF AC's control, such as instances of force majeure.

Classification of incidences

When recording an incidence in the system, it will be classified according to the degree of impact in the service. Based on this classification, a technical intervention will take place.

Critique level	Description	Response time	Resolution time
Anomaly 1: Critical	Incidence causing a critical impact on the business. Client experiences total or significant loss of the service.	1 hour*	10 hours*
Anomaly 2: High	Incidence causing notable impact on the business. Client experiences significant interruptions of the service.	4 hours*	30 hours*
Anomaly 3: Moderate	Incidence causing some impact on the business: - A defect that causes critical impact on the business that can be avoided. - Certain functions in the software are not operational but the business process is still operational.	1 day*	Reasonable follow-up will be provided to requests, as well as needed answers.
Anomaly 4: Low	Incidence causing a decline in service quality, without fully causing interruptions.	2 days*	Reasonable follow-up will be provided to requests, as well as needed answers.

* corresponds to business hours (8x5)

"Response" shall be understood as the formal acknowledgment of receipt and the assignment of a technician responsible for the case.

Should an incidence result from, or be directly linked to an anomaly or design error affecting the solutions, ANF AC will provide an alternate solution and a date will be set in order to rectify said anomaly or error.

c) Technical assistance service guarantee.

The technical department's business hours are Monday through Friday from 9.00 to 18.00. Urgent service requests (critical impact level) must be requested exclusively through 24x7 telephone support

- Business hours + 34 932 661 614
- Outside business hours, contact details of the account manager (telephone and email), which shall be provided to the CLIENT on an individual basis.

2.14.3.Claim procedure

The Subscriber may initiate the claim by e-mail to the customer service department at the address soporte@anf.es, within a maximum period of 30 days after the claimed period.

2.14.4.Limitation of SLA liability

ANF AC cannot be held responsible for the breach of this SLA in situations beyond its control, such as:

- Defects in the equipment or applications provided by the Subscriber.
- Failures caused by inadequate management or omission on the part of the Subscriber, as well as failures caused by third parties that intervene under the direction of the Subscriber.
- Denial of service attacks and other security impacts beyond the control of ANF AC.
- Workload situations directly caused by abuse or inappropriate use of the services by the Subscriber.
- ANF AC, in order to provide the service to the Subscriber, it may have to consult another QTSP, for example, query the OCSP status of third-party certificates. In these cases, the provision of the service may be affected by the practices, policies and SLAs of other TSPs that are not under the control of ANF AC.
- Reasons of force majeure

2.15. Retention period

The period of time during which the information relating to the qualified trust services provided by ANF AC will be retained will be 15 years from the expiry of the certificate or the end of the service provided.

3. General terms for electronic certification services

3.1. Types and purposes of electronic certificates

ANF AC issues qualified certificates for electronic signature, electronic seal, and website authentication, in accordance with the eIDAS Regulation. Electronic certificates are an electronic certification that links their holder with some signature verification data and confirms their identity. Each certificate issued is subject to a specific Certification Policy (CP) which has a unique OID identifier. All the documentation related to the policies corresponding to the certificates issued by ANF AC, is published at :

https://anf.es/en/legal-repository/

Each respective CP details the validation process followed by ANF AC prior to the issuance of the certificate, the return, renewal, revocation, scope, permitted uses, attributes and limitations. The proof of possession of the private key and the certificate acceptance process is defined in the CPS of ANF AC.

3.1.1. Qualified certificates for electronic signature

All certificates issued by ANF AC are in accordance with the eIDAS Regulation, regulated as established in the CPS *(OID 1.3.6.1.4.1.18332.1.9.1.1)* and subject to their respective Certification Policy (CP).

Qualified electronic signature certificates are subject to CP OID 1.3.6.1.4.1.18332.3.1. Available modalities:

Type	Storage		OID
Natural Person Class 2	Cryptographic software.		1.3.6.1.4.1.18332.3.4.1.2.22
	QSCD		1.3.6.1.4.1.18332.3.4.1.4.22
	QSCD. Centralised service.		1.3.6.1.4.1.18332.3.4.1.5.22
Corporate Natural Person	Cryptographic software.		1.3.6.1.4.1.18332.3.4.1.6.22
	QSCD		1.3.6.1.4.1.18332.3.4.1.7.22
	QSCD. Centralised service.		1.3.6.1.4.1.18332.3.4.1.8.22
Legal Representative of Legal Person	Cryptographic software.		1.3.6.1.4.1.18332.2.5.1.3
	QSCD		1.3.6.1.4.1.18332.2.5.1.10
	QSCD. Centralised service.		1.3.6.1.4.1.18332.2.5.1.14
Legal Representative of Entity without Legal Personality	Cryptographic software.		1.3.6.1.4.1.18332.2.5.1.6
	QSCD		1.3.6.1.4.1.18332.2.5.1.11
	QSCD. Centralised service.		1.3.6.1.4.1.18332.2.5.1.15
Legal Representative for Sole and Joint Directors	Cryptographic software.		1.3.6.1.4.1.18332.2.5.1.9
	QSCD		1.3.6.1.4.1.18332.2.5.1.12
	QSCD. Centralised service.		1.3.6.1.4.1.18332.2.5.1.13
Public Employees	High Level	HSM Token	1.3.6.1.4.1.18332.4.1.3.22
	Medium Level	Cryptographic software.	1.3.6.1.4.1.18332.4.1.2.22

Qualified certificates for electronic signature are always issued in the name of a natural person. They can include legal representation and state the legal person they represent. In any case, it is noted that in accordance with the provisions of article 3,9) of the eIDAS Regulation: “signatory: a natural person who creates an electronic signature”.

The maximum period of validity of these certificates is five (5) years.

Article 6.1.a) of Law 6/2020 of November 11, regulating certain aspects of trusted electronic services, expressly contemplates that qualified electronic signature certificates may record the passport number of its holder, when This

person lacks, for lawful reasons, a National Identity Document number, a foreigner's identity number or a tax identification number.

For its part, article 27.1 of Royal Decree 203/2021, of March 30, which approves the Regulations for the action and operation of the public sector by electronic means, establishes that "Systems based on qualified electronic signature certificates accepted by Public Administrations for the electronic identification of individuals referred to in article 9.2.a) of Law 39/2015, of October 1, issued under Law 6/2020, of November 11, must contain as attributes, at least, your name and surname and your National Identity Document number, Foreigner Identification Number or Tax Identification Number that is unequivocally stated as such."

