ANF
AUTORIDAD DE
CERTIFICACIÓN
2021

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

STATEMENT PRODUCT DISCLOSURE

PDS (*Product Disclosure Statement)*

QUALIFIED CERTIFICATES

© 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:

inf o@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 certificates, types of certificates and validation procedures

The electronic certificates issued by ANF AC are qualified and are in compliance with 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 (eIDAS).

The Certificates of Secure Server SSL and SSL Administrative Electronic Office, comply with the eIDAS Regulation, the reference ETIS standards, and the CA / Browser Forum Guidelines for EV Certificates.

ANFAC is officially accredited for the issuance of all types of qualified certificates under the eIDAS requirements. Specifically:

Electronic signature certificate

- Physical person
- Legal representative of a legal entity Legal representative
- sole or joint administrator Legal representative of an entity
- without legal personality Public employee medium and
- high level
- Collegiate
- Attorney

Remote electronic signature

certificate SSL secure server certificate

- SSL DV
- SSL OV
- SSL EV
- SSL Administrative Electronic Headquarters medium and high level

Electronic Seal Certificates

- Electronic Seal
- AAPP Electronic Seal Certificate for medium and high level automated action (AAPP)

PSD2 Certificates

- QSealC
- QWAC

- **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

- **The validation of the validity status of the certificates issued by any of the ANF AC hierarchies can be verified through the online information and consultation service provided by ANF AC, using the OCSP protocol (according to RFC 6960), available at the location of the OCSP responder on the certificate itself. Or, through the verification page published in**

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

At the request of the subscriber, the certificates can be issued under a pseudonym.

What's more, **Subscribers may request the inclusion in the certificate of other information of interest to them.** In that case, **in accordance with Art. 7.5 of Law 6/2020, of November 11,** regulating certain aspects of electronic trust services, when the qualified certificate contains other personal circumstances, such as their status as the holder of a public position, their membership in a professional association or their degree, **these should be checked through the official documents that certify them, in accordance with specific regulations.**

In the same way, when the subscriber wishes to include a representation capacity that has been granted by a third party, either a representation mandate or legal power, **the subscriber shall prove such condition by original document.**

Specific requirements for certificates of Public Administrations and public employees

The use of public employee and public employee certificates with a pseudonym for uses other than those established is not allowed. **in Law 40/2015, of October 1,** of the Legal Regime of the Public Sector. **In particular, in the case of certificates under a pseudonym, the provisions of article 43.2 will be taken into account.**

In the use of qualified certificates for low, medium or high level procedures of the National Security Scheme (ENS), s**e will follow the indications in the Guide to ICT Security -CCN-STIC-807-.**

In the case of Electronic Seal certificates for automated action, the requirements established in article **41.2 of Law 40/2015.**

Certificate usage limits

Certificates are issued subject to their respective Certification Policy (PC) and to the **Certification Practices Statement (CPS) of ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1,** documents detailing the limits of use.

PC Electronic signature certificate

OID 1.3.6.1.4.1.18332.3.1.

PC Electronic signature certificate
from distance

OID 1.3.6.1.4.1.18332.3.1.

PC SSL secure server certificate

OID 1.3.6.1.4.1.18332.55.1.1

PC Electronic Seal Certificates

OID 1.3.6.1.4.1.18332.25.1.1

PC Certificates PSD2 - QSealC

OID 1.3.6.1.4.1.18332.25.1.1

PC Certificates PSD2 - QWAC

OID 1.3.6.1.4.1.18332.55.1.1

The validity period, renewal and revocation procedure are detailed in each PC.
In general, it should be noted that the certificate will be used by the subscriber in the relationships they maintain with third parties they trust, in accordance with the authorized uses in the fields **'Key Usage' and 'ExtendedKeyUsage'** of the certificate and in accordance with the limitation of liability which consists in **the OID 1.3.6.1.4.1.18332.41.1 and / or in QcLimitValue OID 0.4.0.1862.1.2.**

Appropriate Uses of Qualified Certificates

The qualified electronic signature certificate guarantees the identity of the subscriber and the holder of the private signature key. With the intervention of secure signature creation devices, they are ideal to offer support to the qualified electronic signature that, in accordance with Law 6/2020, of November 11, regulating certain aspects of electronic trust services, and with the eIDAS, is equated to the handwritten signature for legal effect, without the need to meet any additional requirement.

