Certificacion Policy for Electronic Seal and Public Administration Electronic Seal Certificates

Paseo de la Castellana, 79 - 28046 – Madrid

Teléfono: 902 902 172 (Llamadas desde España)

Internacional (+34) 933935 946

Fax: +34 933 031 611 · Web: www.anf.es

Security Level

Public

Important Notice

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

Telephone: 902 902 172 (Calls from Spain) International (+34) 933 935 946

Fax: (+34) 933 031 611. Web: www.anf.es

Index

1 Introduction

ANF Autoridad de Certificación (hereinafter, ANF AC) is a legal entity, incorporated under Organic Law 1/2002 of March 22nd, and registered in the Ministry of the Interior with national number 171.443 and VAT number G-63287510.

The Public Key Infrastructure (PKI) of ANF AC has been designed and is managed in accordance with the legal framework of the European Parliament [UE] 910/2014 Regulation, and with the Law 59/2003 on Electronic Signature of Spain. The PKI of ANF AC complies with the ETSI EN 319 411-2 (Part 2: Requirements for Trust Service Providers issuing EU Qualified Certificates), ETSI EN 319 411-3 (Part 3: Policy Requirements for Certification Authorities issuing public key certificates), ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI) and RFC 3739 *(Internet X.509 Public Key Infrastructure: Qualified Certificate Profile)* standards.

ANF AC uses OIDs in accordance with the ITU-T Rec. X.660 and the ISO/IEC 9834-1:2005 (*Procedures for the Operation of OSI Registration Authorities: General Procedures and ASN.1 Object Identifier tree top arcs*) standards. ANF AC has been assigned the SMI Network Management Private Enterprise Code 18332 by the international organization IANA - Internet Assigned Numbers Authority - under the branch iso.org.dod.internet.private.enterprise (*1.3.6.1.4.1 -IANA –Registered Private Enterprise-*).

This document is the Certification Policy (CP) corresponding to the certificates issued by ANF AC, of the type "Electronic Seal" and "Public Administration Seal". These certificates are issued with the consideration of qualified in accordance with the provisions of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and with consideration of recognized as defined in Law 59/2003 of electronic signature.

To develop its content the IETF RFC 3647 PKIX structure has been followed, including those sections that are specific to this type of certificate.

This document defines the operational and procedural requirements to which the usage of these certificates is subjected, and defines the guidelines that ANF AC uses for its issuance, management, revocation, renewal and any other process that affects the life cycle. The roles, responsibilities and relationships between the end user, ANF AC and trusted third parties are described, as well as the application, renewal and revocation rules that must be met.

This document is only one of the several documents governing the PKI of ANF AC, it details and supplements the definitions in the Certification Practice Statement and its addendum. ANF AC oversees and supervises that this CP is compatible and consistent with the other documents produced. All documentation is freely available to users and relying parties at www.anf.es/en.

This Certification Policy assumes that the reader knows and understands the PKI, certificate and electronic signature concepts. If this is not the case, the reader is recommended to be educated in these concepts before continuing the reading of this document.

1.1 Description of Certificates

These certificates per EU Regulation 910/2014 (eIDAS), are an electronic statement that links the seal validation data, created by a legal person, with that legal person and confirms the name of that person.

The certificate identifies the natural person representative of the legal person and credits his powers of attorney over the legal person represented, and includes information on the same, in whose name it acts. Whereas 65 of eIDAS states the following:

"In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers."

ANF AC, in the framework of its Digital Certification Service, issues certificates of identity such as:

- **Electronic Seal Certificate**

Electronic certification issued by ANF AC that links its holder to signature verification data and confirms its identity.

Its use is intended in computer applications automatically running electronic signatures processes, and in data encryption before services and applications.

- **Public Administration Electronic Seal**

Electronic certification issued by ANF AC that links its holder to a Signature verification data and confirms its identity.

ANF AC issues these certificates with the requirements defined by the electronic signature law, and in accordance with of articles 17 and 18 of Law 11/2007, of June 22nd, on electronic access of citizens to public services. They are in accordance with the requirements stated in the Royal Decree 1671/2009, of November 6th, and the profiles and policies published by the Higher Council of Electronic Administration.

These certificates allow the identification of the electronic office of public administrations, bodies or entities, and authentication of the exercise of its jurisdiction in the automated administrative action.

These certificates can be issued in two support formats:

- Cryptographic software Token.
- HSM (hardware security module) Token. Certified with ISO 15408 Common Criteria EAL 4+ or higher.

This policy, regarding certificates of the type "Public Administration Electronic Seal", follows the definitions set by the Information and Communications Technologies Department (DTIC) in its document "Electronic certificates profiles " of April 2016.

a. Medium level:

This level corresponds to a configuration of security mechanisms suitable for most applications.

The expected risk by this level is appropriate to access applications classified by ENS in the levels of Integrity and Authenticity as low or medium risk.

Also, the expected risk in this level corresponds to the low and substantial security levels of the electronic identification systems of the Regulation (EU) 910/2014. Safety levels of the eIDAS regulation apply only to electronic identification systems.

Minimum acceptable security mechanisms include X.509 software certificates. In the case of certificates issued to natural persons, they correspond to a "qualified certificate" as defined in Regulation (EU) 910/2014, for qualified electronic signature without a qualified signature creation device. In the case of certificates issued to legal persons, it corresponds to a "qualified seal certificate", as defined in the Regulation (EU) 910/2014 for qualified electronic seal without a qualified seal creation device. The use of signature hardware devices (HSM or qualified signature creation device) is also permitted.

The maximum validity of these certificates is 5 years.

The expected risk for this level corresponds to the guarantee level 3 provided in the IDABC Authentication Basic Policy *[1].

**1 The IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens) program. Decision of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC) [Official Journal L 144 of 30 April 2004].*

b. High level:

This level corresponds to a configuration of security mechanisms suitable for applications that require additional measures, per the risk analysis performed.

The expected risk for this level is appropriate to access classified applications per the ENS in the levels of Integrity and Authenticity as high risk.

Also, the expected risk in this level corresponds to the high security level of electronic identification systems of the Regulation (EU) 910/2014. Safety levels of the eIDAS regulation apply only to the electronic identification systems.

Acceptable security mechanisms include X.509 certificates in hardware. In the case of certificates issued to natural persons, they correspond to a "qualified certificate", for "qualified electronic signature", as defined in the Regulation (EU) 910/2014. In the case of certificates issued to legal persons, it corresponds with the "qualified seal", as defined in the Regulation (EU) 910/2014.

The expected risk for this level corresponds to guarantee level 4 provided in IDABC Authentication Basic Policy.

The maximum validity of these certificates is 5 years.

1.2 Identification

Document name	Certification Policy for Electronic Seal and Public Administration Electronic Seal Certificates
Version	1.6
Policy state	APPROVED
Document reference / OID	1.3.6.1.4.1.18332.25.1.1
Date of issue	November 7th, 2016

Expiration date	Not applicable
Related DPC	Certification Practices Statement (CPS) of ANF AC
Localization	https://www.anf.es/en

To identify the certificates, ANF AC has assigned the following object identifiers (OID).

CERTIFICATE	OID
Electronic Seal Certificate With SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18332.25.1.1.
High Level Public Administration Electronic Seal Medium Level with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18332.25.1.1.2.
Medium Level Public Administration Electronic Seal High Level with SHA-256 algorithm and 2048 bits length	1.3.6.1.4.1.18332.25.1.1.3.

In the case of "High Level Public Administration Certificate", the extension CertificatePolicies (2.5.29.32) will include the OID:

- 2.16.724.1.3.5.6.1

In the case of "Medium Level Public Administration Certificate", the extension CertificatePolicies (2.5.29.32) will include the OID:

- 2.16.724.1.3.5.6.2

When the certificate is issued with the qualification of qualified, in the extension CertificatePolicies (2.5.29.32), will include at least one of the following PolicyInformation:

- qcp-legal (0.4.0.194112.1.0). Certificate in token software
- qcp-legal-qscd (0.4.0.194112.1.2). When the qualified signature certificate, is stored in a qualified device per Regulation UE 910/2014.

1.3 Users community

1.3.1 Certification Authorities

As defined in the Certification Practice Statement (CPS) of ANF AC. These are the entities which issue electronic certificates which link a public key with the subscriber identity. They act as a trusted third party between the subscriber and relying parties.

1.3.2 Registration Authorities

These are entities that perform registration procedures of applicants for end entity certificates. They perform the identification and authentication of individuals involved in the application, and they can initiate or assist in the procedures for revocation and renewal of certificates.

These entities may belong to the organization of the certification entity, or may be external partners, in which case ANF AC defines two types:

1.3.2.1 Recognized Registration Authority

As defined in the CPS of ANF AC.

1.3.2.2 Collaborating Registration Authority

As defined in the CPS of ANF AC.

