ANF AUTORIDAD DE CERTIFICACIÓN

2021

National Registry of Associations. Number 171,443. CIF G-63287510.

STATEMENT PRODUCT DISCLOSURE

PDS (*Product Disclosure Statement)*

QUALIFIED SERVICE OF CERTIFIED ELECTRONIC DELIVERY

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

ETSI IN319401 ETSI IN319421 ETSI IN319411 ETSI IN319-102 ISO27001 ISO9001 ISO17024 ISO26000

ANF AUTORIDAD DE CERTIFICACIÓN

Security level

Public Document

Important announcement

This document is the property of ANF Certification Authority

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

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

Contact information of the Qualified Trust Services Provider

Servicios de Confianza Cualificados

ANF Certification Authority (ANF AC), NIF G63287510, is the Certification Authority that, as a Qualified Trust Services Provider, issues qualified certificates under eIDAS.

Corporate management

Paseo de la Castellana, 79

28046- Madrid (Spain)

Administration - Legal Services - Engineering

Gran de les Vía Corts Catalanes, 996

08018 - Barcelona (Spain)

Electronic office:

https://www.anf.es

Electronic office:

info@anf.es

ANF AC makes contact forms available to the public through the electronic headquarters of ANF AC

- General matters in **https://www.anf.es/contacto/**
- Press in **https://www.anf.es/contacto/#prensa**

Qualified long-term signature and seal preservation services

ANF AC is a Qualified Trust Service Provider, and an accredited entity to provide the qualified certified electronic delivery service (QERDS).

QERDS of ANF AC, meets the requirements established in article 44 of Regulation (EU) No. 910/2014, of the European Parliament and of the Council, of July 23, 2014, regarding electronic identification and trust services for electronic transactions in the internal market (eIDAS).

It is a service that allows the transmission of data between the sender and the recipients by electronic means, provides evidence relating to the handling of the transmitted data, including proof of the sending and receipt of the data, and which protects the transmitted data against the risk of loss, theft, damage or any unauthorized alteration.

The communication channel used to deliver to the recipient's mailbox **it can be email (REM) or other,** as long as it guarantees the requirements established to be considered ERDS.

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

SIGN TO sign®

Platform Web
Sign to sign

API
Sign to sign

- **You can check your inclusion in the trusted list of trusted service providers (TSL - Trusted Service List) in Spain, through the link,**

https://sede.serviciosmin.gob.es/Prestadores/TSL/TSL.pdf

Service mode identifiers

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

ERDS	OID 1.3.6.1.4.1.18332.60.1
QERDS	OID 1.3.6.1.4.1.18332.60.2

Parties involved

1

QUALIFIED PROVIDER OF VALIDATION SERVICES (QSVSP).

In the context of this document ANF AC. ANF AC assumes general responsibility for the service, even when some functions are assumed by contracted third parties.

tw

ORDERING / SUBSCRIBER.

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

3

ADDRESSEE.

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

4

THIRD WHO TRUST.

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

ERDS service

The "Certified Electronic Delivery Service (ERDS - 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 in the identification and intervention of the parties is:

Medium / substantial level:

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

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

ANF AC intervenes as a service provider
Certified Electronic Delivery System (ERDSP).

QERDS service

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

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

High level:

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

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

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

Permitted uses

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

- Non-repudiation of origin and destination.

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

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

With the use of the qualified Certificate of Electronic Signature or qualified certificate of Electronic Seal, It is allowed to check that the document has not been modified. To ensure integrity, the well-known hash functions are used, which are used whenever an electronic signature or seal is made.

The use of this system allows to verify that a signed or sealed message has not been altered between sending and receiving.

Limits of use

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

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

Prohibited uses

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

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

The contracting of the service only admits the use of the service in the scope of activity of the client that contracts the service or the entity to which it is linked, in accordance with the purpose of the service.

The client may not, except in the specific agreement with ANF AC, make use of the service for commercial purposes. S**e understood by commercial use of the service, any action by which the client offers to third parties parties outside the subscriber owner,** for consideration or free of charge, the use of this certified electronic delivery service.

Obligations and responsibilities of the subscriber / payer and trusting third parties

In sections **9.6.3, 9.6.4, 9.9.2 and 9.9.3 of the Certification Practices Statement of ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1** and in the Terms and Conditions **OID 1.3.6.1.4.1.18332.5.1,** remain Defined the obligations of subscribers and trusting third parties.