Consequently, qualified electronic signature certificates in which the passport number of the certificate holder is entered as an identifier ARE NOT SUITABLE for use in electronic relations with Public Administrations. THEY ARE SUITABLE for any other permitted use.

3.1.2. Qualified certificates for electronic seal

Qualified certificates for electronic seal are subject to CP OID 1.3.6.1.4.1.18332.25.1.1. Available modalities:

Type	Support	OID
Electronic Seal *(QSealC)*	Cryptographic software	1.3.6.1.4.1.18332.25.1.1.1
	QSCD	1.3.6.1.4.1.18332.25.1.1.4
	QSCD. Centralized service.	1.3.6.1.4.1.18332.25.1.1.9
	Distributed key management software	1.3.6.1.4.1.18332.25.1.1.10
AA.PP. Electronic Seal *(QSealC AA.PP.)*	Cryptographic software	1.3.6.1.4.1.18332.25.1.1.3
	QSCD	1.3.6.1.4.1.18332.25.1.1.2
	QSCD. Centralized service.	1.3.6.1.4.1.18332.25.1.1.11
	Distributed key management software	1.3.6.1.4.1.18332.25.1.1.12
PSD2 Electronic Seal *(QSealC PSD2)*	Cryptographic software	1.3.6.1.4.1.18332.25.1.1.5
	QSCD	1.3.6.1.4.1.18332.25.1.1.6
	QSCD. Centralized service.	1.3.6.1.4.1.18332.25.1.1.7
	Distributed key management software	1.3.6.1.4.1.18332.25.1.1.8

The subscriber has to be a legal person. They allow the issuance of electronic seals, which are an electronic declaration that links the validation data of a seal with the legal entity that subscribes the certificate. Recital 65 of the eIDAS Regulation establishes that: "In addition to authenticating the document issued by the legal entity, electronic seals can be used to authenticate any digital asset of the legal entity, for example, computer programs or servers."

The maximum period of validity of these certificates is five (5) years.

3.1.3. Qualified Website Authentication Certificates (SSL/TLS - QWAC)

Website authentication certificates (SSL / TLS) comply with the requirements established in the CA/B Forum Baseline Requirements (BR) and ETSI standards. In addition, SSL certificates identified as EV comply with the CA/B Forum EV Guidelines and Annex IV of the eIDAS Regulation.

Type	Support	OID
SSL Secure Server	DV	1.3.6.1.4.1.18332.55.1.1.1.322
	OV	1.3.6.1.4.1.18332.55.1.1.7.322
Qualified SSL Secure Server *(QWAC)*	Qualified EV *(QWAC)*	1.3.6.1.4.1.18332.55.1.1.2.322
	PSD2	1.3.6.1.4.1.18332.55.1.1.8.322
EV Electronic Headquarters	Medium Level	1.3.6.1.4.1.18332.55.1.1.5.322
	High Level	1.3.6.1.4.1.18332.55.1.1.6.322

The purpose of these certificates is to establish data communications via TLS / SSL in computer services and applications, especially for: the identification of the organization that owns the domain (DNS), providing a reasonable guarantee to the user of an Internet browser that the website you access is owned by the Organization identified in the certificate through its name and address. The encryption of communications between the user and the website, facilitating the exchange of the encryption keys necessary for the encryption of information over the Internet.

The maximum period of validity of these certificates is one (1) year.

3.2. Certificate acceptance

Upon receiving the Certificate issued by ANF AC, they will not use it until they verify the correspondence of the data included in the certificate with the information provided by the Subscriber, as well as the adequacy of the certificate to the request made. The use of the certificate by the Subscriber, presupposes its full acceptance and conformity.

3.3. Certificate usage limits

The Subscriber and, where appropriate, the legal representative, or the subject if they were different, undertake to make appropriate use of the certificate in the relationships they maintain with trusted third parties, in accordance with the authorized uses stipulated in the CP, in the contract signed between ANF AC and the subscriber. , especially those described in the section "Obligations of the Applicant, Holder and Responsible for the Certificate", and also, assuming the limitation of liability set by the issuer in the body of the certificate in the field QcLimitValue OID 0.4.0.1862.1.2.

3.4. Obligations of users of the certificate and services

Prior to the issuance of the certificate or provision of the service, the Subscriber, where appropriate his legal representative, have been informed of all the rights and obligations, applicable fees, and have access to the current CPS and CPs.

3.4.1. Obligation in the application

The Subscriber and the Subject undertakes to apply the necessary measures to guarantee the conformity of the request, providing exact data and following the procedures established for this purpose by ANF AC.

The Subscriber agrees to pay the fees corresponding to the Certificates and/or Services requested, and assumes the obligation to process the request with the sole interest of making use of the purpose for which it is marketed by ANF AC.

Is totally prohibited:

- reverse engineer;
- any action that has the purpose of putting stress on ANF AC's systems, applications, or products;
- any action that has the objective of analyzing, evaluating, or discovering the technology used by ANF AC;
- any action that has the objective of analyzing, or evaluating, or knowing the procedures, algorithms or functions of the applications or solutions of ANF AC; and
- any action that does not correspond to the sole purpose for which the product or service has been provided by ANF AC.

Both parties acknowledge the significant investment in material and human resources made in the development of this platform of services and PKI products, which is an exclusive intellectual property of ANF AC. Therefore, given the serious damages that any of the actions listed above entails, it is established that in the event that the Subscriber or any collaborator, or person under his / her direction incurs in any of the prohibitions listed above, ANF AC will be compensated with the amount of ONE HUNDRED THOUSAND EUROS.

3.4.2. Information obligation

The Subscriber and, where appropriate, the legal representative requesting the certificate o Subject different from the subscriber, authorize the publication and free dissemination of the public part of their certificate without any type of restriction and, in the event that the certificate incorporates associated powers or commandments, they authorize the free publication of the same, especially as part included in the electronic signatures.

If the Subscriber and the requesting subject, or the person responsible for using the certificate are not the same entity, the Subscriber must inform of the obligations applicable to the Subject and / or person responsible for use, specifically:

- The information submitted to ANF AC is accurate and complete, in accordance with the requirements of the CP and CPS, particularly in relation to the registration form.
- The loss of validity of any information included in the certificate must be communicated without delay to ANF AC.
- The key pair is only used in accordance with the limitations notified to the Subscriber
- Reasonable care is exercised to avoid unauthorized use of the Subject's private key.