1.3.3 Issuance Reports Manager

As defined in the CPS of ANF AC.

1.3.4 End entities

1.3.4.1 Certificate subscriber

It is the certificate holder. It offers services through an application executed in a computer system that is identified by the department name, address or Internet domain, and is linked to the certificate holder. Depending on the type of certificate:

1.3.4.1.1 Electronic Seal

It is a legal person, which subscribes to the terms and conditions of a certificate, and whose identity is linked to the signature verification data (public key) of the certificate issued by ANF AC. Therefore, the identity of the certificate holder is linked to the electronically signed by the signer, using the signature creation data (private key) linked to the certificate issued by ANF AC.

1.3.4.1.2 Public Administration Electronic Seal

It is a public administration, body or an entity, which subscribes to the terms and conditions of a certificate, and which identity, and where appropriate, its electronic office, is linked to the signature verification data (public key) of the certificate issued by ANF AC. Therefore, the identity of the certificate holder is linked to the electronically signed by the signer, using the signature creation data (private Key) linked to the certificate issued by ANF AC.

1.3.4.2 Certificate applicant

It is the Legal Representative of the certificate holder and acting on behalf of such holder.

The certificate must be requested by natural person of legal age, or an emancipated minor, with legal capacity to assume the legal representation of the legal person or entity without legal personality associated to the certificate requested.

The applicant is responsible for the custody of the signature creation data associated with the electronic certificate or, where appropriate, of the access means to them. Its identity will be included in the certificate.

In accordance with the provisions of article 6 paragraph 2 of Law 59/2003 of 19 December, on electronic signature (per Final Provision 4.2 of Law 25/2015, of July 28th):

> *"the signer is the person who possess a signature creation device and acts on its own behalf or on behalf of a natural or legal person who he represents."*

1.3.4.3 Certificate responsible

The certificate responsible must have express authorization from the applicant, and his/her identity shall be included in the certificate.

The certificate responsible must be a natural person of legal age with full legal capacity to act and must provide its consent for assuming this responsibility.

The certificate responsible holds the signature creation device and is responsible for its use and custody. His/her identity shall be included in the certificate as legal representative and in accordance with the article 6 of the Law 59/2003:

> *"the signer is the person who owns a signature creation device and acts on its own behalf or on behalf of a natural or legal person who represents."*

1.3.4.4 Relying third parties

As defined in the CPS of ANF AC.

1.4 Certificates usage

1.4.1 Allowed usage

The electronic seal certificate, per the eIDAS regulation, can have three uses:

> (1) "documents sealing" *(key usage will have the bit "ContentComitment"),*
> (2) "code sealing" (*keyusage will have the bit "digitalSignature" combined with the extendedkeyusage ("codeSigning"),* and
> (3) "legal person asset authentication certificate" (acting as component certificate for example for authentication on applications servers) (*keyusage will have the bit "digitalSignature" combined with the keyEncipherment (or KeyAgreement) and with extendedkeyusage ("serverAuth", "clientAuth").*

This certificate should never be used exclusively for encryption, nor as web server authentication certificate.

1.4.2 Limits of certificate usage

The subscriber can only use the private key and the certificate for uses authorized on this CP and restricted to the application or department that appears on the certificate.

Its use and acceptance must follow the usage limitations stated in the certificate, assuming the limitation of liability contained in the OID 1.3.6.1.4.1.18332.40.1. and / or in QcLimitValue OID 0.4.0.1862.1.2. Similarly, the holder may only use the key pair and the certificate after accepting the conditions of use established in the CPS.

The subscriber may only use the key pair and the certificate after accepting the conditions of use established in the CPS.

1.4.3 Prohibited usage

As defined in the CPS of ANF AC.

1.5 Certification entity contact details

As defined in the CPS of ANF AC.

1.6 Definitions and acronyms

As defined in the CPS of ANF AC.

2 Information Publication and Repositories

2.1 Repositories

As defined in the CPS of ANF AC.

2.2 Information publication

As defined in the CPS of ANF AC.

2.3 Frequency of Updates

As defined in the CPS of ANF AC.

2.4 Access controls to repositories

As defined in the CPS of ANF AC.

3 Identification and Authentication

3.1 Name registration

3.1.1 Types of names

The CN (CommonName) attribute must refer to the name of the application or department that uses it. In case of electronic seal certificates, due to compatibility reasons, it is possible the inclusion in the CommonName of the Subject certain attributes that may be necessary for treatment, such as the name of the entity subscriber or responsible for the seal, and its VAT number.

In the electronic seal certificates, the company name is included in the attribute "organizationName" and the VAT number in the attribute "organizationIdentifier":

> *"Additional attributes other than those listed above may be present. In particular, when a natural person subject is associated with an organization, the subject attributes **may** also identify such organization using attributes such as **organizationName** and **organizationIdentifier**. Certificates may include one or more semantics identifiers as specified in ETSI EN 319 412-1 [i.4], clause 5 which defines the semantics for the organizationIdentifier attribute"*

Attributes	Content	Example
organizationName	Company name, as stated in the official records.	Company name. S.L.
organizationIdentifier	VAT number, as contained in the official records. Coded per the European ETSI EN 319 412-1 Standard	VATES-B0085974Z

3.1.2 Specific fields completion guide

Per RFC 5280, which uses UTF-8*[1] string, since it encodes international character sets including Latin alphabet characters with diacritics ("Ñ", "ñ", "Ç", "ç", "Ü", "ü ", etc.). For example, the character (ñ), is represented in Unicode as 0x00F1.

For all literal variables:

- All literals are entered in capital letters, with the exceptions of the domain name/subdomain and email that will be in lowercase.
- Do not include accent marks in the alphabetic literals

- Do not include more than one space between alphanumeric strings.
- Do not include blank characters at the beginning or end of alphanumeric strings.
- The inclusion of abbreviations based on a simplification is admitted, provided they do not difficult the interpretation of information.

*1 *For more information see RFC 2279 improved in 3629 (UTF-8, a transformation format of ISO 10646)*

DNI/NIE

The term NIF covers both DNI and NIE.

If you opt for the DNI or NIE label, instead of NIF, the corresponding one will be used.

The following coding are allowed:

1.- Semantics proposed by the ETSI EN 319 412-1 standard. Consisting in:

- Three characters to indicate the type of document per the following coding:

- "PAS" for identification based on passport number.
- "IDC" for identification based on the number of national identity card (DNI/NIE).
- "PNO" for identification based on () national personal number (number of civic national register).
- "TAX" for identification based on a personal tax identification number issued by a national tax authority. This value is in disuse. The value "ID number" should be used instead. Tax Identification Number "TIN" per the European Commission - Taxation and Customs Union, specification published in:

  (Https://ec.europa.eu/taxation_customs/tin/tinByCountry.html).

- Two characters to identify the country. Encoded in accordance with "ISO 3166-1- alpha-2 code elements".

- Identity number with tax identification letter.

e.g.: IDCES-00000000G.

2.- Basic semantics. Consisting in:

The number and letter as contained in identity document.

e.g.: ID00000000G.

3.1.3 Anonymous or pseudonyms

In all cases the distinguished names must make sense.

3.1.4 Rules for interpreting various name formats

As defined in the CPS of ANF AC.

3.1.5 Uniqueness of names

As defined in the CPS of ANF AC.

3.1.6 Resolution of conflicts in relation to names and trademarks

ANF AC is not liable for the use of trademarks in the issuance of Certificates issued under this Certification Policy. ANF AC is not required to verify ownership or registration of trademarks and other distinctive signs.

Certificate applicants shall not include names in applications that may involve infringement.

The usage of distinctive signs whose right of use is not owned by the subscriber or duly authorized to do so is not allowed.

ANF AC reserves the right to refuse a certificate request because of name conflict.

3.2 Initial identity validation

3.2.1 Prove of possession of the private key

As defined in the CPS of ANF AC.

3.2.2 Authentication of the identity

Certificates issued under this Certification Policy will identify the subscriber under whose name the certificate is issued and the certificate applicant.

The Issuance Reports Manager will use appropriate means to ensure the accuracy of the information contained in the certificate. Among these means it is included external registry databases and the ability to require information or documents to the subscriber.

The tax identification of the applicant and subscriber will be incorporated into the certificate.

In accordance with art. 13.3 of Law 59/2003 on Electronic Signature, when the qualified certificate contains other personal circumstances or attributes of the applicant, such as its status as holder of a public office or membership of a professional association or qualification, this must be verified with official documents that prove it, in accordance with the applicable legislation.

The documentation type, processing forms, authentication and validation procedures are specified in the this document.

3.3 Re-key requests

In the event of re-keying, ANF AC shall previously inform the subscriber about any changes that may have occurred in the terms and conditions in relation to the previous issuance.

A new certificate may be issued maintaining the previous public key, if it is considered cryptographically secure.