> **In particular, the subscriber and the third parties who trust before placing their trust in the supporting documents issued by the service ERDS / QERDS, have the obligation to verify the validity of the electronic seal with which ANF AC authenticates them, having to use a qualified validation system for signature and qualified electronic seals.**

Obligations of the CA and its responsibilities

In sections **9.6.1, 9.6.2 and 9.9.1** of the **ANF AC OID Certification Practice Statement 1.3.6.1.4.1.18332.1.9.1. 1**and in the Terms and Conditions **OID 1.3.6.1.4.1.18332.5.1,** remain Defined the obligations and responsibilities of the CA.

> **ANF AC, to face the risk of liability for damages that may be caused by the certificate issuance service, as well as the intervention of its AR and OVP, has subscribed the corresponding civil liability insurance of FIVE MILLION EUROS (5,000,000. €).**

Policy Number:
HD IP6 2056529

Insurance carrier
HISCOX, SA,

Events, evidence and supporting document

Each ERDS service has a unique identifier.

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

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

The set of evidence generated in each certified electronic delivery service is compiled in a single PDF document called "Evidence Document". East document has a unique evidence identifier, includes i**ERDS dentifier,** In which the service modality is recorded, the final result of the service performed, and details information on all the evidence generated.

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

To obtain related evidence of the transmitted data, **the ERD application has of a system that allows obtaining an authenticated copy of the evidences and probative document of the transmission made.** The ERD application requires, prior to access, user identification, which will at least have a substantial security level.

CA liability limitations

In the section **9.8 of the ANF AC OID Certification Practice Statement 1.3.6.1.4.1.18332.1.9.1.1** and in the Terms and Conditions **OID 1.3.6.1.4.1.18332.5.1,** remain defined the liability limitations of ANF AC.

Especially,

Limitation of liability with the subscriber / payer

- **ANF AC does not assume responsibilities derived from denials of service,** except in those cases in which the subscription contract establishes a penalty in this regard.
- **ANF AC does not assume responsibility for the transactions carried out by its subscribers** by using your certificates.
- **ANF AC does not assume responsibility when the holder makes use of the certificates** using instruments that are not They are approved by ANF AC.
- **ANF AC takes advantage of other exemptions established in the Certification Policy** corresponding to the type of certificate in question.
- Except for what is established in this document, **ANF AC does not assume any other commitment or offer any other guarantee,** nor does it assume any other responsibility before certificate holders, their legal representatives and / or those responsible for certificates.

Limitation of liability with the trusting third party and recipients

- TO**NF AC does not assume responsibility when the trusting third party does not assume its obligation** to verify the status of the certified, using the verification instruments of ANF AC.
- **ANF AC takes advantage of other exemptions established in the Certification Policy** corresponding to the type of certificate in question.
- Except for what is established in this document, **ANF AC does not assume any other commitment nor does it offer any another guarantee,** nor does it assume any other responsibility before trusting third parties.

ANF AC does not guarantee the cryptographic algorithms nor will it be liable for damages caused by successful external attacks on the cryptographic algorithms used, especially if you saved the Due diligence according to the current state of the art, the PC, DPC and its addendum, and the in the **EIDAS Regulation and Law 6/2020, of November 11,** regulating certain aspects provisions of the electronic trust services.

It will not be liable for any software that has not been provided directly by ANF AC.

In l**electronic seal certificates and TSA / TSU certificates,** issued with the rating of qualified, the limit assumed by the CA is established in the certificate itself, specifically in the Extension "**QcStatements**" in the countryside "**QcLimitValue**" **OID 0.4.0.1862.1.2.** and / or in the proprietary extension **OID 1.3.6.4.1.18332.41.1.**

If no amount is set, it should be interpreted that the CA in its QSVSP operations does not assume the use of this certificate for transactions that carry any financial risk, and therefore the compensation limit is zero.

Service Level Agreement (SLA)

ANF AC, is committed to the quality of its services, and has prepared the document corresponding SLA (Service Level Agreement) with the **OID 1.3.6.1.4.1.18332.5.4**

1

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 peak consumption points, is always within optimal parameters.

tw

SERVICE CONTINUITY GUARANTEE

ANF AC, guarantees a service level of 99.99%. In the event of a service interruption, the following table shows the penalty that THE CLIENT is entitled to receive according to the degree of non-compliance with the objective, based on the average monthly response time by deduction of interruptions.

Privacy Policy

ANF AC is the entity responsible for the processing of personal data.