Duty to immediately inform ANF AC in case of:

a. Inaccuracies or changes related to the information contained in the Certificate, urging the revocation of the certificate when said modification constitutes cause for revocation.

b. The loss, theft or any risk that compromises the private key. After the commitment of the private key, its use will be immediately and permanently interrupted.

c. The loss or mere suspicion of risk in the personal control of the signature activation data (PIN).

3.4.3. Obligation of correct use

The Subscriber and, where appropriate, the Subject and/or the Responsible for the Certificate is/are obliged to use the certificates in compliance with the Terms and Conditions, Policies, CPS and addendum of ANF AC, in a purely enunciative manner in no limiting case, the following obligations are highlighted:

a. They undertake to review and comply with these Terms and Conditions for the use of certificates and services, and the rest of the obligations that are detailed in the corresponding Certification Policy to which the issuance of the certificate or provision of the service is subject, and to the Certification Practice Statement and its addendum, all these documents are published on the website,
https://www.anf.es/repositorio-legal/

b. They undertake to adapt the use of the Certificates and / or Services contracted to the permitted uses and to accept the restrictions imposed on them by ANF AC.

c. They recognize that the PKI of ANF AC is a system open to the public, and that the free publication of the public part of the certificates, as well as the powers of representation that determine the scope of action of the legal representative, is the model followed by ANF AC to reinforce the trust of Relying Third Parties.

d. They will guarantee the proper use, private custody and preservation of the certificate supports.

e. In the event of using a secure cryptographic device, Subscriber and Subject assume the obligation to use it.

f. They will use the certificate appropriately and, in particular, they will comply with the limitations of use.

g. When creating electronic signatures/seals, the signer will ensure:

i. That the certificates are valid..
ii. That the electronic signature/seal generation devices used guarantee the privacy and full control of the signer regarding the signature generation data (private key) and signature activation data *(PIN)*.
iii. The electronic signature certificates issued by ANF AC, have as their sole purpose and destination, to prepare signatures with full legal effects, or to carry out identity authentication with full legal security. The use of these certificates to carry out test or test signatures or authentications is prohibited.
iv. It is the responsibility of the signer to maintain the custody and privacy of the private signature key and the signature activation data *(PIN)*. Therefore, the signer, until the moment of its revocation or expiration, will assume the obligations derived in the custody and use of the certificate, committing not to repudiate transactions in which his certificate has intervened in validity.

h. They will stop using the private key after the period of validity of the certificate, or when it has been revoked.

i. It will not be monitored, nor manipulated, it will be subjected to tests or stress tests, nor will reverse engineering acts be carried out on the certification products and services, without express written permission of ANF AC.

j. They will not use the private keys corresponding to the public keys contained in the certificates, for the purpose of signing any certificate, as if it were a CA.

3.4.4. Obligation of protection and custody

The Subscriber and, where appropriate, the Subject and/or the Responsible for the Certificate is/are obliged to be diligent in the custody of their private key, and will maintain the privacy of the signature activation data in order to avoid unauthorized uses.

They will not intentionally compromise the security of the certification services.

The transfer of the certificate to centralized electronic signature services is restricted to centralized ANF AC services. The transfer and custody to other providers or companies is prohibited, even if they are qualified providers of trust services. Breaking this obligation can lead to serious harm to trusted third parties by jeopardizing the legal effectiveness of the transactions, which in turn causes serious damage to the image and prestige of the ANF AC PKI. In case of infringement of this obligation, the parties agree to compensation in favor of ANF AC of FIVE THOUSAND EUROS.

3.5. ANF AC (CA) Obligations

3.5.1. Obligations in the provision of the certification service

The obligations of ANF AC are defined in the CPS of ANF AC. It should be noted:

Generally:

- Provide certification services in accordance with the provisions of the CPS, in the corresponding CPs, and respecting the provisions of current legislation, especially Regulation (EU) 910/2014 (eIDAS), Law 6/2020 (LRDASEC), Regulation (EU) 679/2016 (RGPD), Organic Law 3/2018 (LOPDPGDD) and Law 34/2012 (LSSI).
- Issue, deliver, revoke or renew the certificates according to the instructions of the subscriber in the cases and for the reasons described in the CPS, CP and applicable regulations.
- Notify the subscriber of the proximity of the expiration date and, where appropriate, of the option to renew the certificate.
- Communicate to trusted third parties the validity status of the certificates issued by ANF AC through access to the CRLs revocation lists, and access to the OCSP Responder online consultation service *(in accordance with RFC 6960)*.

Of security:

- Use reliable systems and products that are protected against any alteration and that guarantee the technical and cryptographic security of the certification processes and systems, in accordance with its Security Policy.
- Take measures against the falsification of the media and guarantee confidentiality in the generation process and its delivery by a secure procedure to the signer.
- Use reliable systems to store qualified certificates that allow verification of their authentication and prevent unauthorized persons from altering the data, restricting their accessibility in the cases or to the persons indicated by the signer, and allowing the detection of any change that affects these security conditions.
- Periodically carry out regular security checks, in order to verify compliance with established standards.
- The correct management of your security, in accordance with the principles established by ISO / IEC 27001.
- Select exclusively suppliers that have the capacity to guarantee the security levels required by ANF AC, according to the type of services or products that they are going to supply.

Of personal:

- Employ personnel with the qualifications, knowledge and experience necessary to provide the services offered and the appropriate security and management procedures in the field of eDIAS services.
- Comply with the regulations and security standards ETSI, ISO, Protection of Personal Data.

Procedural:

- Before providing the service, ANF AC makes the corresponding terms and conditions, price, Statement of Certification Practices and Certification Policies available to all users.
- ANF AC has a plan to cease its activity in which the conditions under which it would be carried out are specified.
- ANF AC has a business continuity and disaster recovery plan.
- ANF AC will inform in advance the proximity of expiration of the certificate.
- ANF AC, in case of ex officio revocation, will report the causes of said revocation.
- All ANF AC public repositories are defined in the Certification Practice Statement.

3.5.2. Obligation to verify information

ANF AC will carry out the verifications it deems appropriate regarding the identity and other personal information, in compliance with what is required in the CPS, CP and applicable ANF AC regulations.

In case of errors in the information, deficient information or lack of supporting documentation, ANF AC will notify the subscriber to make the changes it deems necessary or request additional documentation, prior to the issuance of the certificate.

ANF AC reserves the right not to issue a certificate when it considers that the documentary justification is insufficient for the correct identification and authentication of the subscriber.

3.5.3. Retention Period

ANF AC will keep the evidence corresponding to the requests for issuance and renewal of certificates for a minimum period of 15 years from the expiration of the certificate or the end of the service provided, in compliance with section 5.5.2. of the CPS.