3.4 Revocation request

All revocation requests must be authenticated. ANF AC verifies the applicant's ability to handle this requirement.

4 Operational Requirements

4.1 National Interoperability scheme and national security scheme.

4.1.1 Operations and management of the public key infrastructure

Operations and procedures performed for the implementation of this Certification Policy are made following the controls required by the standards recognized for such purpose, describing these actions in sections "Physical Security, Facilities, Management and Operational Controls" and "Technical Security Controls" of the Certification Practice Statement of ANF AC.

The Certification Practice Statement of ANF AC, responds to different sections of the ETSI EN 319 411-2 standard.

4.1.2 Interoperability

The certificates corresponding to this Certification Policy are issued by ANF AC in accordance with Resolution of November 29th, 2012, of the Secretariat of State for Public Administration, by which the Approval Agreement of the Electronic Signature Policy and of General State Administration Certificates is published, and its publication is announced in the corresponding electronic office, and specifically the profile of this type of certificates is in accordance with the profile approved by the Higher Council for Electronic Administration, at a meeting of the Permanent Commission, on May 30th, 2012 and published in Annex II of the mentioned Resolution

4.2 Certificate application

ANF AC only accepts certificate issuance requests processed by natural persons of natural age, with full legal capacity to act.

The applicant must complete the Application Form of the certificate undertaking responsibility for the accuracy of the information provided, and submitting it to ANF AC using any of the following means:

a) **Electronically**: On the website https://www.anf.es, the interested parties may access an application form that shall be filled and electronically signed with a qualified certificate, in accordance to the Law 59/2003, December 19th, on Electronic Signature. The certificate used must have been issued by a CA approved by ANF AC.

b) **In person**: the applicant may appear before a Recognized Registration Authority, in whose presence will proceed to sign the application form, which shall be dully fill out.

c) **By mail**: the applicant may submit the application form to the offices of ANF AC certificate, having duly completed and authenticated his signature before a Collaborating Registration Authority.

4.3 Processing procedure

4.3.1 Identity authentication

4.3.1.1 Applicant

When the application is done before a Recognized Registration Authority, the applicant must prove his/her identity and submit valid original or certified copies of the following documents:

a) Physical address and other contact details of the applicant. If deemed necessary by the Registration Authority or the Issuance Reports Manager, additional documents may be solicited to verify the reliability of the information, such as recent utility bills or bank statements. In case the RRA or the IRM know the applicant personally, they shall issue and sign a Declaration of Identity *[1].

b) The RRA, as proof of attendance and to preclude the repudiation of the procedure done, can get a set of biometric evidence: photography and/or fingerprints.

c) ID card or passport in case of national citizens, whose photograph allows verifying the identity of the person appearing. In case of low sharpness of the picture, another official document with picture may be requested (e.g. driver's license).

d) In case of foreign citizens, the following will be required:

I. To European Union members or European Economic Area members:

- National Identity Card (or local equivalent), or NIE (issued by the Registry of Citizen Members of the Union), or passport. The physical identification must be performed using as a reference one of this documents which includes a photograph of the person appearing before them. In case of low sharpness of the picture, another official document with picture may be requested (e.g. driver's license).

- Certificate issued by the Registry of Citizens of Members of the European Union.

II. To non-EU citizens:

- Passport, residence permit and work permit with photograph that allows comparing the identity of the person appearing. In case of low sharpness of the picture, another official document with picture may be requested (e.g. driver's license).

e) The representative must have sufficient powers of attorney.

f) In case the applicant requires to include other personal circumstances, these shall be verified with official documents in accordance with the applicable regulation.

The applicant may be waived of appearing before the Registration Authority in any of the following cases:

1. If the appropriate forms have been duly filled, and the signature of the subscriber has been legitimized before a notary, and certified copies of the identity, authorization and legal representation documents have been attached.

2. Online

   The https://www.anf.es website includes an application form that should be filled and electronically sign with a qualified certificate, per the Law 59/2003, of December 19th, on Electronic Signature. The certificate used must has been issued by a CA approved by ANF AC.

***1** *Declaration of Identity*

It consists of a formal declaration under oath, in which the declarant states he/she personally and directly knows and directly a natural person or a legal entity. Besides, it states, up to their direct knowledge, that he has verified the filiation data outlined in the Application Form are true: the address, telephone and e-mail. The Declaration of Identity incorporates the identity of the declarant, his ID card number, the data verified, the date and time of verification, the signature of the declarant and the appropriate legal warnings in case of perjury.

4.3.1.2 Certificate responsible

The same procedure will be followed as the one specified in the preceding paragraph "4.3.1.1 Applicant", with the particularity that, in this case, the required powers of attorney to the applicant will be replaced by the signing of the Authorization and Acceptance of Liability Minute included in this document. The minute shall be signed by the Legal Representative and the Certificate Responsible.

4.3.1.3 Certificate subscriber

The legal representative processing the application for a certificate, must submit original or certified copy of the following valid documentation:

1.- In any event:

- Physical Address and other contact details. If deemed necessary by the Registration Authority or the Issuance Reports Manager, additional documents may be solicited to verify the reliability of the information, such as recent utility bills or bank statements. In case the RRA or the IRM know the applicant personally, they shall issue and sign a Declaration of Identity.

- Tax identification card of the entity (VAT number).

2.- Per legal form:

- Trading companies and other legal persons which registration is required in the Mercantile Register, shall certify the valid incorporation by providing original or certified copy of the Mercantile Registry in relation to the incorporation data and valid director positions of the entity.

- The Associations, Foundations and Cooperatives shall certify their incorporation by providing original or certified copy of their incorporation certificate from the public registry where they

are registered.

- Civil and other legal entities, shall provide original or certified copy of the document that attest their incorporation irrefutably.

- Public Administrations and entities belonging to the public sector:

  - Entities which registration is mandatory in a Registry, they will certify their incorporation by providing original or certified copy of a certificate stating their incorporation data constitution and legal personality.

  - Entities created by a norm, shall provide the reference to such norm.

4.3.2 Approval or rejection of certificate applications

The Issuance Reports Manager (IRM) assumes the final responsibility of verifying the information contained in the Application Form, to assess the adequacy of the documents provided and of the application, in accordance with the provisions of this Certification Policy.

Moreover, he/she will determine:

- That the subscriber has had access to the terms and conditions relating to the use of the certificate, as well as to the issuance fees.

- That the subscriber has had access and has permanent access to all documents relating to the duties and responsibilities of the CA, the subscriber, applicant, those responsible for the certificate and relying parties, especially the CPS and Certification Policies.

- Shall monitor compliance with any requirement imposed by the legislation on data protection, as established in the security document included in the CPS, per the LOPD as provided in article 19.3 of the Spanish Law 59/2003, of December 19th, on Electronic Signature.

The process of issuing the certificate shall not begin if the Issuance Reports Manager has not issued the corresponding compliance report. The maximum period established for issuing the report is 15 days. After that period without issuing the mandatory report, the applicant may immediately cancel the order and be reimbursed of the fees paid.

The IRM may require additional information or documentation from the applicant, which will have 15 days to deliver it. After this period, without having completed the requirement, the IRM will issue a report denying the issuance. Should the applicant meet the requirement, the IRM will have 7 days to issue the final report.

In case the IRM verifies that the information provided by the applicant is not true, he/she will deny the issuance of the certificate, and will generate an incident report to the Security Manager, to determine whether to include the applicant in the blacklist of individuals and entities with OID 1.3.6.1.4.1.18332.56.2.1.

The validation procedure to be followed, depending on the type of certificate, is the following:

- The IRM shall verify the documentation provided by the applicant and the Registration Authority.

- The validation process will be supported by the Legal and Technical Departments, which will review and technically validate the PKCS#10 certificate request.

- In the process of verification of the information and documentation received, the following means may be used:
    - Consultation of official public registries in which the entity must be registered to verify existence valid management positions and other legal aspects such as activity and date of incorporation.
    - National or regional Official Gazettes of public bodies to which public bodies or companies belong to.

- It is verified that none of the natural or legal persons associated with the request appear in the blacklist of individuals and entities with OID 1.3.6.1.4.1.18332.56.2.1.

4.3.3 Time to process certificate issuance

The issuance of a certificate means the complete and final approval of an application by the Issuance Reports Manager. The issuance of a certificate must be made within 48 hours from the issuance of the IRM's report, as defined in the CPS of ANF AC.

4.4 Certificate issuance

As defined in the CPS of ANF AC.

ANF AC will avoid generating certificates that expire after the CA's certificates that issued them.

4.4.1 Certification entity's actions during the certificate issuance process

As defined in the CPS of ANF AC.

Once the electronic certificate is issued, the certificate delivery is always done electronically. The same cryptographic device that the subscriber or his legal representative used to generate the cryptographic key pair and the PKCS#10 request certificate must be used.

