Electronic signature policy

based on certificates issued by hierarchies of

ANF Certification Authority

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

Security level

Public Document

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 Certification Authority, (hereinafter ANF AC), is a legal entity, established under Organic Law 1/2002 of March 22 and registered with the Ministry of the Interior with the national number 171,443 and CIF G-63287510.

ANF AC has been assigned the private company code (SMI Network Management Private Enterprise Codes) 18332 by the international organization IANA -Internet Assigned Numbers Authority-, under the iso.org.dod.internet.private.enterprise branch (1.3.6.1.4.1 -IANA –Registered Private Enterprise-)

The purpose of this policy is to reinforce confidence in electronically signed acts through certain conditions for a given context.

When data is signed, the signer indicates acceptance of general conditions and specific conditions applicable to electronic signatures. This acceptance is done by including an OID field in the signature. This object identifier uniquely specifies a certain electronic signature policy.

If the field corresponding to the electronic signature regulations is absent and no applicable regulations are identified, then it must be assumed that the signature has been generated without any regulatory restriction, and consequently, that no specific legal or specific meaning has been assigned to it. contractual. It would be a signature that does not expressly specify any specific semantics or meaning
and, therefore, it will be necessary to derive the meaning of the signature from the context (and especially, from the semantics of the signed document).

This document details and complements what is generically defined in the Certification Practice Statement of ANF AC OID 1.3.6.1.4.1.18332.1.9.1.1.

This Electronic Signature Policy (hereinafter, PFE) has been structured in accordance with the provisions of international reference technical standards and current legal standards, details of all those contemplated in the References section of this document are specified.

This Electronic Signature Policy assumes that the reader knows the concepts of PKI, certificate and electronic signature; otherwise, the reader is recommended to learn the above concepts before continuing to read this document.

1.1 Purpose of the document

This policy represents the set of criteria assumed by ANF Certification Authority (hereinafter, ANF AC) in relation to transactions that have been electronically signed using an electronic certificate issued by one of the ANF AC hierarchies.

In accordance with the provisions of Law 59/2003, of December 19, on electronic signature (hereinafter, LFE) Art.18.b) .2 this document informs of the mechanisms that ANF AC makes available to its subscribers for guarantee the reliability of the electronic signature of a document over time.

1.2 Legal definition of the electronic signature

The Law 59/2003, of December 19, on electronic signature (hereinafter, LFE), and the Regulation (EU) 910/2014 of the European Parliament and of the Council, define three signature concepts:

Electronic signature:

"It is the set of data in electronic form, consigned together with others or associated with them, which can be used as a means of identifying the signer".

Advanced electronic signature:
"It is the electronic signature that allows the signer to be identified and to detect any subsequent change in the signed data, which is uniquely linked to the signer and to the data to which it refers and which has been created by means that the signer can maintain under his exclusive control".

Recognized / qualified electronic signature:
"It is the advanced electronic signature based on a recognized certificate and generated by a secure signature creation device"

For an electronic signature to be considered an advanced electronic signature, the following requirements are inferred:

Identity:
It guarantees the identity of the signer in a unique way.
Integrity:
It guarantees that the content of a data message has remained complete and unaltered, regardless of the changes that the medium that contains it may have undergone as a result of the communication, filing or presentation process.
I do not repudiate:
It is the guarantee that messages cannot be denied in a telematic communication.

The requirements and use of recognized certificates, and the classification of the devices that contain them, are detailed in the Declaration of Certification Practices and in the Certification Policies of ANF AC.