3.6. Using the certificate validation service

The validation service is in compliance with RFC 6960. And it complies with the provisions of Article 9.2 of Law 6/2020 (LRDASEC).

The access point to the OCSP and CRLs online consultations is outlined in the body of the certificate issued by ANF AC.

OCSP responders and revocation lists CRLs are free and publicly accessible.

3.7. Obligation of Relying parties

Relying third parties, prior to placing their trust in certificates issued by ANF AC or other certification services, must:

- Check and take into account the restrictions that appear in the certificate regarding its possible uses and the individualized amount of the transactions that can be carried out with it.
- Check the validity status of the certificates, and verify the authenticity and integrity of the certificates and any other certification services they wish to trust. To carry out the verification, a qualified validation system must be used, either from ANF AC or from another QTSP.

3.8. Limited warranty and disclaimer of liability

ANF AC, as provided in article 9.3.b) of Law 6/2020, regulating certain aspects of electronic trust services (LRDASEC), and in accordance with the provisions of the SSL certificate issuance and management guides of Extended Validation (EV) published by CAB / Browser Forum, a civil liability insurance has been established for the amount of FIVE MILLION EUROS (€ 5,000,000): This RC policy guarantees the patrimonial liability derived from the provision of services.

ANF AC will assume, up to the limit established in the certificate, the responsibilities contemplated in Art. 13 of Regulation (EU) 910/2014 (eIDAS), in Art. 10 of Law 6/2020 (LRDASEC), in the CPS and in the corresponding CP to the service of interest.

In any case, the following assumptions are excepted:

a. ANF AC will not be responsible for any direct and indirect, special, incidental, emergent damages, any loss of profits, loss of data, punitive damages, whether foreseeable or not, arising in relation to the use, delivery, license, operation or non-operation of the certificates, electronic signatures, or any other transaction or service offered or contemplated in the corresponding CPS or CP, in case of improper use, or when they are used in transactions that involve a risk greater than that expressed in the compensation limit of expressed by ANF AC and that appears in the corresponding certificate.

b. In all the cases provided for in article 11 of Law 6/2020, regulating certain aspects of electronic trust services.

c. ANF AC does not assume any other commitment or responsibility than those detailed in the CPS.

d. Specifically, the subscribers, their legal representatives and those responsible for the certificates when they fail to comply with the obligations contained in the CPS and in the CP corresponding to the service of interest.

e. Specifically, the third parties who trust when they fail to comply with the obligations contained in the current legislation in the CPS and in the CP corresponding to the service of interest.

3.9. Trust limits of eIDAS electronic signatures/seals.

Confidence in a signed message with an advanced or qualified electronic signature or seal, in compliance with eIDAS is based on the following conditions:

a. The electronic signature was generated using a valid qualified certificate for electronic signature/seal and can be verified using a verified certificate chain. To determine the validity of the certificate, it is necessary to verify, among other issues, that the issuer of the certificate was accredited in the TSL list of the country where it carries out its operations to issue that certificate at the time it was issued.

b. The type of certificate is appropriate and the trust is reasonable under the circumstances. If circumstances require additional guarantees, these must be obtained for such confidence to be reasonable. For this, it may be essential that the signature has included an express submission to a specific signature policy or that its scope can be deduced from the context of the signed document. If a signature policy is included, the signature will be validated against said policy.

c. The electronic signature was generated during the operational period of a valid qualified certificate for electronic signature/seal, and can be verified using a verified certificate chain. To determine the validity of the certificate, it may be essential to determine the exact time it was used, for this it may be necessary to include a qualified electronic time stamp or use a qualified service for the preservation of electronic signatures/seals.

d. The signature corresponds to the signed document, and the document and the certificate used are authentic. For this, a qualified service for the validation of electronic signatures/seals must be used.

Relying third parties or the signers themselves can only place their trust in the certificate issued by ANF AC or in the electronic signatures, after having proceeded to verify at least the conditions outlined.

The electronic certificates issued by ANF AC are qualified certificates that serve the purposes specified in the corresponding CP.

The registration information of all certificates issued and all events that take place during the life cycle of a certificate, including renewal and possible revocation, is kept for a period of at least fifteen (15) years.

4. Specific terms applicable to centralized certificates

4.1. Centralized electronic signature certificates and remote electronic signature service

ANF AC issues "Qualified Certificates of Centralized Electronic Signature" in accordance with eIDAS. These certificates issued by ANF AC are subject to the general terms of section 3 above. This section 4 details additional specific terms.

This type of certificate is subject to the corresponding CP according to the characteristics of the subscriber, natural person or legal representative, and they are uniquely identified by a specific OID.

ANF AC issues the following types of **Qualified Certificates of centralized electronic signature**:

a. Natural Person Class 2 certificate 1.3.6.1.4.1.18332.3.4.1.5.22
b. Legal Representative for Sole and joint administrators 1.3.6.1.4.1.18332.2.5.1.13
c. Legal Representative of a Legal Person 1.3.6.1.4.1.18332.2.5.1.14
d. Legal Representative of an Entity without Legal Personality 1.3.6.1.4.1.18332.2.5.1.15

It is noted that in accordance with the provisions of article 6 point 2 of Law 59/2003, of December 19, on electronic signatures (according to Final Provision 4.2 of Law 25/2015, of July 28): "*The signer is the person who uses a signature creation device and who acts on his own behalf or on behalf of a natural or legal person whom he represents. "*

On January 1, 2017, the PKI Governing Board approved the creation of the remote electronic signature service. This service has been adapted to comply with the requirements set out in Articles 29b and 39b, introduced by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024, amending Regulation (EU) No 910/2014 (eIDAS) with regard to the establishment of the European Digital Identity Framework.

This service uses a qualified electronic signature device (QSCD) that complies with the provisions of Annex II, and article 30.3 of the eIDAS Regulation and, therefore, is included in the list of qualified devices maintained by the European Commission in compliance with Articles 30, 31 and 39 of the eIDAS Regulation..

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

This remote signature service allows the Subscriber:

- generate theirkey pair (public and private),
- decide without third party intervention their signature activation data (PIN),
- generate the certificate signing request (CSR), and
- process the request to issue the certificate to ANF AC.

Once issued, the certificate is installed on the QSCD device. The signer has exclusive control over the use of his electronic signature creation data.

This remote signature service when it prepares signatures with qualified centralized signature certificates, meets the requirements of a qualified electronic signature.

