ANF
AUTORIDAD DE
CERTIFICACIÓN
2021

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

STATEMENT PRODUCT DISCLOSURE

PDS (*Product Disclosure Statement)*

QUALIFIED VALIDATION

© 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 validation services for electronic signatures and stamps

ANF AC is the Qualified Provider of the Electronic Signature and Stamp Validation Service (QSVSP) and provides this qualified validation service (QSVS).

ANF AC's signature and electronic stamp validation services are qualified and, respectively, **comply with articles 32 and 40 of 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).

This service verifies that the documents submitted for validation meet the requirements of the eIDAS Regulation and standards in the matter, using operating procedures and information security management procedures that exclude any probability of data manipulation:

- Check the validity of **QES / AES and QEseal / AESeal.**
- **Valid qualified certificates:** verifying qualification, integrity, authenticity and validity.
- **Valid qualified electronic time stamps:** verifying qualification, integrity, authenticity and validity.

Validation reports are issued in PDF and XML format, and they are electronically sealed by ANF AC.

- **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

Supported Validation Service Policy (s)

The QSVS works on the basis of a validation policy of signatures as input, that is, the validation of signatures / stamps, is always performed against a validation policy.

The validation policies supported and whose requirements are used to perform the process are:

ANF AC Validation Policy	OID 1.3.6.1.4.1.18332.56.1.1
Conforms to the ETSI TS 119 441 validation criteria	OID 0.4.0.19441.1.1
Conforms to the ETSI TS 119 441 qualified validation criteria	OID 0.4.0.19441.1.2

- **This Validation Policy of ANF AC permanently updated and published in,**

https://www.anf.es

The validation report specifies the key and level of the validated electronic signature / seal.

Parties involved

1

QUALIFIED PROVIDER OF VALIDATION SERVICES (QSVSP).

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

tw

SUBSCRIBER.

It is the responsibility of the client who hires the validation service and submits signatures and / or electronic seals to validation.

3

USERNAME.

Application or human interacting with a signature validation client.

4

THIRD WHO TRUST.

Third parties that without being the subscriber or the user, are authorized to access the qualified validation reports and trust them.

Signature commitments

In accordance with ETSI TS 119 172-1, the possible inclusion of signature commitments will be taken into account and will be recorded in the validation report.

Specifically, the accepted signature commitments (may include one or more) are:

- **OID 1.2.840.113549.1.9.16.6.1 -**The signature is intended for data authentication purposes only. Indicates that the signer acknowledges having created, approved and sent the signed data, the URI of this commitment ishttp://uri.etsi.org/01903/v1.2.2#ProofOfReceipt.

- **OID 1.2.840.113549.1.9.16.6.2 - As acknowledgment of receipt.** Indicates that the signer acknowledges have received the content of the signed data; the URI of this commitment ishttp: // uri. etsi.org/01903/v1.2.2#ProofOfReceipt.

- **OID1.2.840.113549.1.9.16.6.3 -Cor proof of delivery.** Indicates that the TSP providing that indication has delivered the signed data in a mailbox accessible to the recipient of the signed data. The URI of this commitment ishttp://uri.etsi.org/01903/v1.2.2#ProofOfDelivery.

- **OID1.2.840.113549.1.9.16.6.4 -Sender's proof.** Indicates that the entity that provides that indication has sent the signed data (but didn't necessarily create it). The URI of this commitment ishttp://uri.etsi.org/01903/v1.2.2#ProofOfSender.

- **OID 1.2.840.113549.1.9.16.6.5 - Approval test.** Indicates that the signer has approved the content of the signed data. The URI of this commitment ishttp://uri.etsi.org/01903/ v1.2.2 # ProofOfApproval.

- **OID 1.2.840.113549.1.9.16.6.6 - Creation test.** Indicates that the signer has created the data signed (but not necessarily approved, nor sent that); the URI of this commitment ishttp://uri.etsi.org/01903/v1.2.2#ProofOfCreation.

ANF AC, in accordance with the provisions of Annex B of ETSI TS 119 172-1, has created the following proprietary OIDs:

- **OID 1.3.6.1.4.1.18332.27.1.9 - Use of the signature as a credential in an access control.** The signature is intended solely for the authentication of entities in order to leave evidence of the access request made by the signer.

- **OID 1.3.6.1.4.1.18332.27.1.12 - Intermediate authorization.** The signature is intended only as an intermediate approval as part of a decision process.

- **OID 1.3.6.1.4.1.18332.27.1.14 - Seen, reading mark.** The signature is intended solely to indicate having reviewed a document.