- **ANF AC has a Privacy Policy published in,**

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

ANF AC, is committed to the quality of its services, and has prepared the document corresponding SLA (Service Level Agreement) with the **OID 1.3.6.1.4.1.18332.5.4**

ANF AC protects its personal data files in accordance with the provisions of Organic Law 3/2018, of December 5, Protection of Personal Data for the Guarantee of digital rights, and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which Directive 95/46 / EC (General Data Protection Regulation) is repealed.

In accordance with Art. 8 of Law 6/2020, of November 11, regulating certain aspects of electronic trust services, this CPS is the security document for the purposes provided for in the legislation on data protection of a personal nature.

ANF AC has carried out a Data Protection Impact Assessment (EIPD) with a low risk level result.

- **ANF AC publishes its Register of Data Processing Activities in,**

https://www.anf.es/registro-de-actividades-tratamiento-de-datos/

- **To exercise the rights of the interested parties, you can contact our Delegate of Data Protection,**

delegadoprotecciondatos@anf.es

- **It also has an online form,**

https://www.anf.es/ejercicio-de-derechos/

- **For personal visit, previously arranged**

Gran de les Vía Corts Catalanes, 996
08018 - Barcelona (Spain)

- **You can call the phone:**

+ 34 **932 661 614**

Return policy

It does not apply to the qualified validation service of electronic signatures and seals.

Applicable law, inquiries and complaints

ANF AC's electronic time stamping service is carried out in accordance with,

- **Regulation (EU) No. 910/2014, of the European Parliament and of the Council, of July 23 from 2014,** on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
- **Law 6/2020, of November 11,** regulating certain aspects of electronic trust services.

ANF AC, makes available to subscribers and third parties who trust online service for,

- **Report problem with your certificate in,** https://micertificado.anf.es/
- **Report breach or misuse in,** https://anf.es/sat-incumplimiento-uso-indebido/
- **Open an incident in,** https://www.anf.es/ac/abrir-incidencia

It also offers customer service through the following channels:

- **In person, administrative address,** legal and technical, arranging a previous interview days working days of **9 a.m. to 2 p.m. and 3 p.m. at 18 h.**
- By phone, +**34 932 661 614**
- **e-mail,**
  - ◊ Administration: **administracion@anf.es**
  - ◊ Technical: **support@anf.es**
  - ◊ Commercial: **info@anf.es**
  - ◊ Legal: **mcmateo@anf.es**
  - ◊ Data protection: **delegadoprotecciondatos@anf.es**

Applicable norms and standards

The qualified certificate issuance service is carried out in accordance with reference standards, by way of example, it should be noted:

- **ETSI EN 319 401** "General Policy Requirements for Trust Service Providers"
- **ETSI EN 319 411** "Part 1: General Requirements"
- **ETSI EN319 411** "Part 2: Requirements for Trust Service- Providers issuing EUQualified Certificates"
- **ETSI EN 319 412** "Electronic Signatures and Infrastructures (ESI): Certificate Profiles"
- **ETSI EN 319 122-1** "CAdES digital signatures, Part 1: Building blocks and CAdES baseline signatures"
- **ETSI EN 319 122-2** "CAdES digital signatures, Part 2: Extended CAdES signatures"
- **ETSI EN 319 132-1** "XAdES digital signatures, Part 1: Building blocks and XAdES baseline signatures"
- **ETSI EN 319 132-2** "XAdES digital signatures, Part 2: Extended XAdES signatures"
- **ETSI EN 319 142-1** "PAdES digital signatures, Part 1: Building blocks and PAdES baseline signatures"
- **ETSI EN 319 142-2** "PAdES digital signatures, Part 2: Additional PAdES signatures profiles"
- **IETF RFC 3647** "Public Key Infrastructure Certificate Policy and Certification Practices Framework"
- **IETF RFC 6960** "Public Key Infrastructure Online Certificate Status Protocol - OCSP"
- **IETF RFC 3739** "Public Key Infrastructure: Qualified Certificates Profile"
- **IETF RFC 3161** "Internet X.509 Public Key Infrastructure Time-stamp Protocol"
- **ETSI TS 119 312** "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites "
- **ETSI TS 119 612** "Electronic Signatures and Infrastructures (ESI), Trusted Lists"
- **ETSI TS 119 441** "Policy requirements for TSP providing signature validation services"
- **ETSI TS 119 172-1** "Signature Policies, Part 1: Building blocks and table of contents for human readable signature policy documents"
- **ETSI TS 119 172-2** "Signature Policies, Part 2: XML format for signature policies"
- **ETSI TS 119 102-1** Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation "
- **ETSI TS 119 102-2** Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report "
- **ETSI EN 319 521** "Policy and security requirements for Electronic Registered Delivery Service Providers"
- **ETSI EN 319 522** "Electronic Signatures and Infrastructures (ESI) Electronic Registered Delivery Services"
- **ETSI EN 319 531** "Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Registered Electronic - Mail Service Providers"
- **ETSI EN 319 532** "Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Registered Electronic - Mail Service Providers"