4.2. Users specific obligations

In addition to what is established in section 3.4. of this document:

a. It undertakes to review and comply with the Terms and Conditions for the use of the Qualified Certificates of Centralized Electronic Signature. These are detailed in the corresponding CP, and in the CPS. These documents can be found on the Website.

b. It is committed to the correct use of the Qualified Certificate of Centralized Electronic Signature and to apply the necessary measures to guarantee the conformity of the request with the permitted uses and to accept the restrictions imposed on them by ANF AC.

c. It undertakes to apply measures to prevent access to the Qualified Certificate for Centralized Electronic Signature by third parties.

d. The subscriber, at the time of requesting his certificate, provides mailbox addresses of his trust that are under his exclusive control, email and mobile phone number. In these mailboxes ANF AC communicates, among other issues, the value of double authentication used in the remote signature system, therefore in case of change of address or number, loss, theft or mere suspicion of risk of any of them, you must inform the CA without delay.

e. The certificates must be used for their own function and established purpose, without being able to be used for other functions and for other purposes. Similarly, certificates should only be used in accordance with applicable law, especially taking into account import and export restrictions on cryptography that exist at any given time. In the case of Centralized Electronic Signature Certificates to sign electronically (non-repudiation and commitment to what is signed), to carry out identification and authentication processes before computer systems.

4.3. Specific ANF AC (CA) obligations for centralized certificates

4.3.1. Management of Qualified Remote Signature and Seal Creation Devices

ANF AC provides this qualified trust service under the following criteria:

In compliance with the requirements established in Articles 29b and 39b of Regulation (EU) 2024/1183, which amends Regulation (EU) No 910/2014 with regard to the European Digital Identity Framework.

In alignment with Commission Implementing Regulation (EU) 2025/1567 of 29 July 2025, laying down implementing provisions for Regulation (EU) No 910/2014 concerning the management of qualified remote electronic signature creation devices and qualified remote electronic seal creation devices as qualified trust services. In particular, with reference to the list of standards and specifications set out in its Annex, especially ETSI TS 119 431-1 V1.3.1.

4.3.2. Key generation for centralized certificates

In the field of Qualified Certificates of Centralized Electronic Signature, ANF AC for the generation of the keys, their storage and subsequent use, exclusively uses devices certified specifically in accordance with the applicable requirements in accordance with article 30.3 of the eIDAS Regulation and, therefore , included in the list of qualified devices maintained by the European Commission in compliance with articles 30, 31 and 39 of the eIDAS Regulation.

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

ANF AC makes available to subscribers secure communication channels and specific management and administrative security procedures.

ANF AC has a procedure for destroying the private key of subscribers who request it. The Subscriber who requires the destruction of his private key must identify himself personally before ANF AC, or one of its Registration Authorities, a notary public or make the request by means of an electronically signed document.

4.3.3. Secure signature creation environment

ANF AC applies specific management and administrative security procedures and uses reliable systems and products, including secure electronic communication channels to ensure that the electronic signature creation environment is reliable and is used under the exclusive control of the signer.

4.3.4. Custody

ANF AC guards the signature/seal creation data of the signer and protects them against any alteration, destruction or unauthorized access

Its continuous and total availability for the signer is guaranteed.

4.3.5. Backup

ANF AC duplicates the signature creation data solely in order to make a backup copy of the aforementioned data and always fulfilling the following requirements:

i. the security of duplicate data sets is of the same level as for original data sets;

ii. the number of duplicate data sets does not exceed the minimum necessary to ensure continuity of service:

4.3.6. Specific software for centralized certificates

Due to the technical and usability characteristics of the centralized certificate, the installation of specific ANF AC, Middleware software is required. ANF AC will provide said software to the user.

5. Terms applicable to website authentication certificates (SSL / TLS)

5.1. Specific obligations of the Applicant, Holder and Responsible for the SSL certificate

The subscriber guarantees and agrees to:

a. Install and use each SSL / TLS Certificate:
   i. only in the domains owned or controlled by the Subscriber and
   ii. only on servers accessible in the SubjectAltName listed in the Certificate;

b. The subject mentioned in each requested SSL / TLS Certificate has exclusive control of the domain names listed in said Certificate;

c. Inform ANF AC in case of losing exclusive control over at least one domain name listed in the Certificate;

d. Provide ANF AC with an operational contact that allows the AC to notify the APPLICANT at any time of incidents or anomalies related to the certificate, its revocation and replacement, if applicable.

The subscriber expressly understands and accepts that ANF AC's practices regarding the SSL/TLS certificate service may suffer variations and changes that affect the contracted certificate during its validity, without such changes being grounds for termination of the contract or any compensation, always and when they are motivated by an imposition of CA/Browser Forum or some application software provider that has agreed to include the root certificate of ANF AC in their distributed software.

5.2. Obligaciones de ANF AC (CA) específicas para certificados SSL

5.2.1. Keypair generation

ANF AC does not generate in any case the SSL/TLS certificate key pair.

5.2.2. Incidents and revocation

In case of detecting directly or by notification of a third party, any anomaly or breach in the SSL certificate issued, ANF AC will notify the subscriber of this circumstance within 24 hours and must investigate and correct the problem within 5 days.

ANF AC will notify the subscriber in case of need for revocation, and may unilaterally revoke the certificate in the first 24 hours in case of detecting that the certificate has been badly issued or in the event of a serious security incident. In which case, the certificate will be replaced by a valid one.

6. Qualified Timestamping Service Applicable terms

6.1. General terms

The ANF AC time stamp service complies with the eIDAS Regulation, the LRDASEC and the ETSI EN 319 421 standard "Electronic Signatures and Infrastructures (ESI): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps and other related standards" .

The TSU of ANF AC issues qualified electronic time stamps according to the eIDAS Regulation. ANF AC's TSU does not issue unqualified electronic time stamps. ANF AC issues the TSTs in accordance with the ETSI EN 319 421 standard and with the following OID: 1.3.6.1.4.1.18332.15.1. By including this object identifier (OID) when generating time stamps, ANF AC TSA stipulates compliance with this time stamp policy.

Qualified Electronic Time Stamps:

- link the date and time to the data in such a way as to reasonably eliminate the possibility of modifying the data without detection;
- are based on a temporary information source linked to Coordinated Universal Time, and
- have been signed by using an advanced electronic signature or sealed with an advanced electronic seal from ANF AC.

The URL of the service is specified in the Subscription Agreement. Each TST contains a time stamp policy identifier, a unique serial number and a TSU certificate that contains the identification information of the ANF AC TSA.