These certificates can also be used, if so defined in the corresponding certificate type, to sign authentication messages, in particular SSL or TLS client challenges, S / MIME secure email, encryption without key recovery, or others. This digital signature has the effect of guaranteeing the identity of the subscriber of the signing certificate.

The Qualified Electronic Seal Certificate (QSealC), bind the validation data of a stamp with a legal person and confirm the name of that person. They allow the generation of electronic stamps, which serve as proof that an electronic document has been issued by a legal person, providing certainty about the origin and integrity of the document. ANF AC electronic seal certificates meet the requirements of annex III of eIDAS to be considered qualified.

Qualified SSL Secure Server Authentication Certificate (QWAC), allows to authenticate a website and link the website with the natural or legal person to whom the certificate has been issued. This certificate meets the requirements of annex IV of eIDAS to be considered qualified and the Guidelines for EV Certificates of the CA / Browser Forum.

The qualified certificate of Electronic Seal and Administrative Electronic Headquarters (QsealC), I know Issues for the identification of the administrative headquarters and the electronic sealing of documents. **The Electronic Headquarters certificates in the field of public administration, as established in Law 39/2015, of October 1, on the Common Administrative Procedure of the Administrations** Public.

In the case of centralized certificates to sign electronically (non-repudiation and commitment to what is signed), to carry out identification and authentication processes before computer systems.

Authentication of the applicant's identity

ANF AC only admits application for certificate issuance processed by a natural person of legal age, with full legal capacity to act.

The subscriber must fill in the Certificate Request Form assuming responsibility for the veracity of the information outlined, and process it before ANF AC using any of the following means:

TO

PRESENTIALLY

The subscriber may appear before an ANF AC OVP Operator, in whose presence they will proceed to sign the application form that must be duly completed.

B

BY ORDINARY MAIL

Certificate request form handwritten by the subscriber and legitimized by a Notary Public signature. Documentation sent by ordinary mail.

C

TELEMATICALLY

Identifying yourself, completing the electronic certificate request form and authenticating the documents in accordance with those established in the Certification Policy.

The fiscal identifiers of the subscriber will be incorporated into the certificate. In addition, the subscriber must provide a mobile phone number and an email address that they trust.

L**The email address and the SMS or WhatsApp service associated with your mobile phone will be considered authorized mailboxes so that ANF AC can deliver certified electronics,** even double authentication in the case of centralized electronic signature certificate service, or any other that is deemed necessary. The user assumes the obligation to inform ANF AC of any change in email address or mobile phone number.

Authentication of the identity of an organization and domain

ANF AC is based on the specifications of the Implementing Regulation (EU) 2015/1502 of the Commission of September 8, 2015 on the establishment of specifications and minimum technical procedures for the security levels of electronic identification means in accordance with the provisions of Article 8, paragraph 3, of Regulation (EU) No 910/2014 of the Parliament Council and European Council, on electronic identification and trust services for electronic transactions in the internal market.

Each Certification Policy establishes the procedure for authenticating the identity of a legal person, determining the following aspects in general:

- Types of valid documents for identification.
- Identification procedure to be carried out by the
- ARR. Need or not for face-to-face identification.

• How to prove membership in a specific organization and sufficient legal powers of representation.

The Secure Server SSL Certificate Certification Policy OID 1.3.6.1.4.1.18332.55.1.1, details the procedure followed in the authentication process of a Domain.

Obligations and responsibilities of the subscriber 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** The obligations of the subscribers, those responsible for use and the third parties who trust are defined.

In particular, the subscriber and the third parties who trust before placing their trust in the certificates, have the obligation to verify the validity of the certificate, having to use a qualified validation system of electronic signatures and seals that has verification of integrity and validity of qualified certificates.