1.3 Document identification

For the development of its content, the following technical specifications have been taken into account:

Document name	Electronic signature policy
Version	1.3
Policy status	APPROVED
Document / OID reference	1.3.6.1.4.1.18332.27.1.1
Publication date	June 1, 2016
Expiration date	Non applicable
Related DPC	Certification Practice Statement (DPC) of ANF AC
Location	https://www.anf.es/documentos

1.4 References

For the development of its content, the following technical specifications have been taken into account:

ETSI TS 101 733, v.1.6.3, v1.7.4, v.1.8.1 and 2.2.1., Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES);
ETSI TS 103 173, v.2.1.1., Electronic Signatures and Infrastructures (ESI); CAdES Baseline profile. Defines a profile of CAdES signatures (advanced signatures built on CMS signatures) suitable for use within the scope of the European Services Directive, by the national authorities of the EU member states;

ETSI TS 119 124- (5 pts), v.1.1.1., Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability;
ETSI TS 101 903, v.1.2.2, v.1.3.2, and 1.4.1., Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES);
ETSI TS 103 171, v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES Baseline profile. Defines the profile of XAdES signatures suitable for use within the scope of the European Services Directive, by the national authorities of the EU member states;
ETSI TS 119 134- (5 pts), v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability;
ETSI TS 103 174, v.2.1.1., Electronic Signatures and Infrastructures (ESI); ASiC Baseline profile. Defines an ASiC container profile (Associated Signatures Container: container that encompasses in a single package a set of electronic documents and a set of XAdES or CAdES electronic signatures on one, several or all documents) convenient to be used in the field of European Directive on Services, by the national authorities of the EU member states;

ETSI TS 102 778-3, v.1.2.1., Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview, Part 2: PAdES Basic;
ETSI TS 103 172, v.2.1.1., Electronic Signatures and Infrastructures (ESI); XAdES Baseline profile. Defines a profile of PAdES signatures (advanced signatures for PDF documents) suitable for use within the scope of the European Services Directive, by the national authorities of the EU member states;

ETSI TS 119 144- (5 pts), v.2.1.1., Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability;
ETSI TS 102 176-1 V2.0.0., Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; Part 1: Hash functions and asymmetric algorithms;
ETSI TS 102 023, v.1.2.1 and v.1.2.2., Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities;
ETSI TS 101 861 v.1.3.1., Time stamping profile.
ETSI TR 102 038, v.1.1.1., Electronic Signatures and Infrastructures (SEI); XML Format for signature policies.

ETSI TR 102 041, v.1.1.1., Electronic Signatures and Infrastructures (SEI); Signature policies report.

ETSI TR 102 045, v.1.1.1., Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
ETSI TR 102 272, v.1.1.1., Electronic Signatures and Infrastructures (SEI); ASN.1 Format for signature policies.
ETSI TS 103 174, v.2.2.1., Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile

ETSI TS 102 918, v.1.1.1., Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)

ETSI TS 101 862 (*Qualified Certificate Profile). It is defined in the rules*EN 319 412-1, EN 319 412-5)

ETSI TS 101 533, Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management

IETF RFC 6960, X.509, Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.

IETF RFC 3125, Electronic Signature Policies.
IETF RFC 3161. Updated by RFC 5816, Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP).

IETF RFC 5280, RFC 4325 and RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
IETF RFC 5652, RFC 4853 and RFC 5652, Cryptographic Message Syntax (CMS).
ITU-T Recommendation X.680 (1997), Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.
ISO 32000-1: 2008, v.1.7., PDF (Portable Document Format).

Likewise, it has been considered as applicable basic regulations:

Regulation (EU) 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC. Law 59/2003, of December 19, on Electronic Signature.

Law 11/2007, of June 22, on Electronic Access of Citizens to Public Services. Law 56/2007 or Law for the Promotion of the Information Society.
Royal Decree 1671/2009, of November 6, which partially develops Law 11/2007, of June 22, on Electronic Access of Citizens to Public Services.
Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration.
Royal Decree 4/2010, of January 8, which regulates the National Interoperability Scheme in the Field of Electronic Administration.
Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016 regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which it is repealed Directive 95/46 / EC (General Data Protection Regulation)

Organic Law 15/1999, of December 13, on the Protection of Personal Data.
Royal Decree 1720/2007, of December 21, approving the Regulations for the Development of Organic Law 15/1999, of December 13, on the Protection of Personal Data.