ANF AC accepts SHA256, SHA384, SHA512 hashing algorithms in timestamp requests and uses the SHA-256 cryptographic function to sign TSTs.

The keys in the TSU are 2048-bit RSA keys. The key is used only to sign the TSTs.

The useful life of a TST is indefinite.

ANF AC records all TSTs issued. Log records are retained for at least three (3) months. The time stamp protocols, which means each time stamp issued, are maintained for at least fifteen (15 years. ANF AC can demonstrate the existence of a specific TST from the request of a Trusting Third Party.

The use of the timestamp service is carried out according to the protocol described in RFC 5816, or in its most recent publication.

The service is based on, and its use subject to the Time Stamping Authority Policy and Statement of Practices, which is available on the website, www.anf.es

The technical parameters of the time stamp service, and the certificate of the time stamp service, is published on the website, www.anf.es

6.2. Subscriber obligations

The subscriber will respect what is established in the CPS of ANF AC, in the TSA Practice Statement and Timestamping Policy, as well as what is agreed in the contractual documents and, especially, the Terms and Conditions of ANF AC.

The Subscriber is obliged to verify the TST signature and to ensure that the certificate used to sign the TST was valid. To perform these checks, a qualified signature service and qualified electronic stamps must be used.

If the subscriber is not using an ANF AC timestamp client, they will need to check that the hash contained in the timestamp matches the hash they sent in their TST request.

If the subscriber does not use an ANF AC timestamp client, the subscriber is obliged to use the secure cryptographic functions for timestamp requests.

If the subscriber not contracted the service for the custody of evidence and long-term preservation of electronic signatures and stamps, the storage and conservation of the time stamps issued by the TSA is the responsibility of the subscriber.

The Subscriber is obliged to inform its end users (for example, Trusting Third Parties) about the correct use of the time stamps and the conditions of the CPS ANF AC TSA. In the event that the Subscriber is a legal entity, it will be responsible if the end users do not correctly comply with their obligations. When the Subscriber is an end user, he will be directly responsible if he does not correctly fulfill his obligations.

Prior to the issuance of the certificate, the Subscriber has been informed of all the rights and obligations in the use of this instrument, of the fees of the ANF AC certification services, and that he has received a copy of the CPS ANF AC TSA, as well It has given its full agreement to the publication and free dissemination of the public part of its certificate and, if it associates powers or commandments with it, it also authorizes its free dissemination and publication, without any type of restriction. It recognizes that the PKI of ANF AC is a system open to the general public, and that free publication is the model followed by ANF AC to reinforce the trust of Relying Third Parties..

6.3. ANF AC (TSA) Obligations

ANF AC TSA guarantees that its clock is synchronized with UTC within the stated accuracy of one (1) second using NTP.

ANF AC TSA supervises the synchronization of its clock and guarantees that, if the time indicated in a TST drifts or goes out of synchronization with UTC, such a case is detected. In case the TSA clock is derived from accuracy, no time stamps will be issued until the clock is synchronized.

The time stamping service is located in Spain, where a time signal is provided through the ROA (Royal Observatory of the Navy), a laboratory recognized by the international public body Bureau International des Poids et Mesures (BIPM). Declared for legal purposes as National Pattern of said unit, as well as the maintenance and official dissemination of the "Coordinated Universal Time" (UTC (ROA)) scale, considered for all purposes as the basis of legal time throughout the national territory (RD 23 October 1992, no. 1308/1992)

The timestamp service uses this ROA timestamp, and a set of NTP servers as time sources. With that configuration, the timestamp service achieves an accuracy of +/- 100 ms or better relative to UTC.

Log records are retained for at least three (3) months. Time stamp protocols, which means each time stamp issued, is kept for at least fifteen (15) years.

6.4. Obligations of Relying parties and verification of the status of the TSU

The Trusting Third Party is obliged to study the risks, responsibilities, limitations and uses related to the acceptance of the TSTs, which are included in the CPS ANF AC TSA and these Terms and Conditions.

The Trusting Third Party is obliged to verify the validity of the status of the TSU's public key certificate by reference to the CRL or OCSP services located in the certificate.

The public keys of the TSU will be made available to Third Parties who trust a public key certificate.

The Trusting Third Party is obliged to verify the signature of the TST and guarantee that the private key used to sign said TST has not been compromised until the moment of verification by reference to the CRL or OCSP services located in the

certificate. The Trusting Third Party is obliged to take the necessary measures in order to guarantee the validity of the TST beyond the validity period of the ANF AC TSA certificates..

6.5. Limited warranty and disclaimer of liability

ANF AC is responsible for the execution of all the obligations specified in the CPS ANF AC TSA in accordance with Spanish and European Union legislation.

ANF AC, to face the risk of liability for damages that may be caused by the time stamp service, has subscribed the corresponding civil liability insurance, and has increased the amount required by current legislation, up to the amount of FIVE MILLION EUROS (€ 5,000,000).

ANF AC will inform all Subscribers before ANF AC stops providing the time stamp services and will maintain the documentation related to the completed services and the necessary information in accordance with the processes established in the CPS ANF AC TSA.

ANF AC will not be responsible for:

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

b. Non-compliance with their obligations if said non-compliance is due to failures or security problems of the supervisory body (Ministry of Industry, Energy and Tourism), the data protection supervisory authority (Spanish Data Protection Agency), the Trust List or any other public entity.

c. Non-compliance if said non-compliance was caused by force majeure.

d. Due to the interruption of the service in compliance with section 7.7.2. of ETSI EN 319 421, whereby if ANF AC TSA detects that the time to be entered in a time stamp deviates or loses synchronization with UTC, it is obliged to stop the broadcast. When the service interruption is carried out in compliance with said rule, the subscriber will not have the right to claim.

e. The Subscriber, with the acceptance of the time stamp, exempts ANF AC from all responsibility, and in particular, undertakes to hold ANF AC harmless from any damage arising from any action or omission that results in liability, damage or loss, expense of any type, including judicial and legal representation that may be incurred, due to the publication and use of the time stamp, when any of the following causes concur:
    i. Falseness or erroneous manifestation made by the user of the time stamp.
    ii. Error of the user of the certificate when providing the data of the request, if in the action or omission mediated fraud or negligence with respect to ANF AC, the registration entity or any Third Party that trusts the time stamp.
    iii. Negligence in the protection of the private key, in the use of a reliable system or in maintaining the necessary precautions to avoid the compromise, loss, disclosure, modification or unauthorized use of said key.
    iv. Use by the Subscriber of a name, or other information in the certificate, that infringes the intellectual or industrial property rights of third parties.
    v. Improper use of the private key of the certificate, for operations that are not authorized in it.
    vi. Failure to pay the fees for issuance, renewal, payment of the Cryptographic Device, electronic signatures or any other that the subscriber has contracted.

f. Relying Parties who relies on the certificate undertakes to hold ANF AC harmless from any damage arising from any action or omission that results in liability, damage, loss or expense of any kind, including judicial and legal representation that may be incurred by the publication and use of the certificate, when any of the following causes concur:
    i. Breach of the obligations of the third party who trusts the certificate.

ii. Reckless reliance on a certificate, depending on the circumstances.
iii. Failure to verify the status of a certificate, to determine that it is not suspended or revoked.
iv. Verification of the certificate using devices not approved by ANF AC.
v. Do not use the signature re-marking service, when any of the cryptographic components are at risk in accordance with the publication that ANF AC makes on the Website for this purpose.