The cryptographic device establishes secure connection to ANF AC trusted servers. The system automatically performs the appropriate security verifications, and in case of validation the certificate is automatically downloaded and installed.

4.4.2 Notification to subscriber

ANF AC notifies the subscriber via e-mail, the certificate issuance and publication.

4.5 Certificate acceptance

4.5.1 Acceptance

As defined in the CPS of ANF AC.

4.5.2 Return of Certificate

The subscriber has a period of 7 days, from the delivery of the certificate, to verify its correct functioning.

In case of malfunction, or due to technical errors in the data contained in the certificate, the applicant or the certificate responsible can send an electronically signed e-mail to ANF AC, reporting the reason for the return. ANF AC shall verify the causes for return, revoke the certificate issued and issue a new certificate within 72 hours.

4.5.3 Monitoring

ANF AC is not responsible for monitoring, investigating or confirming the accuracy of the information contained in the certificate after its issuance. In case of receiving information regarding the inaccuracy or the current non-applicability of the information contained in the certificate, it can be revoked.

4.5.4 Certificate publication

The certificate is published in the repositories of ANF AC within a maximum period of 24 hours since its emission has occurred.

4.5.5 Notification of certificate issuance to third parties

No notification is made to third parties.

4.6 Rejection

As defined in the CPS of ANF AC.

4.7 Renewal of Certificates

Generally, as defined in the CPS of ANF AC.

4.7.1 Valid certificates

ANF AC notifies the subscriber and the applicant the expiration of the certificate expiration via email, forwarding the application form to proceed with its renovation. These notifications are sent 90, 30 and 15 days prior to the expiration date of the certificate.

Only valid certificates can be renewed.

4.7.2 Persons authorized to request the renewal

The renewal application form must be signed by the same applicant, be the subscriber or the legal representative that processed the certificate request. The personal circumstances of the applicant should not have changed, especially its legal representation capacity.

4.7.3 Identification and authentication of the Routine renewal applications

Identification and authentication for certificate renewal can be done in person using one of the methods described in this section, or processed electronically by completing the corresponding form and signing it with a valid certificate electronically issued as "qualified", and stating as holder the certificate subscriber of which renewal is requested.

In accordance with article 13.4 b) of Law 59/2003, December 19th, on Electronic Signature, certificate renewal by electronically signed applications requires that less than five years have passed since the personal identification took place.

To ensure compliance with art. 13.4. b) of the Electronic Signature Law and to not exceed the period of 5 years from the initial identification, ANF AC applies the following procedures and technical security measures:

- Certificates of ANF AC shall be always generated using a token that must be used to perform any renewal process.

  This token is unique to any other provided by ANF AC and is programmed so that the user may be able to make a single renewal. This technical procedure prevents an automatic processing once 5 years have passed since the initial identification.

- ANF AC follows a system of registration of applications, distinguishing date of request, -which coincides with the identification - and of issuance of the certificate. This control allows a second renewal if the period of 5 years has not been reached since the initial identification.

  The technical system requires a specific request of the user, the direct intervention of an ANF AC operator, which in turn, requires validating the application by applying coherent security verification. If 5 years have exceeded, the application itself blocks the process, otherwise facilitates the operator the process until the certificate renewal.

4.7.3.1 Certificate renewal of ones that have exceed 5 years from the initial identification.

The formalization of the application by handwritten signature of the applicant is required, process done in-situ by the person concerned and using sufficient original documentation. The procedures may be performed before:

- **Recognized Registration Authority**, as defined in the CPS of ANF AC, are natural or legal persons who ANF AC has provided with the technology to perform the functions of a registry entity, having ratified the corresponding assumption of liabilities agreement and collaboration agreement.

- **Collaborating Registration Authority** as defined in the CPS of ANF AC, are people who, per current legislation, have powers of a public notary.

- **Trustworthy entity**, as defined in the CPS of ANF AC, are entities which per ANF AC, have the necessary capacity to determine the identity, capabilities and freedom of action of the applicants.

4.7.4 Approval or rejection of applications for renewal

The same procedure performed for the emission process specified herein shall be followed.

4.7.5 Notification of certificate renewal

The same procedure performed for the emission process specified herein shall be followed.

4.7.6 Acceptance of the certificate renewal

The same procedure performed for the emission process specified herein shall be followed.

4.7.7 Publication of the renewal certificate

The same procedure performed for the emission process specified herein shall be followed.

4.7.8 Notification of certificate renewal

Not provided

4.7.9 Identification and authentication of re-keying applications after revocation (non-compromised key)

The renewal of expired or revoked certificates is not authorized.

4.8 Certificate modification

Not applicable.

4.9 Revocation and suspension of certificates

As generally defined in the CPS of ANF AC.

4.9.1 Circumstances for revocation

Besides those defined in the CPS, ANF AC shall:

- Provide instructions and legal support for reporting complaints or suspicions regarding the compromise of the private key, of certificate misuse or about any type of fraud or misconduct.

- ANF AC shall investigate incidents of which they become away within twenty-four hours of their receipt. The Security Manager, based on inquiries and verifications, shall issue a report to the Issuance Reports Manager, whom shall determine, if appropriate, the corresponding revocation substantiated in a Minute, which shall include:

    - Nature of the incident.
    - Received information.

4.9.2 Identification and authentication of revocation applications

The revocation of a certificate may be requested by:

- The certificate subscriber
- The legal representative of the subscriber
- A representative duly authorized
- The Recognized Registration Authority that intervene in the processing of the certificate issuance application

The identification policy for revocation requests accepts the following methods of identification:

- **Electronically**: by the applicant or certificate responsible electronically signing the revocation request on the date of the revocation request.
- **By telephone**: by replying to the questions asked from the telephone support service available at the number 902 902 172 (calls from Spain) or (+34) 933 935 946 (International).
- **In person**: the subscriber or the legal representative of the certificate holder appearing before any of ANF AC's offices published in the web address https://www.anf.es/sedes.html, proving their identity through original documentation, and manually signing the appropriate form.

ANF AC, or any of the Recognized Registration Authorities that form the National Proximity Network, may request the revocation of a certificate if they knew or suspected the private key associated to the certificate had been compromised, or any other fact that would recommend taking such action.

ANF AC must authenticate requests and reports relating to the revocation of a certificate, verifying they come from an authorized person.

These requests and reports will be confirmed following the procedures set out in the Certification Practice Statement.

4.9.3 Procedure for revocation request

The applicant of a revocation must fill the Certificate Revocation Application Form and process it before ANF AC by any of the means provided herein.

The revocation application shall contain at least the following information:

- Revocation request date.
- Identity of the subscriber.
- Reason given for the revocation request.
- Name and title of the person requesting the revocation.
- Contact information of the person requesting the revocation.

The revocation application shall be processed upon receipt.

The request must be authenticated, in accordance to the requirements established in the corresponding section of this policy, before proceeding with the revocation.

Once the request has been authenticated, ANF AC may directly revoke the certificate and inform the subscriber and, where appropriate, the certificate responsible on the certificate's change of status.

4.9.4 Revocation request grace period

As defined in the CPS of ANF AC.

Revocation requests shall be processed immediately when reasonably aware of the cause of revocation and the applicant has been authenticated and its capacity to act has been verified.

4.9.5 Maximun processing time of the revocation request

The revocation request will be processed in the shortest possible time, always following the procedure of verification and authentication of the request, which is the Issuance Reports Manager's responsibility.

4.9.6 CRL lists verification requirements

The relying parties must verify the status of the certificates on which they will rely; for such purpose, they can verify the latest CRL issued within the period of validity of the certificate of interest.

4.9.7 CRL issuance frequency

As defined in the CPS of ANF AC.

4.9.8 On-line verification availability of the revocation

ANF AC makes available to relying parties an on-line revocation verification service, which is available 24 hours a day, 7 days a week.

4.9.9 On-line verification requirements of the revocation

Relying parties may verify online the revocation of a certificate in the website https://www.anf.es.

The ANF AC's certificates consultation system requires prior knowledge of some parameters of the certificate of interest. This procedure prevents massive data collection.

This service meets the requirements in terms of personal data protection and only provides copies of these certificates to duly authorized third parties.

Access to this system is free.

4.9.10 Certificate suspension

Not applicable.

4.9.11 Suspension requests identification and authentication

Certificate suspension is not allowed.

4.10 Keys storage and recovery

As specified in the agreement for the provision of services.

5 Physical Security, Facilities, Management and Operational Controls

ANF AC maintains the following criteria in relation to the information available for audit and analysis of incidents related to certificates.

a) Control and incident detection

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

- By telephone: 902 902 172 (calls from Spain); (+34) 933 935 946 (International).
- By email: info@anf.es
- Filling the electronic form available on the website https://www.anf.es
- In person at one of the offices of the Recognized Registration Authorities.
- In person at one of the offices of ANF AC.