Dispute resolution

EXTRAJUDICIAL PROCEDURE

ANF AC will endeavor to amicably resolve conflicts that arise with third parties for the exercise of their activity, only resorting to the procedure provided in the following section, when the agreement between the parties is unattainable.

JUDICIAL PROCEDEMENT

ANF AC submits voluntarily, for the solution of any litigious question that could arise from the exercise of their activity, to the institutional arbitration of the Arbitration Tribunal of the Distribution Business Council (TACED) https://www.taced.es, who is entrusted with the appointment of the Arbitrator - who will be the only one - and the administration of the arbitration - which will be fair - in accordance with its Regulations, binding itself from now on to comply with the arbitration decision.

If for any reason it is not possible to settle the controversy through the arbitration procedure outlined in the previous point, the Parties waive any other jurisdiction that may correspond to them and submit to the Courts for the resolution of any conflict that may arise between them. of the city of Barcelona, renouncing its own jurisdiction if it were different.

ANF AC official audits and accreditations

ANF AC, as a Qualified Trust Service Provider, has achieved official accreditation of its Public Key Infrastructure (PKI) in the following services:

- Issuance of qualified certificates of **Electronic signature.**
- Issuance of qualified certificates of **public employee.**
- Issuance of qualified certificates **centralized.**
- Issuance of qualified certificates **PSD2.**
- Issuance of qualified certificates of **electronic seal.**
- Issuance of qualified certificates of **electronic stamp PSD2.**
- Issuance of qualified certificates of **electronic seal and AAPP seal.**
- Issuance of qualified certificates of **SSL secure server.**
- Issuance of qualified certificates of **SSL secure server Electronic Office.**
- Electronic signature service **remote qualified.**
- Qualified service of **electronic time stamps.**
- Qualified service of **electronic delivery.**
- Qualified service of **long-term preservation.**
- Qualified service of **validation of qualified electronic signatures and seals.**

In addition, ANF AC has other accreditations and approvals for advanced IT services:

- Mozilla, Microsoft, Apple, Google approval for **issuance of certificates SSL electronics:**
  - ◊ **DV**
  - ◊ **OV**
  - ◊ **EV**
- **Certification Entity (EC)** in accordance with the Data Protection Agency Scheme for Data Protection Delegates.
- **Certified Scanning Services (LegalSnapScan)** accredited by the Agency Spanish Tax Administration.

In addition to ETSI audits (eIDAS services), ANF AC has achieved compliance audits against the standards:

- **ISO 27001: 2013** Information Security Management System
- **Iso 9001** Quality of service CA
- **ISO 17024** Certification of Persons
- **ISO 14001** Environmental Management System