7. Qualified signature/seal validation services Applicable terms

The recipients of these Terms and Conditions are subscribers and Relying third parties.

7.1. Description of the service, regulatory and legal framework

The Qualified Electronic Signature Validation Service is provided in accordance with articles 32 and 33 of the eIDAS.

The Qualified Electronic Seal Validation Service is provided in accordance with article 40 of the eIDAS Regulation.

The Qualified Validation service applies the requirements established in clause 6.2 of ETSI EN 319 401, and works on the basis of a validation policy of signatures as input, that is, the validation of signatures/seals, is always carried out against a validation policy. The validation policies accepted and whose requirements are used to carry out the validation process of signatures and electronic seals are:

- ANF AC Validation Policty OID 1.3.6.1.4.1.18332.56.1.1
- Validation Policy that meets the basic criteria ETSI TS 119 441 OID 0.4.0.19441.1.1
- Validation policy that meets the qualified validation criteria ETSI TS 119 441 OID 0.4.0.19441.1.2
- ANF AC Validation Policy permanently updated and published at https://www.anf.es/repositorio-legal/

The Qualified Validation Service follows the requirements established by ETSI TS 119 102-2 and ETSI TS 119 441. In the event that ANF AC decides to make any variation in them, this variation will be included in the OID 1.3.6.1 Validation Policy. 4.1.18332.56.1.1 and service subscribers will be informed by email.

The qualified service of validation of advanced/qualified signatures/seals electronic (QSVS) of ANF AC, supports the following formats of QES/QESeal,

- XAdES - ETSI EN 319 132
- CAdES - ETSI EN 319 122
- PAdES - ETSI EN 319 142

And levels

- XAdES - B – T - LT y LTA
- CAdES – B – T - LT y LTA
- PAdES – B – T - LT y LTA

7.2. Specific terms

A. The service accepts the following levels: Qualified Signatures and Seals (QAdES) and Advanced Signatures and Seals (AdES)

B. In the case of multiple signatures, the signed document must be of the envelopement type (signature includes the signed document)

C. In the event that the signature includes non-current elements (eg, expired or revoked certificates, time stamps or obsolete cryptographic elements –ETSI TS 119 312-) the criteria published by the EU Commission and regulations in the matter, and especially what is established in this matter in ETSI TS 119102-1.

D. The proof of signature (PoE of the signature) is made up of the signed document and the signature, both elements can be included in a single file if the signature is envelopement.

E. In the event that the ANF AC Validation Service allows the subscriber to send only the hash summaries of the signed documents and the subscriber decides to use this option, the verification of the integrity of the signed document and its correspondence with the signature remains outside the control and responsibility of ANF AC.

F. ANF AC in the provision of its services currently uses SHA256 hash functions and RSA signature algorithm. In any case, ANF AC keeps track of the evolution of technology and always follows the recommendations of ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"

G. ANF AC, in order to provide the service, you may have to consult another QTSP, for example OCSP status query. In this case, the communication channel between ANF AC and other providers requires that the called PSC be qualified, the information received is signed and it is possible to validate it.

H. The validation service may be affected by the practices, policies and SLAs of other TSPs that are not under the control of ANF AC.

I. The rights and obligations of the recipients of this service and of ANF AC are set out in this document, in the CPS and in the corresponding CP.

8. Qualified signature/seals preservation services Applicable terms

The recipients of these Terms and Conditions are subscribers and Relying third parties.

8.1. Description of the service, regulatory and legal framework

The qualified electronic signature and seal preservation service complies with the provisions of Articles 34 and 40 of Regulation (EU) 910/2014 of the European Parliament and of the Council. And it is subject to the Policy for the preservation of qualified electronic signatures and qualified electronic seals OID 1.3.6.1.4.1.18332.61

The service for the preservation of qualified electronic signatures and qualified electronic seals of ANF AC, applies the requirements established in clause 6.2 of ETSI EN 319 401, and uses procedures and technologies capable of increasing the reliability of the signature and seal data. qualified electronics beyond the technological validity period.

The qualified electronic signature and seal preservation service complies with those established in the ETSI TS 119 511 V1.1.1 (2019-06) Annex A, B, C and D.

ANF AC provides the preservation service in the temporary storage mode (WTS). The duration of the service is the duration of the contract with the customer. Upon termination of the contract, ANF AC communicates to the client the option of being able to provide them with a copy and portability of the stored documents, for a period of 60 days, prior to their destruction. You can find information on the preservation profiles admitted are defined in the OID Preservation Policy 1.3.6.1.4.1.18332.61, available on the website https://www.anf.es/repositorio-legal/

The preservation service of ANF AC, in addition to being applied to electronic signatures and seals, can be applied to other objects, in particular to documents with tax or fiscal significance .