2 Scope of the signature policy

This document proposes an electronic signature policy that details the general conditions associated with them.

For its unique identification, the signature policy will be identified with a unique identifier that will be OID: **1.3.6.1.4.1.18332.27.1.1.** This must be included in the electronic signature, using the corresponding field to identify the framework policy and the general and specific conditions of application for its validation.

This signature policy is available in a readable format, so that it can be applied in a specific context to comply with the requirements for the creation and validation of electronic signatures.

2.1 User community

The operators involved in the electronic signature creation and validation process are:

Signatory: is the person who owns a signature creation device and who acts in his own name or on behalf of a natural or legal person whom he represents.
Trusting third party: natural or legal person receiving the electronic signature who, prior to trusting it, validates or verifies the electronic signature relying on the conditions required in this document.

Electronic certificate issuer: It is the certification body that issues the electronic certificate on which the creation of the electronic signature is based.
Issuer of the signature policy: It is the entity that is in charge of generating and managing the signature policy document, by which the signer and the third party who trusts in the electronic signature generation and validation processes must be governed.

2.2 Area of application

2.2.1 Permitted Uses

The electronic signature of ANF AC 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 questions in which he has expressed a mention or except, with the commitments 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.

2.2.2 Restricted uses

The scope of application of this Electronic Signature Policy is limited exclusively to electronic signatures that have been generated by means of an electronic signature creation device approved by ANF AC, using an electronic certificate issued by ANF AC.

2.2.3 Prohibited uses

The creation of electronic signatures subject to this Electronic Signature Policy in order to carry out tests without legal value is prohibited.

2.3 Common signature formats

Signature formats are specifications, commonly approved as recognized standards, that define what information an electronic signature must or can contain and how that information is structured.

By way of example, not limiting, the following are specified:

CAdES format (CMS AdvancedElectronicSignatures).
It is the evolution of the first standardized signature format. It has the ability to sign any type of file format (.jpg, .avi, .doc, .exe, etc.). The end result is a * .slc file.
The signed electronic document will therefore be embedded in the signature itself: *Attached / implicit signature:* the two elements (document and signature) are in the same file, and the entire file is signed

According to technical specification ETSI TS 101 733.

XAdES format (XML AdvancedElectronicSignatures).
It can sign any type of file, although it is especially suitable for * .xml files. The final result is a * .xml file

The signed electronic document can be included in the signature, the regulations contemplate the following options:

or *Attached:* although the signature and the document are returned in a single XML file, both are found separated within it and only the part where the document is located is signed.

or *Enveloped:* If a part of the XML document containing it has been signed, it is called a signature *enveloped. Enveloping:*If it contains the signed data within itself it is called a signature

or

enveloping.

According to technical specification ETSI TS 101 903.

PAdES format (PDF AdvancedElectronicSignatures).
It is basically an implementation of PKCS # 7. It can sign PDF files, although it supports XML data. The end result is a * .pdf file.
The signature is embedded in the structure of the document, as specified by the ISO 32000-1: 2008 standard.

PAdES format according to ETSI TS 102 778-3 technical specification.

PDF Sign Format (Interpretable signature of ANF AC).
You can sign any type of file. The final result is a * .pdf file in which the signature is readable based on an interpretable template.
The original document is signed in format **CAdES** and the interpretable signature is signed in Format **PAdES,** all this integrated into a single signature document.

2.3.1 Validity of the electronic signature

In accordance with international standards, the term "long term of the signature - XL" should be established, as long as the requirements that allow **maintain its validity** and the ability to power **verify it over time.**

The verification process aims to determine:

The integrity of the signed data ensuring that they have not undergone any modification. The authenticity of the certificates that have been used to sign, and
Check that the status of the certificate with which it was signed was current at the time of signing.

Once the certificate expires or is revoked, if the signature does not include an Electronic Time Stamp, the signature verification will be **negative,** since it is not possible to determine whether the certificate, when it was used, was valid or not.