- **OID 1.3.6.1.4.1.18332.27.1.15 - Intervention in the legal certification of a document original.** The signature is intended solely to certify that the signer guarantees that the signed document is an authentic copy that fully corresponds to an original.

- **OID 1.3.6.1.4.1.18332.27.1.16 - Intervention as a witness.** Indicates that the signature is intended solely to indicate having witnessed the signature of another person on the same document (signed data) which has read the document in its entirety, and has signed it as proof of their compliance with them.

- **OID 1.3.6.1.4.1.18332.27.1.1 - Full legal effects according to OID Signature Policy 1.3.6.1.4.1.18332.27.1.1.** Indicates that the signature is intended to be used in a legal and contractual framework, in which it is desired to prove with probative force and full legal validity, that the signer agrees, except in those matters in which a mention or exception has been made. , or commitment to the agreements and conditions that are implicitly or explicitly outlined in the signed data.

  The electronic signatures generated within the scope of this Electronic Signature Policy, can be used to subscribe all types of electronic documents, in accordance with the use limitations established by current legislation, and the restrictions derived from the Certification Policy to which it is submitted the electronic certificate used in its creation.

TSP validation

QSVS manages a repository with the Trusted Lists (TSL) published by each of the member countries of the Union and versioning control.

Before use, it is verified that the version to be used is the latest version published.

The interpretation of the TSL is carried out in accordance with the provisions of ETSI TS 119 612.

OCSP service

The SVSServ proceeds to verify the validity status of the certificates used in the elaboration of the electronic signature / seal by means of OCSP consultation. The OCSP response is required to comply with IETF RFC 6960, X.509, Internet Public Key Infrastructure Online Certificate Status Protocol –OCSP.

OCSP Responders must attend inquiries in real time, directly on the repositories of the issuing entity of the certificates used, either in the elaboration of the signature, issuance of a time stamp, or electronic time stamp.

OCSP responses are electronically signed by the QTSP. The The validation process includes the certificate submitted for consultation and the entire chain of the Certification Hierarchy up to the first level (excluding Root CA).

Signature validation report

The validation report includes information on ANF AC in accordance with ETSI TS 119 612 Section 5.5.2, and on the application used.

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 collected in the **OID Validation Policy 1.3.6.1.4.1.18332.56.1.1.**

ANF AUTORIDAD DE CERTIFICACIÓN

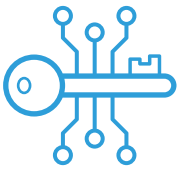
Signature validation report

Status indication	Semantics	Validation report data
TOTAL-CONFIRMED	**The QES / QESeal validation process has a TOTAL-CONFIRMED:** • QES / QESeal cryptographic checks have been successful (including hash checking of the QES / QESeal different data objects, indirectly signed). • The certification of the identity of the signer has been positively validated (that is, the signature certificate is valid). • Successfully validated QES / QESeal.	The validation process confirms that the certification chain is validated, including **the certificate for QES / QESeal,** used in the validation process together with a **specific signed / stamped attribute (if it exists),** which is considered as a validation test.
TOTAL-FAILURE	**The QES / QESeal validation process has a FULL-FAIL result because the cryptographic checks of the QES / QESeal.** They are unsuccessful (including the Hashes controls of the different data objects, Indirectly signed / sealed) or it has been shown that the generation of the Signature / seal has occurred after Revocation / in QC suspension time.	**The validation process explains the cause of issuing a TOTAL-FAILURE report** in order to each of the elements that are taken into account and that have given negative results.
INDETERMINATE	The information available is not enough to carry out the validation process and determine the status indication **by QES / QESeal: AWAY- CONFIRMED or AWAY FAILURE.**	The validation process provides information in order to explain the cause that gives as **result "indeterminate",** and help to determine the missing data to complete the validation process.

Certificate validation limitations

Restrictions for the validation of X.509 certificates apply in the certification chain verification process according to **ETSI TS 119 172-1, clause A.4.2.1.**

Cryptographic limitations



Cryptographic restrictions on algorithms and parameters used in QES / QESeal creation apply, **as indicated in ETSI TS 119 172-1, clause A.4.2.1.**

Limitations of the elements of the signature

Restrictions apply regarding QES / QESeal items that indicate DTBS (Data To Be Signed) requirements, **according to ETSI TS 119 172-1, clause A.4.2.1.**

Limitations of formats and levels supported by QES / AES and QEseal / AESeal

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

and levels:

QES / AES and QEseal / AESeal restrictions supported

Signature / stamp position and signed data object	Value
Covering QES / QESeal - the signature / stamp covers the data object	✓
Covered (type "letter") QES / QESeal - The signed data object covers the signature / stamp	✓
Separate QES / QESeal - Signature / stamp and data object are separate (independent)	✓
Simultaneously, positions were repeatedly compared A	✓
document has more than one QES / AES and QEseal / AESeal	✓

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** 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 qualified validation certificates, have the obligation to verify the validity of the electronic seal with which ANF AC authenticates it, having to use a qualified validation system of qualified electronic signature and seals.**

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

CA liability limitations

In section 9.8 of the Declaration of **ANF Certification Practices 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 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

- **ANF 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 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

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 humanreadable 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 "

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.