8.2. Specific terms

ANF AC provides the service of preservation of qualified electronic signatures and seals, with the following requirements:

a. The preservation platform uses the services of ANF AC TSA and has been developed to extend the reliability of the qualified electronic signature data beyond the technological validity period. In the same way, it applies to the preservation of electronic Seals which, according to article 40 establishes "mutatis mutandis will be applied to the preservationof the Seals". For this reason, the ANF AC preservation platform applies indistinctly to qualified electronic signatures and qualified electronic seals.

b. ANF AC will apply the requirements detailed in clauses 5 to 9 of ETSI TS 119 511 V1.1.1 (2019-06)

c. The preservation service will retain all the information necessary to verify the qualification status of the electronic signature or seal that would not be publicly available until the end of the preservation period.

d. The preservation service when it is not possible to collect and verify all the validation data, will cancel the preservation request.

e. The timestamps used in the preservation evidence are provided by ANF AC as a qualified TSA.

f. The preservation service has a digital service identifier that allows the service to be uniquely and unambiguously identified within an EUMS trusted list (https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers)

g. ANF AC's preservation platform provides:

- evidence of the existence of data over long periods of time; and
- extends the ability to validate a digital signature and maintain its validity status for long periods of time

h. The service provides proof of existence of:
   - The signature;
   - The signed data; and
   - The validation data (certificate paths, revocation information)

i. The demonstration of a proof of existence is based on two factors:
   - an audit of the preservation service according to the criteria established in ETSI TS 119511; and
   - the use of digital signature techniques that prove that the data thus authenticated has not been modified since a certain date.

j. The ANF AC preservation platform uses algorithms recommended by ETSI TS 119 312. When the ANF AC preservation service has access to the signed data, it proceeds to verify the signature and performs a new signature including a time stamp based on a new hash of the received information, thus guaranteeing the integrity and proof of existence of the signed data before the original hash algorithm is weakened.
   In the event that the preservation sender has only sent the hash of the signed data, the proof of the existence of the signed data is beyond the control and responsibility of the preservation service. The preservation client is responsible for creating submitted abstracts and preserving signed data. The preservation service will apply the signature and time stamp techniques to the hash received.
   In the event that the state of the art puts any of the cryptographic elements used at risk, the service will proceed to apply a new signature and time stamp using cryptographic components classified as secure.

k. Time claims are protected by obtaining a new timestamp that covers the original data.

l. Revocation of a certificate indicates that the use of the private key can no longer be trusted.
   The Preservation Service addresses this risk by including information on the status of the revocation through OCSP consultation. This procedure avoids the problem that the revocation information for the QTSP that issued the certificate is no longer available.
   This principle applies to digital signatures sent by the preservation sender, as well as any signature / time stamp created by the preservation service.

m. The preservation platform has two procedures so that subscribers can transmit the data objects:
   - API to establish communication between the subscriber's automated system and the ANF AC preservation platform.
   - End user console on web server.

n. In order to ensure the confidentiality of information, electronic data objects related to different owner organizations are stored and archived in specific folders, and intended for the exclusive use of each organization. In addition, each data object has a unique identifier of its owner (subscriber code) and access to the data is restricted based on its owner.

o. When the ANF AC preservation platform cannot collect and verify all the validation data, a denial of service will be made.

p. The service is only provided to customers who have signed the corresponding contract with acceptance of these Terms and Conditions and the Preservation Policy, OID 1.3.6.1.4.1.18332.61.

q. The subscriber, as stated in the OID Preservation Policy OID 1.3.6.1.4.1.18332.61 clause 6.7, may request the export of the data stored on the preservation platform. ANF AC will provide the information in a standardized format (always based on an open format). This service, depending on the volume and complexity of the information, will be previously budgeted and the cost will be borne by the subscriber.

r. Customers who require the import or export of electronic signature and seal preservation service packages must request it by sending an email to soporte@anf.es, indicating their customer details. ANF AC will process the request in accordance with the applicable requirements and will notify the customer of the procedure to follow.

9. Qualified electronic registered delivery service (eDelivery) Applicable terms

The recipients of these Terms and Conditions are the subscribers (senders), recipients and Relying third parties.

9.1. Description of the service, regulatory and legal framework

The Electronic Registered 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.

ANF AC has developed and has the Registered Delivery Policy OID 1.3.6.1.4.1.18332.60, to which all available service modalities are subject:

- **ERDS Service.** A Electronic Registered Delivery Service (ERDS) guarantees the safe and reliable delivery of electronic messages between the parties, which generates evidence of the shipping and delivery process for legal purposes . The level of security of the identification and intervention of the parties is medium / substantial.
- **QERDS Service**. eIDAS 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 the Conventional ERDS and the entities that provide them. The level of security in the identification and intervention of the parties is high.

ANF AC makes the CPS, the Policy corresponding to this service, and this Terms and Conditions document available to service subscribers, recipients and all trusting parties, these documents are permanently published in pdf format and can be downloaded at https://www.anf.es/repositorio-legal/.

The registered electronic delivery service complies with the provisions of Art. 43 of Regulation (EU) 910/2014 of the European Parliament and of the Council, and applies the requirements established in clause 6.2 of ETSI EN 319 401.

ANF AC's electronic registered delivery service is provided in accordance with the standards ETSI EN 319 521 “Policy and security requirements for Electronic Registered Delivery Service Providers”, and ETSI EN 319 522 “Electronic Signatures and Infrastructures (ESI) Electronic Registered Delivery Services ”And ETSI EN 319 531 V1.1.1.

9.2. Specific terms

9.2.1. Contracting the service.

The service is only provided to subscribers who have formally subscribed the corresponding contract by which they accept these Terms and Conditions and the Service Policy.

9.2.2. Constitution of the delivery

The Qualified Registered 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 at the moment 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 Electronic Registered Delivery Service Provider that a specific event, rigorously detailed, related to the delivery process occurred at a specific time. The evidence can be immediately delivered to the payer or it can be saved or it can be saved in a repository for later access by interested parties.

The evidence 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.

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

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

9.2.3. 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 exceed six months. Once this threshold is exceeded, the delivery data will no longer be available for receipt by the recipient.

9.2.4. 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 (SLA) are detailed in section 21.2 of these terms and conditions.

9.2.5. Information Management System Security

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

10. Applicable Law, Complaints and Conflict Resolution

The trust services provided by ANF AC are governed by the jurisdictions of Spain and the European Union since it is the place where ANF AC is registered as a QTSP.

Any controversy derived from the Terms and Conditions, Contract, contract or legal act, as well as those that derive or are related to it -including any question related to its existence, validity, termination, interpretation or execution- will be definitively resolved by arbitration of Law, administered by the Arbitration Court of the Distribution Business Council (TACED), in accordance with its Arbitration Regulations in force on the date of submission of the arbitration request.

The Arbitral Tribunal designated for this purpose will be composed of a single arbitrator, and the seat of arbitration and substantive law applicable to the resolution of the dispute will be those corresponding to the registered office of TACED.

If for any reason it is not possible to settle the controversy through the arbitration procedure outlined above, the parties, waiving any other jurisdiction that may correspond to them, submit to the resolution of any conflict that may arise between them, to the courts of the city of Barcelona, renouncing its own jurisdiction if it were different.

The Subscriber or other interested party can send their complaints or claims to the following email: info@anf.es