Cryptographic Hardware Modules (HSM) used to provide the time stamping service,

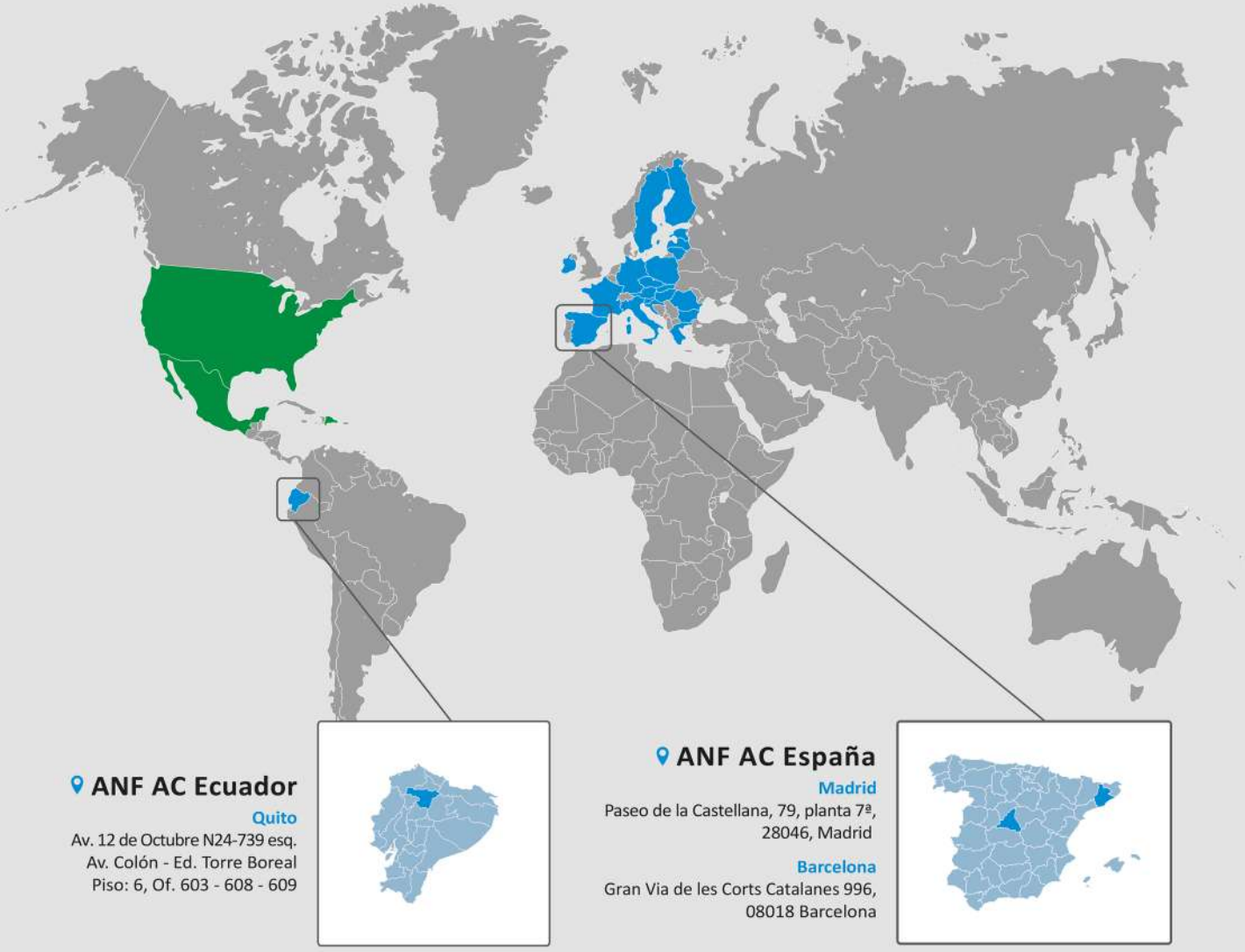
- The private keys of CA, CAi, TSU, and centralized end-user certificates are generated and kept in a secure cryptographic device (HSM) certified as qualified electronic signature devices (QSCD). They meet the requirements detailed in FIPS PUB 140-2 level 3 or higher, or with an EAL level 4+ or higher in accordance with ISO / IEC 15408.
- The QSCD SmartCards supplied to end users are certified and meet the requirements detailed in FIPS PUB 140-2 level 3 or higher, or with an EAL level 4+ or higher in accordance with ISO / IEC 15408.

In the use of time stamps for low, medium or high level procedures of the National Security Scheme (ENS), the indications of the ICT Security Guide -CCN- STIC-807- will be followed.

Certifications of conformity published in,

https://www.anf.es/auditorias-de-conformidad/

Ámbito geográfico de interoperabilidad legal



ANF AC Ecuador

Quito
Av. 12 de Octubre N24-739 esq.
Av. Colón - Ed. Torre Boreal
Piso: 6, Of. 603 - 608 - 609

ANF AC España

Madrid
Paseo de la Castellana, 79, planta 7ª,
28046, Madrid

Barcelona
Gran Via de les Corts Catalanes 996,
08018 Barcelona

ANF AC acreditación gubernamental.

Acuerdo de reconocimiento mutuo internacional.

Datos de Contacto

ANF AC España

Teléfono: 93 266 16 14
Dpto. Cíal: info@anf.es
Dpto. SAT: soporte@anf.es

ANF AC Ecuador

Teléfono: +593 02 3826877
Dpto. Cíal: ecuador@anf.ac
Dpto. SAT: soporte.ec@anf.ac