The annual internal audit protocol specifically requires the completion of a review of the operation of certificates issuance, with a sample of 3% of the issued certificates.

b) Incident Registry

ANF AC has an Incident Registry in which it is registered every incident that has occurred with the certificates issued and the evidences obtained. These incidents are registered, analyzed and resolved per the procedures of ANF AC's Information Security Management System.

The Security Manager determines the severity of the incident and names a responsible and, in case of significant security incidents, reports to the PKI Governing Board.

5.1 Physical security controls

As defined in the CPS of ANF AC.

5.2 Procedural controls

As defined in the CPS of ANF AC.

5.3 Personnel controls

As defined in the CPS of ANF AC.

6 Technical Security Controls

6.1 Key pair generation and installation

As defined in the CPS of ANF AC.

6.2 Private key Protection

As defined in the CPS of ANF AC.

6.3 Other management aspects of key pair

As defined in the CPS of ANF AC.

6.4 Activation data

As defined in the CPS of ANF AC.

6.5 Computer security controls

As defined in the CPS of ANF AC.

6.6 Life cycle technical controls

As defined in the CPS of ANF AC.

6.7 Network security controls

As defined in the CPS of ANF AC.

6.8 Time-stamping

As defined in the Time-Stamping Authority Policy and Practice Statement.

6.9 Cryptographic Module Security Controls

As defined in the CPS of ANF AC.

7 Certificates profiles and Lists of Revoked Certificates

The certificate incorporates information structured in agreement with THE IETF's X.509 v3 standard as defined in the specification RFC 5280 *(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)*.

Certificates which are issued as "qualified" comply with the standards:

- ETSI TS 101 862 v.1.2: Qualified Certificate Profile.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

ANF AC is currently undergoing the process of adaptation to the ETSI EN 319 412 *(Certificate Profiles)* standard.

The certificate validity period is outlined in Universal Coordinated Time, and coded per the specification RFC 5280.

The subject public key is encoded per the specification RFC 5280, as well as the signature's generation and codification.

Within the certificates, besides the already standardized common fields, there are also included a group of "proprietary" fields which provide information in relation to the subscriber, or other information of interest.

Proprietary fields

Internationally unambiguous identifiers have been assigned. Specifically:

- Fields referenced with OID 1.3.6.1.4.1.18332.x.x are proprietary extensions of ANF AC. The complete list of OID codes and the information associated to the same may be consulted in the section "Proprietary fields of ANF AC" of the Certification Practice Statement of ANF AC.
- Fields with ISO/IANA of MPR 2.16.724.1.3.5.x.x, are proprietary extensions required and identified in the Identification and Electronic Signature Scheme v.1.7.6 published by the High Council of Electronic Administration.
- Fields with OID 1.3.6.1.4.1.18838.1.1 are proprietary of the Spanish State Tax Administration Agency (Agencia Estatal de Administración Tributaria "AEAT").

QCStatements

The certificates issued by ANF AC follow what is defined in the ETSI EN 319 412-5 *(Certificate Profiles-QCStatements)*:

- **QcCompliance**, refers to a declaration of the issuer in which it states the qualification with which the certificate is issued, and the legal framework to which it is submitted. Specifically, the certificates submitted to this policy, issued as qualified, outline:

  "This certificate is issued with the qualification of qualified in accordance with Annex I of Regulation (EU) 910/2014 of the European Parliament "

- **QcLimitValue**, informs about the monetary limit, which the CA assumes as a liability for the loss of transactions attributable to it. This OID contains the values sequence: currency (coded in

accordance to the ISO 4217), quantity and exponent. E.g. EUROS 100x10 raised to 1, which presupposes a monetary limit of 1000 EUROS.

Furthermore, to facilitate the consultation of this information, the liability limit is included in the proprietary extension of the OID 1.3.6.1.4.1.18332.41.1, outlining the amount in euros. In case of doubt or dispute, one must always give preference to the reading value outlined in the OID 1.3.6.1.4.1.18332.41.1.

- **QcEuRetentionPeriod**, determines the period in which all the information relevant to the use of the certificate, after it has expired, is stored. In case of ANF AC, it is 15 years.
- **QcSSCD**, determines that the private key associated to the public key contained in the electronic certificate, is in a qualified signature creation device as defined in accordance with Annex II of the Regulation (UE) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and repealing the Directive 1999/93/CE.
- **QcType**, when the certificate is issued with the profile (SIGNATURE), QcType 2 is outlined
- **QcPDS,** The URL that allows access to all the ANF AC PKI policies is provided (*PDS Policy Disclosure Statements*)

Subject Alternative Name

Specification IETF RFC 5280 provides the use of the following data type:

- Email-based identity.
- Identity based on Distinguished Name (DN), which is often used to construct an alternative name based on proprietary attributes, which are not ambiguous in any case.
- Identity based on internet domain name (DNS).
- IP address-based identity.
- Identity based on universal resource identifier (URI).

7.1 Certificate Profiles

As defined in the technical background document.

7.2 CRL profile

As defined in the CPS of ANF AC.

7.3 OCSP profile

As defined in the CPS of ANF AC.

8 Compliance Audit

8.1 Frequency of compliance controls for each entity

As defined in the CPS of ANF AC.

8.2 Identification of the personnel in charge of the audit

As defined in the CPS of ANF AC.

8.3 Relationship between the auditor and the audited entity

As defined in the CPS of ANF AC.

8.4 List of items audited

As defined in the CPS of ANF AC.

8.5 Actions to be taken because of a lack of compliance

As defined in the CPS of ANF AC.

8.6 Treatment of audit reports

As defined in the CPS of ANF AC.

9 General Provisions

9.1 Fees

As defined in the CPS of ANF AC.

9.2 Financial responsibility

As defined in the CPS of ANF AC.

9.3 Confidentiality of information

As defined in the CPS of ANF AC.

9.4 Privacy of personal information

As defined in the CPS of ANF AC.

9.5 Intellectual property rights

As defined in the CPS of ANF AC.

9.6 Obligations and guaranties

As defined in the CPS of ANF AC.

9.7 Disclaimers of guaranties

As defined in the CPS of ANF AC.

9.8 Limitations of liability

As defined in the CPS of ANF AC.

9.9 Interpretation and execution

As defined in the CPS of ANF AC.

9.10 Management of the CP

As defined in the CPS of ANF AC.

Appendix I

Electronic Certificate Application Form

I. Certificate type

First specify the type of certificate you want to solicit.

Remember that in case of Public Administration Electronic Seal Certificates, the Security Levels are automatically outlined by the system and depending on the type of device (Medium Level software token / High Level HSM token)

Certificate type		
Electronic Seal	Public Administration Electronic Seal	☐

II. Certificate Subscriber Data

Entity type		
Private organization	☐	Public administration ☐

Legal Person	
Denomination:	VAT number:
Legal Form:	
Department:	
System Name / Application:	

Public Administration	
Denomination:	VAT number:
Department:	
System Name / Application:	
Address:	

Contact details	
Address:	
Locality:	Province:
Country:	Zip code:
Phone (landline):	Fax:
E-mail:	Website:

III. Certificate Applicant Data (subscriber's legal representative)

Personal details
Name:
First Surname:
Second name:
Department:
Nationality:
ID card type (DNI/NIE/Passport):
ID card number *Include letter:

Contact details	
Address:	
Locality:	Province:
Country:	Zip code:
Phone (landline):	Fax:
E-mail:	Website:

Representation data	
Title of representation (Director, proxy ...):	
Notary that formalizes powers of attorney (or another grantor):	
Protocol number / identifier:	Date:

IV. Certificate Applicant Responsible

Please complete the following fields in case the certificate responsible is a person other than the applicant.

Remember that, in addition to the application form and contract for the provision of certification services, the applicant and the certificate responsible must fill and sign the "Authorization and Acceptance of Liability in the Certificate Use Minute".

Personal details
Name:
First surname:
Second surname:
Department:
Nationality:
ID card type (DNI/NIE/Passport):
ID card number (DNI/NIE/Passport):

Contact details	
Address:	
Locality:	Province:
Country:	Postal code:
Phone (landline):	Fax:
E-mail:	Website:

Representation data	
Title of representation (Director, proxy ...):	
Notary that formalizes powers of attorney (or another grantor):	
Protocol number / identifier:	Date:

IV. Optional details

Trade name or trademark	
Include trade name ☐	Include registered trademark ☐

Name:	Trademark:

Important notice: The trade name or trademark can only be included if:

- You are the rightful owner of the trade name or trademark.
- You have express permission by the trademark or trade name legitimate owner.

In any event, attach certifying document.

Informative attributes to be incorporated in the certificate

Notice: Supply documentation in which the information listed is accredited. Remember that ANF AC reserves the right to include only information on which it can verify its veracity.

Usage Limitations
Signature limit amount:
Base currency for signature limit amount:
Certificate usage limit*1:
Other:

*1 The outlined concept assumes that the certificate can only be allocated to such use.