Obligations of the CA, AR, OVP, and their responsibilities

In sections **9.6.1, 9.6.2, 9.9.1** Y **9.9.4** of the ANF Certification Practice Statement **AC OID 1.3.6.1.4.1.18332.1.9.1.1** The obligations and responsibilities of the CA and the RA are defined.

> **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,

CA liability limitations

In section 9.8 of the Certification Practices Statement**ANFACOID1.3.6.1.4.1.18332.1.9.1.1** ANF AC's liability limitations are defined.

Especially,

Limitation of liability with the subscriber

- **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 made by its subscribers through the use of their certificates.
- **ANF AC** does not assume responsibility when the holder makes use of the certificates using instruments that are not approved by ANF AC.
- **ANF AC** It 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 to certificate holders, their legal representatives and / or their certificate managers.

Limitation of liability with the trusting third party

- **ANF AC** does not assume responsibility when the trusting third party does not assume its obligation to verify the status of the certificate, using the verification instruments of ANF AC.
- **ANF AC** It 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 to third parties that trust.

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 provisions of the eIDAS Regulation and Law 6/2020, of November 11, regulating certain aspects of electronic trust services.

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

The Certificates issued with the qualification 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.**Yes no amount is set, it should be interpreted that the CA does not assume the use of that certificate for transactions that involve any financial risk, and therefore the compensation limit is zero.

Method to prove possession of the private key

In the PKI of ANF AC the keys are always generated by the certificate subscriber himself, which determines the signature activation data independently and without third party intervention.

Possession of the private key, corresponding to the public key for which the certificate is requested to be generated, it will be proven by sending the certificate request (–Certificate Signing Request-CSR) according to the RSA PKCS # 10 standard, in which the signed public key will be included using the associated private key.

This certificate request is sent to ANF AC for processing, what makes possible the detection of errors in the generation of the certificate and proof that the subscriber already has the key pair in his possession, and has the ability to make use of them.

> **This certificate request is sent to ANF AC for processing, which enables the detection of errors in the generation of the certificate and proves that the subscriber already has the pair of keys in his possession, and has the ability to make use of them.**

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 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 Data Protection Delegate,**

✉ 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

ANF AC guarantees the correct operation of the instruments it supplies, what These work according to the characteristics that are required of it. **The subscriber You have 7 calendar days to verify the certificate, the software and the cryptographic device.**

- In the event of malfunctions due to technical causes (among others: malfunction of the certificate support, program compatibility problems, technical error in the certificate, etc.) or due to errors in the data contained in the certificate, **ANF AC will revoke the certificate issued and will proceed to issue a new one within a maximum period of 72 hours.**

- The acceptance of the certificate is formalized by the subscriber with the ratification of the Subscription Contract, as stated in the section **4.1 of the CPS of ANF AC.** What's more, **ANF AC may request the improvement of the acceptance of the certificate** requiring the subscriber to sign a Certificate of Receipt and Acceptance of the Certificate. This requirement must be met by the subscriber within a maximum period of 15 days.

  After this term has elapsed without the subscriber having attended the request, ANF AC may proceed to revoke the certificate.

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:** “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers ”
- **ETSI EN 319 411** "Part 1: General Requirements"
- **ETSI EN319411** "Part 2: Requirements for Trust Service- Providers issuing EUQualifiedCertificates"
- **ETSI EN 319 412** "Electronic Signatures and Infrastructures (ESI): Certificate Profiles"
- **ETF RFC 3739** "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile"
- **IETF RFC 3628:** "Policy Requirements for Time-Stamping Authorities (TSAs)"
- **IETF RFC 3161:** "Internet X.509 Public Key Infrastructure Time-stamp Protocol"
- **ETSI TS 119 312:** “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites "