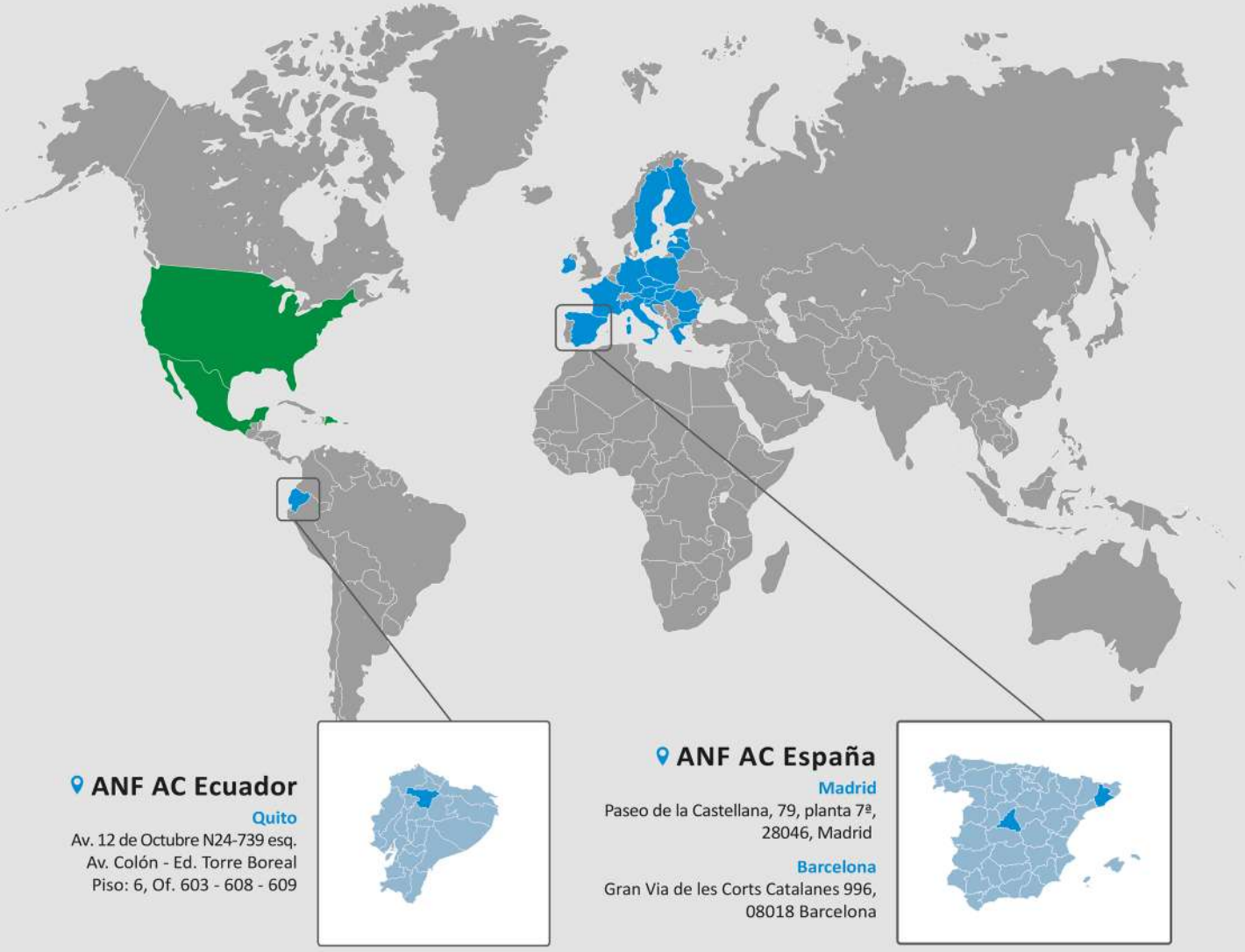
• The QSCD SmartCards supplied to end users are certified and meet the requirements detailed in FIPS PUB 140-2 level 3 or higher, or with an EAL level 4+ or higher in accordance with ISO / IEC 15408.

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