V. The Applicant/Subscriber STATES:

That ANF AC has made available to the subscriber, prior to delivery of the certificate:

- The cryptographic signature device, signature verification, encryption or decryption of any of the types specified in the specific Certification Policy, depending on where the key pair is generated and stored.
- Basic information about the policy and certificate usage, especially including information on ANF AC and its applicable Certification Practice Statement, and their duties, powers and liabilities.
- Information on the certificate and the cryptographic device.
- Information on the obligations of the certificate responsible.
- Information on the liabilities of the certificate responsible.
- Information on the exclusive imputation method to the responsible of its private key and its certificate activation data and, where appropriate, the cryptographic device.

It has been informed that all the information detailed below is available on the website https://www.anf.es. Specifically:

- Certificate Application Form Template.
- Agreement for the Provision of Certification Services Template.
- Law 59/2003 on Electronic Signature.
- Organic Law on Data Protection (LOPD).

- Data Protection Regulation.
- Certification Practice Statement of ANF AC.
- Certification Practice Statement of ANF TSA CA.
- Certification Policy to which the requested certificate is submitted.
- Electronic Signature Policy associated with the certificate and signature device.
- Issuance and certification services fees.

VI. The Applicant/Subscriber DECLARES:

1. The application is made freely and under no duress.
2. The applicant / subscriber has not been declared ineligible by a court.
3. In case the applicant is acting on behalf of a third party, the subscriber is in possession of his mental faculties, has sufficient intellectual capacity to know the scope of the electronic signature certificate and performs this procedure following their instructions.
4. The certificate application has NOT been rejected by any other Trust Service Provider.

And that he/she has been properly instructed prior to the application on the following issues:

1. Obligations on:
   a) The generation of the signature creation data without third party mediation and its exclusive knowledge of the activation password.
   b) The escrow procedures for the signature creation data and the activation password.
   c) The procedure to be followed for reporting the loss or possible misuse of the data and the obligation to revoke the certificate.
   d) The usage of the certification devices delivered.
2. The mechanisms to ensure the reliability of the electronic signature of a document over time.
3. The method used by the provider to verify the identity of the signer and other information contained in the certificate.
4. The precise conditions of use of the certificate, its possible usage limits and how the provider ensures its liability.
5. Regarding the certifications obtained by ANF AC and applicable procedures for settling conflicts extrajudicially that may arise from the exercise of their activity.
6. The certificate holder acknowledges been informed that the information provided, including biometric data obtained in the identification process, will be uploaded in automated files, resulting applicable the legislation on personal data protection. Expressly authorizes ANF AC, responsible for the files, to its computer storage and that it can transfer them to third parties within the public key infrastructure for the provision of electronic certification services.
7. The Subscriber authorizes the publication of his certificate.
8. The address and contact details of ANF AC are continuously updated on the web address https://www.anf.es/address/

VII. The Applicant/Subscriber AGREES, without exception:

1. The Certification Policy associated with this certificate, the Certification Practices Statement of ANF AC, the ANF AC CPS as Time Stamp Authority and Certification Policies related to the TSA, without exception.
2. Permitted, restricted and prohibited uses of the certificate, as detailed in the Certification Policy associated with this certificate, as well as the use limitations.
3. ANF AC limits its liability to the issuance and management of certificates and cryptographic devices supply (signing and signature verification, as well as encryption or decryption).
4. ANF AC has a sufficient liability guarantee coverage through an insurance policy issued by Lloyd's, in the amount of FIVE MILLION EUROS (€ 5,000,000), which covers the risk of liability for

damages that could result from using certificates issued by this Certification Authority, thus fulfilling the obligation established in article 20.2 of Law 59/2003, of December 19th, on Electronic Signature.

5. Limit use of electronic certificates and certification services ANF AC, is 1,000 Euros. The use of electronic certificate or certification services ANF AC which exceed this limit will be under the sole responsibility of the applicant/subscriber.
6. The responsibility assumed by using the certificate, is equivalent to handwritten signature.
7. If considered impaired by the certification services received, the applicant/subscriber has been instructed as to the mechanisms of complaint and claim for damages that may have occurred.
8. All data reported in this document are true and assumes the obligation to notify ANF AC of any change that may occur over time.
9. The data will be loaded and stored into computer files. The applicant/subscriber has been instructed about the rights of access, rectification, cancellation and opposition established by ANF AC security norms; that the storage is computer and that ANF AC can transfer them to third parties within the public key infrastructure

The Registration Authority which handles this request, claims to have thoroughly proven the identity of all parties involved in the application, ensures that documents that have been shown are true, to the best knowledge and belief, original, and that scanned copies attached to the electronic form have been collated and asserts its full agreement with the original.

Those appearing request ANF Autoridad de Certificación the issuance of the certificates of the types established in point IV of the form.

In at

Signature of Applicant / Subscriber

Signature of Certificate Responsible

Signature of RA Operator

Appendix II

Agreement for the provision of Electronic Certification Services

PARTIES

FROM ONE PART,

Mr. Florencio Díaz Vilches, of legal age, with VAT number 37.271.387W, established for this agreement in Gran Via de les Corts Catalanes, 996, Floors 3rd and 4th of Barcelona.

FROM THE OTHER PART,

Mr. / Mrs.....,

of legal age, with VAT number ....., for communication purposes, determines

residence in .....,

Town.....Province..... Country.....,

email.....Mobile phone (country prefix).....(number).....,

Telephone (landline) (country prefix)....(number).....fax(country prefix)....(number).....

INVOLVED

Mr. Florencio Díaz Vilches on behalf of **ANF Certification Authority**, acting in his capacity as Chairman, a non-profit entity incorporated under the Spanish Organic Law 1/2002 of March 22 and registered with the Ministry of Interior with the national number 11,465, VAT number G-63287510 and having its registered office in Paseo de la Castellana, 79 -28046 - Madrid- Spain, hereinafter **ANF AC**.

Mr./Mrs....., hereinafter **APPLICANT**.

The **APPLICANT** of the services, intervenes on behalf of:

.....,

with VAT number ....., that for the communication purposes, determines

residence in.....,

Town.....Province..... Country.....,

email.....Mobile phone (country prefix).....(number).....,

Telephone (landline) (country prefix)....(number).....fax(country prefix)....(number).....

The **APPLICANT** intervenes in its capacity as.....,

Being **SUBSCRIBER** of the services .....,

And mutually recognizing the legal capacity necessary for the effectiveness of this agreement freely and voluntarily,

DECLARE

I. That **ANF AC** is an entity that issues electronic certificates with the qualification of qualified, and provides professional electronic certification services, in accordance with Spanish Law 59/2003, of December 19th, on Electronic Signature, and Regulation (EU) No 910/2014.

II. That the activity of **ANF AC**, as a provider of electronic certification services, is regulated by the LFE, the Regulation (EU) 910/2014, and as stated in its Certification Practice Statement (CPS), Certification Policies (CP), as well as additional documents supplied to the **APPLICANT**.

III. That the **SUBSCRIBER/APPLICANT** understands the electronic certification services offered by **ANF AC**, and wants to use them for its professional or business activity development.

IV. That the **SUBSCRIBER/APPLICANT** understands and accepts the fees associated with these electronic certification services, which are permanently posted and updated on the website https://www.anf.es

V. That the **SUBSCRIBER/APPLICANT** receives in this act an Electronic Signature Device approved by ANF AC, in which it is stored a copy of:

- ANF AC Certification Practices Statement.
- ANF TSA AC Certification Practices Statement.
- Certification Policies published by ANF AC.
- ANF AC Electronic Signature Policy.
- Law 59/2003, of December 19th, on Electronic Signature.
- Regulation (UE) 910/2014.

All ANF AC documents are published and available in the website https://www.anf.es/en/

Therefore, the parties agree to the implementation of this Agreement, subject to the following

CONDITIONS

1. PURPOSE

The purpose of this document is to regulate the contracting of electronic certification services of **ANF AC**, consisting on the issuance of an electronic certificate, pursuant to the request made by the **SUBSCRIBER/APPLICANT**, which will be attached as an annex to this agreement.

2. REGULATION

The relations arising between **ANF AC** and the **SUBSCRIBER/APPLICANT**, within the framework given by the Certification System developed by **ANF AC** will be governed by this Agreement, by the Certification Practice Statement (CPS), the specific policy to certificate contracted (CP), and in accordance with the current legislation.

The CPS and the CP are public documents and available permanently in the website https://www.anf.es/en

3. OBLIGATIONS OF THE SUBSCRIBER/APPLICANT

3.1. Provide accurate and updated information on the processing of their applications for certificates.

3.2. Do not allow third party intervention in the process of generating the signature creation data.

3.3. Properly safeguard the Electronic Signature instruments, and especially the signature activation data.

3.4. Adapt the use of the certificate to the permitted uses in accordance with the provisions of the Certification Policy to which it is associated.