To solve this problem, information on the date of its creation must be included in the electronic signature (*Time Stamping)* and the validity of the certificate at that time (*OCSP response signed by the issuing CA of the certificate used).* In this way, the validity of the signature lasts beyond the validity of the certificate.

All signatures created with devices approved by ANF AC, are signatures **AdES (Ad**vanced **AND**lectronic **S**ignature) **XL (**and**X**lying **L**long term = long-term signatures).

The ETSI standards of reference define certain extensions according to the attributes that the electronic signature incorporates, specifically:

Basic Signature

or **AdES - BES,** It is the basic format to satisfy the requirements of the advanced electronic signature. Provides basic authentication and integrity protection, does not provide for “non-repudiation” or long-term validation.

or **AdES - EPES,** It is an AdES-BES that includes information on the signature policy, such as information about the certificate used and the CA that issued it.

AdES T, (T for TimeStamp). It is an AdES-EPES to which a time stamp is added in order to place in time the moment when a document is signed. This is a second signature made by ANF TSA CA (Time Stamp Authority).

AdES C, (C for String). It is an AdES-T to which references are added about the certificates and the validation source used to confirm the validity of the certificate used. This modality is the basis for a long-term verification.

AdES X, (X of eXtendida). It is an AdES-C to which information about the date and time of the data entered in the C extension is added to the references created in the AdES-C model.

AdES XL, (Long-term eXtended XL). It is an AdES-X to which the certificates (only public key) and the validation sources that were used are added. Unlike -C, where only one reference (a pointer) was included, in this format a third signature (OCSP response) made by ANF AC is added. This is used to ensure validation many years after signing even in the case that the CA that issued the certificate, or the validation source (OCSP

Reply or CRL), is no longer available. That is to say,**guarantees long-term off-line validation.**

AdES A, (A for File). This format includes all of the above information but includes meta-information associated with re-signing policies. A re-signed policy establishes an expiration period for the digital signature, and after this time, a re-signing is carried out. The ideal scenario for this signature format are those documents whose validity is very high: 15, 20, 50 years, etc.

2.3.2 Attributes of signature formats

The complete basic structure of each signature format is published in http://www.anf.es.

The especially relevant information according to the signature format is:

2.3.2.1 XAdES format

The version of XAdES. The identifier of the XAdES version that has been followed to build the signature will be indicated in the tags.

The following tags within the field ***SignedProperties:***

SigningTime: indicates the date and time. This label is only included if the signature has a Digital Time Stamp.

SigningCertificate: It contains references to the certificates and security algorithms used for each certificate.

SignaturePolicyIdentifier: identifies the signature policy on which the electronic signature generation process is based.
DataObjectFormat: defines the format of the original document.
SignatureProductionPlace: defines the geographic location where the document was signed.

SignerRole: defines the role of the person in the electronic signature. At least one of these ClaimedRoles or CertifiedRoles elements must be present in this field.

or In the case of its use in an invoice in eInvoice format, it must contain one of the following values in the ClaimedRoles field:
"Supplier" or "issuer": when the signature is made by the issuer.
"Customer" or "receiver": when the signature is made by the receiver.
"Third party" or "third party": when the signature is made by a person or entity other than the issuer or receiver.

or In the case of using attribute certificates to certify the role of the signer, the CertifiedRoles field will contain the base-64 encoding of one or more attributes of the signer's certificates.

CommitmentTypeIndication: defines the action of the signer on the signed document (approves it, informs it, receives it, certifies it, ...)
AllDataObjectsTimeStamp: contains a time stamp, calculated before the signature generation, on all the elements contained in *Reference.*
IndividualDataObjectsTimeStamp: contains a time stamp, calculated before the signature generation, on some of the elements contained in *Reference.*
The label **CounterSignature:** endorsement of the electronic signature and that can be included in the field *UnsignedProperties.* The following signatures, whether serial or parallel, will be added as indicated by the XAdES standard, according to the ETSI TS 101 903 v1.4.2 document (admitting implementations according to v1.2.2 and later).

Unsigned properties of the XAdES-C mode.