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,

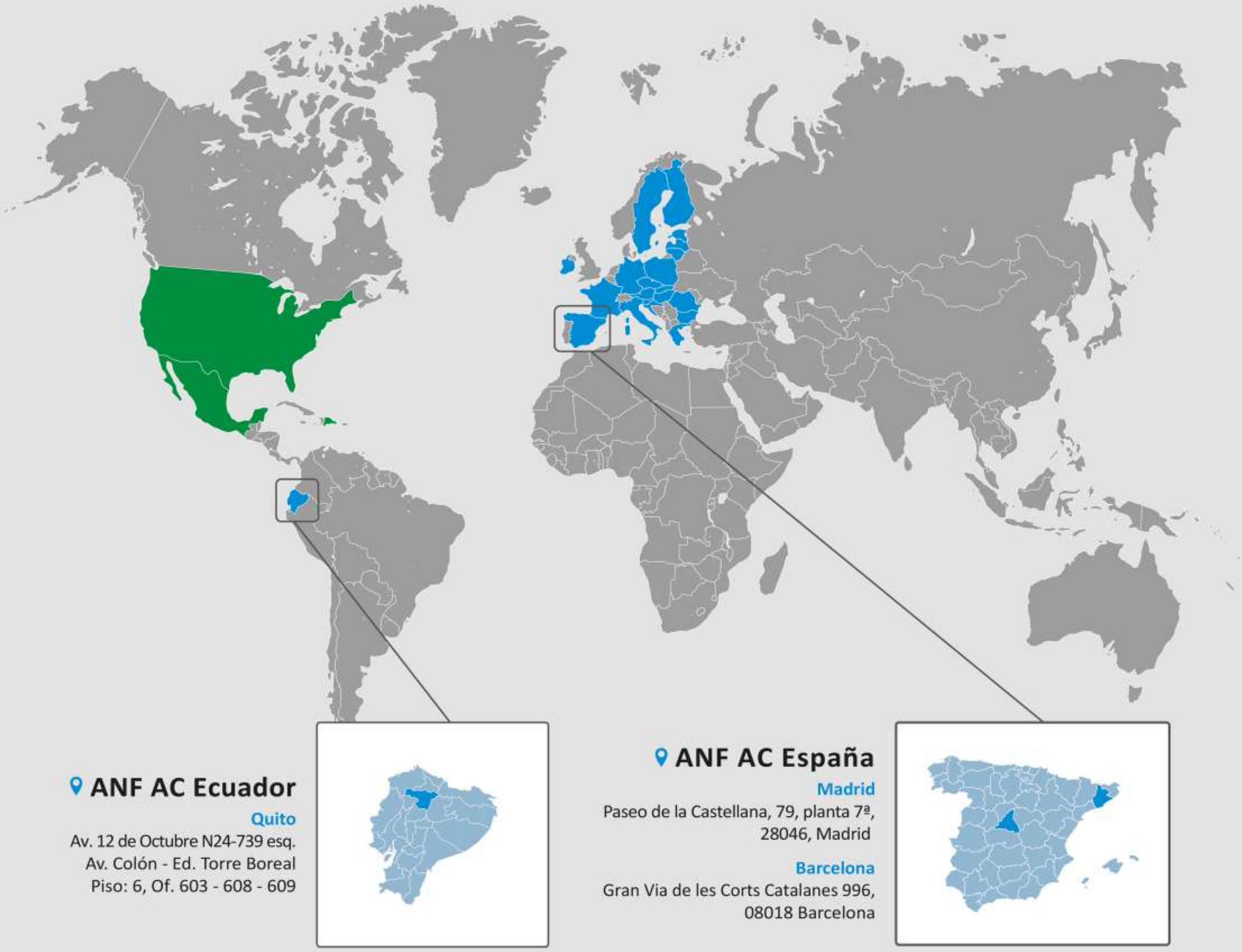
- The private keys of CA, CAi, TSU, and centralized end-user certificates are generated and kept in a secure cryptographic device (HSM) certified as qualified electronic signature devices (QSCD). They meet the requirements detailed in FIPS PUB 140-2 level 3 or higher, or with an EAL level 4+ or higher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

www.anf.es