3.5. Immediately inform **ANF AC** on any suspected risk of the certificate and to not use it once notified.

3.6. Immediately inform **ANF AC** about any variation of the data provided in the certificate request.

3.7. Pay the fees for the services requested.

3.8. Acknowledges and accepts the legal equivalence of electronic signatures to handwritten ones.

3.9. Agrees that all authenticated electronic communications using electronic signatures provided by **ANF AC**, have the same legal effect, validity and binding force as a written notice duly authenticated.

3.10. Agree that electronic documents obtained after the scanning process carried out by the RA Manager application of electronic certificates management, correspond to the true image of the respective original documents.

3.11. In case of revocation of the certificate, it obliged to cease their use.

3.12. The **SUBSCRIBER/APPLICANT** guarantees that the denominations, names or domains described in the application form in this agreement for the provision of services do not infringe third parties' rights.

3.13. Use the certificate within the constraints that are imposed by the corresponding Certification Policy and the Electronic Signature Policy.

And in general, all the specified in the CPS, with special relevance to section 9.5.3 Responsibilities of subscribers and certificate responsible.

3.14. To the general obligations previously mentioned, the following requirements are added per the type of certificate:

- For the issuance of SSL with or without EV and Electronic office certificates in any of its modalities, the **SUBSCRIBER/APPLICANT** shall appoint a technical manager, as a contact person for ANF AC.

- Regarding the SSL or Electronic Office certificates, **ANF AC** may require the **SUBSCRIBER/APPLICANT** additional information and documentation relative to the DNS and e-mail accounts.

- Regarding the SSL EV and Electronic Office EV, the **SUBSCRIBER/APPLICANT** declares that he/she has the exclusive use of the domain for which the certificate is requested.

- The refusal by the **SUBSCRIBER/APPLICANT** to provide the information or documents referred to in the preceding paragraph, shall restrict ANF AC in providing the certification contracted, without this situation involving the waiver of the established fees, which shall be promptly paid by the SUBSCRIBER.

- Any other requirement or condition expressed in the Certificate Policy for Secure Server SSL, Extended Validation Secure Server SSL, Electronic Office in any of its modalities.

4. REJECTION

4.1. The **SUBSCRIBER/APPLICANT** declares that it has informed the RA Operator of all those applications that have been rejected, and the causes that motivated the rejection.

4.2. A Public Key Infrastructure (PKI) system is developed in a framework of mutual trust and good faith relationships. The

SUBSCRIBER/APPLICANT declares that it does not have nor has had a conflict of interest with **ANF AC** or its Governing Board members.

4.3. Application for certificates or certification services is prohibited to persons or entities having a direct or indirect dependence, with entities that are competition to ANF AC. When conducting a transaction with manifest falsehood, the **SUBSCRIBER/APPLICANT** shall compensate with FIFTY THOUSAND EUROS (€ 50,000) as a penalty.

5. PROVISION OF SERVICES, OBLIGATIONS, LIABILITIES OF THE CA.

5.1. **ANF AC** provides certification services in accordance with the provisions of the CPS, the applicable Certification Policy and the Law 59/2003, on Electronic Signature.

5.2. **ANF AC** shall be liable for negligence or lack of due diligence by the terms of this agreement, except in cases of limitation of liability provided in its CPS and Policies.

By accepting the certificate, the **SUBSCRIBER/APPLICANT** agrees to indemnify and, if necessary, to compensate **ANF AC** of any act or omission that causes damage, loss, liabilities, expenses, procedural or otherwise, including professional fees, in which **ANF AC** may incur, that are caused by the use or publication of certificates and arise from any of the reasons specified in the CPS or Policies applicable to the requested certificate.

5.3. **ANF AC** will not be able to modify a certificate once it is issued.

5.4. **ANF AC**, in accordance with the functions assigned under this agreement, ensures the logical and physical security of the certification process to be performed.

5.5. **ANF AC** ensures that it will proceed to revoke the electronic certificate at the request of **SUBSCRIBER/APPLICANT.**

5.6. **ANF AC** agrees to not store or copy signature-creation data of its served users.

5.7. **ANF AC** will retain all information and documentation relating to the issued certificates and valid certification practice statements during a period of 15 years from the date of issuance, so signatures made with them can be verified.

5.8. **ANF AC**, in accordance to article 18 c) of Law 59/2003, on Electronic Signature, guarantees the publication of certificate revocation lists, which are freely accessible through the web site https://www.anf.es

The Periods of updating the CRLs are specified in the CPS and Certification Policy to which each type of certificate is subject to, and the maximum date for the next update is indicated in the corresponding field of the CRL.

6. SERVICE CONDITIONS

6.1. For the provision of electronic certification services, **ANF AC** has published performance and security standards, such as the CPS. Likewise, relationships with third parties and entities are formalized by corresponding written contractual agreements.

6.2. **ANF AC** has informed the **SUBSCRIBER/APPLICANT** of this document, in writing, and providing electronic access to information about the following issues:

1. º The obligations of the undersigned, the way in which signature creation data are safeguarded, the procedure to be followed for reporting the loss or potential misuse of such data and certain creation and verification devices of electronic signatures that are compatible with signature data and the certificate issued.

2. º The mechanisms to ensure the reliability of the electronic signature of a document over time.

3. º The method used by the provider to verify the signer's identity or other information contained in the certificate.

4. º The precise conditions of use of the certificate, its possible usage limits and the way in which the provider guarantees its liability.

5. º The certifications obtained by the certification service provider and procedures for settling the conflicts that may arise from the

exercise of the certification activity.

6. º All other information contained in the Certification Practice Statement.

7. º Likewise, **ANF AC** undertakes to provide the information, previously mentioned, upon request of third parties affected by the certificates.

6.3. The validity of the certificate shall be for a period of two years from the time of issuance.

6.4. The revocation of a certificate is irreversible, producing its definite cancellation.

6.5. **ANF AC** does not store, nor has opportunity to store signature creation data, activation data, or even the activation password of the Identification Minute. Consequently, it is impossible to retrieve any of these values in case of loss.

7. PLACE OF ACTIVITY PROVISION

The place of performance of the obligations relating to electronic certification services and, where appropriate, software licenses, is the registered office of **ANF AC**.

8. SOFTWARE LICENCE

ANF AC provides to the **SUBSCRIBER**, non-exclusive and non-transferable license to use copies of the software received from **ANF AC** to operate the signature device where appropriate, and the other services included in the software**.**

It is strictly prohibited, unless authorized in writing by **ANF AC**, subject the signature device or any software to reverse engineering technique.

9. USAGE OF THE NAME AND CORPORATIVE IMAGE OF THE PARTIES

The parties mutually grant a non-exclusive and non-transferable license to use the different elements of its corporate image, including the distinctive signs, logos and registered trademarks by each party, exclusively on marketing materials, advertising, products and services information sheets, products and services packages, web pages that use the products and services of the parties, as well as on the signature devices and documents used in certification procedures.

The usage of each party's corporate image elements must be in accordance to the corresponding corporate image manual as well as to the instructions of each party.

No party grants to the other party any rights on the trademark, trade name, company name or good business practices of each party, except rights which are specified in these terms.

No party can neither remove nor destroy any indication regarding copyrights, patents or trademarks contained in any product, electronic service or documents of all kinds.

10. FEES

The rates for the services provided by this Certification Entity, are published in the URL https://www.anf.es

11. DATA PROTECTION

ANF AC, in the treatment of personal data necessary for the development of its business as a provider of certification services, is subject to the provisions of the Organic Law 15/1999 on personal data protection, its development norms and the Law 59/2003, on Electronic Signature.

The **SUBSCRIBER/APPLICANT** knows that the personal data provided to ANF AC will be incorporated into an automated file under the responsibility of ANF AC.

The **SUBSCRIBER/APPLICANT** consents in the capture and storage of photographic image and fingerprints, in cases that are necessary for the provision of the requested certification service.

The **SUBSCRIBER/APPLICANT** consents also the publication of the public part of their electronic certificates.

The **SUBSCRIBER/APPLICANT** shall defend, indemnify and hold harmless ANF AC for any loss

or damage that results from any infringement attributable to the **SUBSCRIBER/APPLICANT** on the protection of personal data.

ANF AC will not be able to modify a certificate that has already been issued to rectify or cancel personal data contained in it, since this requires the revocation of the certificate.

Also, data rectified or canceled concerning revoked certificates, will be maintained by ANF AC for a period of 15 years, in accordance to article 20.1 f) of the Law 59/2003 on Electronic Signature.

12. DIVISIBILITY OF THE GENERAL CONDITIONS

The clauses of this agreement are independent from each other, which is why if any clause is held invalid or unenforceable, the remaining clauses of this document shall remain applicable, except expressly agreed by the parties.

13. LAW AND JURISDICTION

a) Both parties agree that any dispute arising from this agreement or legal act, as well as those arising thereof or in connection with it- including any question regarding its existence, validity, termination, interpretation or execution- shall be finally settled by Arbitration, administered by the International Court of Arbitration of the Distribution Business Council (TACED), in accordance with the Arbitration Rules in effect on the date of submission of the request for arbitration. The Arbitral Court appointed for this purpose shall consist of a sole arbitrator and the place of arbitration and the substantive applicable law to the settlement of the dispute, shall be those corresponding to the TACED's registered office.

b) If for some reason is not possible to settle the dispute by the arbitration procedure outlined in the previous section, the parties, waiving any other jurisdiction that may correspond, are subjected to the resolution of any conflict that may arise between them to the courts Barcelona.

Both sides, in evidence pursuant to every end of this agreement, sign in duplicate and one effect, in

Barcelona, 201

SUBSCRIBER/APPLICANT Signature

In the presence of the RA Operator

SPECIAL CONDITIONS

Electronic invoice with enforceable character

With support of the art. 2 ter of the Law 56/2007, December 28th, on Measures to Promote Information Society, included by Law 25/2013, of December 27th, on Promotion of Electronic Invoice and creation of an accountability registry of invoices in the public sector, ANF Certification Authority [ANF AC] and the Subscriber / Applicant of services, expressly agree that electronic invoices issued by ANF AC due to electronic certification services provided by ANF AC, or other services provided to the Subscriber / Applicant by institutions member of the ANF AC Cluster*, will have an enforceable character, circumstance that shall be stated in the invoice, serving the signature at the bottom as the Subscriber's acceptance, understanding the present document annexed to the invoice for the purposes of Law 25/2013, December 27th.*

Barcelona, 201

SUBSCRIBER/APPLICANT Signature

In the presence of the RA Operator

Appendix III

Authorization and Acceptance of Liability in the certificate Use Minute

Instructions: For renewing the electronic certificate, just **sign** this letter template. For the generation of the signature, it is essential to use the **certificate** you want to renew.

A/A Issuance Reports Manager

ANF AUTORIDAD DE CERTIFICACIÓN

Dear Sir / Madam:

Since no more than 5 years have passed since I made the identification process before one of your RRAs, and being near the expiration date of my electronic certificate, I wish to proceed with its renewal by the Certification Authority to which I address.

I agree to the cost of the renewal fees established in your website www.anf.es plus any applicable tax, to be charged into the bank account of which I am owner, number ……

By signing this document, I formally express my electronic certificate renewal request, which I have used for carrying this authentication. I declare that no change has been produced in the data incorporated to the certificate.

Yours sincerely,

Important notice: Per the provisions of Article 13, paragraph 4, letter b of Law 59/2003, of December 19th, on Electronic Signature, this type of renewals can only be performed if no more than five years have passed since the identification was performed before a Registration Authority.

Appendix IV

Certificate Revocation Application Form

Application Reference:

Known details of the certificate
Certificate serial number:
Type of certificate:

Data of the certificate subscriber
Name of subscriber:
DNI (natural person) or VAT number (legal person):

Data of the revocation applicant:	
Name:	
Surname:	
Last surname:	
Identity card type (DNI/NIE/Passport):	
Identity card number *Include letter:	
Telephone number:	E-mail address:

Acts on own behalf: YES ☐ NO ☐

Acts on subscriber representation: YES ☐ NO ☐

Power of Attorney:

Other representation *Add information thereon:

Reason for revocation request:	
☐	Owner's voluntary request
☐	Loss of the storage support
☐	Death or incapacity, total or partial, of subscriber
☐	Completion of representation
☐	Key compromised
☐	Obsolete information
Faulty issuance of a certificate due to:	
☐	1. A requirement was not complied with for issuing the certificate
☐	2. Reasonable belief that some fundamental data relevant to the certificate is or could be false
☐	3. Existence of an error through data entry or other process error
☐	Deliberate misuse of keys and certificates, or the lack of observance or violation of operational requirements contained in the CPS or in this PC.
☐	Certificate replace
☐	The length of keys has been shown to be insecure
☐	The algorithms used have been shown to be insecure
☐	One of the higher-level certificates in the Certification Route has expired
☐	Other:

The subscriber/applicant DECLARES:

That he/she has been informed that, prior to revoking the certificate, ANF Authority of Certification (henceforth, ANF AC) must carry out the corresponding checks in relation to the applicant's identity and their capacity to make this revocation request.

That he/she understands that written in the Certificate Practice Statement and Certification Policy associated with ANF AC's certificate, and that the effects of revocation are irreversible.

That he/she has the legal capacity to carry out this revocation and that otherwise he accepts all damages and costs that this request carries, both the administrative costs caused to ANF AC, as well as those caused to the certificate Subscriber.

And the revocation will take effect from the moment that it is published in ANF AC's repositories.

In , at 201 Signature of applicant

Appendix V

Certificate Reception and Acceptance Minute

The signatory, whose data correspond to those contained in the electronic certificate used to sign this minute:

DECLARE

- That has checked and verified the veracity of all information included in the electronic certificate issued by ANF AC, and that it is used for signing this document.
- That prior to the issuance of the certificate, the CA provided them with the following information and documentation:
    - Certification Practice Statement (CPS).
    - Certification Policy (PC) associated to the issued certificate.
    - Applicable fees.
    - Forms of application, renewal and revocation of certificates.
    - Procedure to request certificate revocation.
    - Procedure to request certificate renewal.
    - How to contact the issuer:
        - Telephone: 902 902 172 (calls from Spain)
          (+34) 933 935 946 (International)
        - Web: www.anf.es
        - E-mail: info@anf.es
        - In person: Barcelona, Gran Via de les Corts Catalanes, 996, 4º. Zip Code: 08018.
- That prior to the issuance of the certificate, the CA made available the key generation device, the certificate processing request (PKCS#10) and signature creation and verification device. Through these instruments, and without third party intervention, the signatory privately and freely selected the signature activation data (PIN), and generated the keys and the request certificate.
- That he/she has downloaded the certificate in the same electronic device that contains the cryptographic keys associated with it.
- That he/she acknowledges, understands and accepts the Certification Practice Statement of ANF AC, the Signature Policy, Certification Policy, and other documents associated with this electronic certificate.
- Commits to make a proper and responsible use of the certificate, subject to the use limitations contained therein and the purpose of its issuance.
- That he/she assumes the limitation of liability of the issuer reflected in the electronic certificate.
- That he/she agrees to guard the private key of the certificate and the electronic device containing it with due diligence, keeping the activation signature data (PIN) with absolute privacy and confidentiality.
- That he/she has checked all the information contained in the certificate, claiming to be truthful and compliant.
- That he/she assumes its obligations as a subscriber, or where appropriate, as a legal representative, and agrees to immediately notify the issuer any changes to the information contained in the certificate, immediately ceasing use when security has been compromised or there are suspicions of it, requesting the certificate revocation.
- That he/she agrees to cease using the certificate when it has become obsolete, either by expiration or revocation.
- That he/she acknowledges and agrees that he/she has 15 days, from the receipt of the certificate, to verify its correct functionality, and such time shall be deemed to verify that both

the certificate and the electronic device used for storage, meet the required functional and technical requirements without suffering deficiency.
- That he/she ratifies the previously signed documents associated to the application form and the agreement for the provision of services.
- That he/she ratifies the authorization of publishing the public part of the certificates received and accepted in this minute.
- That he/she has verified that the certificate issued by ANF AC is also correct.

And in witness whereof, electronically signs this Certificate Reception and Acceptance Minute.

He/she also wants to, **expressly and formally**, sign the acceptance of:

Membership as user in the **Universal Exports Asia** platform

The membership in **Universal Exports Asia [UEXS]** carries no commitment nor obligation, your signature authorizes only **ANF AC** to provide your data so that **UEXS** gives you authorized access as professional buyer in the e-Commerce platforms managed by this entity, accessing to the associated manufacturers products, and benefiting from International Distributor prices.

SEPA Order

The present order sets up **ANF AC** to present to the collection of the receipts issued by the services that **ANF AC** has invoiced to the signatory, due to the services that he/she has received from **ANF AC** or from some of the member entities of the **ANF AC** Cluster.

Through the signature of this domiciliation mandate, the signatory (debtor) authorizes (A) **ANF AC** to send instructions to his/her banking entity / savings to debit in his/her account and (B) the entity to perform the debts in his/her account following the instructions of **ANF AC** creditor. This domiciliation mandate is intended exclusively for operations between companies and/or freelancers. The signatory (debtor) has no right for his/her entity to refund him once the debit has been made, but he/she can ask his/her institution not to make the debt in the account until the due date. He/she will be able to obtain detailed information of the procedure in his/her financial entity.