CompleteCertificateRefs A containing references to all certificates in the chain of trust required to verify the signature, except the signing certificate.
CompleteRevocationRefs It contains references to the CRLs and / or OCSP responses used in the verification of the certificates.

In the case that you want to incorporate this validation information into the signature, it is recommended to use the XAdES-X format, which adds a time stamp to the previous information.

The XAdES-XL format, in addition to the information included in XAdES-X, includes two new unsigned properties.

CertificateValues.
RevocationValues.

These properties allow including not only the references to the validation information but also the complete chain of trust and the CRL or OCSP response obtained in the validation.

2.3.2.2 CAdES format

Main labels that can be included in the signature document:

Content-type: specifies the type of content to be signed. It is a mandatory label according to the CAdES standard.
Message-digest: identifies the encryption of the content *signed OCTET STRING* on *encapContentInfo.* It is a mandatory label according to the CAdES standard.
ESS signing-certificate or **ESS signing-certificate-v2:** Allows the use of SHA-1 (only for ESS signing-certificate) and the SHA-2 family of algorithms as the security algorithm. It is a mandatory label according to the CAdES standard.
Signing-time: indicates the date and time of the signature. This label is only included if the signature has a Digital Time Stamp.
SignaturePolicyIdentifier: indicates the signature policy on which the generation of the electronic signature will be based. The document must include the reference (OID) to the particular signature policy applied and the fingerprint of the corresponding signature policy document and the algorithm used, in the element *SigPolicyHash* of the corresponding signature policy document and the algorithm used, in the element *SigPolicyHash,* so that the verifier can verify, calculating in turn this value, that the signature is generated according to the same signature policy that will be used for its validation.

Content-hints: describes the format of the original document.
Content-reference: it can be used as a way of relating a reply to the original message to which it refers.

Content-identifier: contains an identifier that can be used in the above attribute.
Commitment-type-indication: indicates the action of the signer on the signed document (approves it, informs it, receives it, certifies it ...).
Signer-location: It allows to indicate the geographical place where the document was signed. At least one of these items *ClaimedRoles* or *Certified Roles* must be present on this label.

Signer-attributes: indicates the role of the person in the electronic signature.
Content-time-stamp: It allows a time stamp, before the generation of the signature, on the data to be signed, to be incorporated with the signed information.
CounterSignature, endorsement of the electronic signature. The following signatures will be added according to the CAdES standard, according to the ETSI TS 101 733 v2.2.1 document (admitting implementations according to v1.6.3 and later).

Within the CAdES signature format, the CAdES-C extended format incorporates two attributes:

complete-certificate-references A containing references to all the certificates in the chain of trust required to verify the signature.
complete-revocation-references It contains references to the CRLs and / or OCSP responses used in the signature verification.

The CAdES-X Long format, in addition to the information included in CAdES-C, includes two new attributes **certificate-values** and **revocation-values** They include not only the references to the validation information, but also the complete chain of trust and the CRL or OCSP response obtained in the validation.

It is recommended to use the following formats:

In the case that the validation is carried out through OCSP query: to the CAdES-X Long type 1 or CAdES-X Long type 2 formats, which add a time stamp to the information included in a CAdES X Long signature.

In this case, the certificate-values and revocation-values attributes will be incorporated since the response to an OCSP query does not take up much space.
In the event that the validation cannot be carried out through OCSP and is carried out by consulting a CRL: to the CAdES-X type 1 or CAdES-X type 2 formats, which include a time stamp to the information included in a CAdES- signature. C, that is, to the references to the CRLs consulted and the certificates of the trust chain, it is not recommended to include the certificate-values and revocation-values attributes as they can be very voluminous.

In the event that the time stamp added to build the long-lived signature is close to expiration, the CAdES-X Long type 1 or CAdES-X Long type 2 signature can be transformed into a CAdES-A signature, adding a stamp file time to signature before

2.3.2.3 PAdES format

Main labels that can be included in the signature document:

Content-type: specifies the type of content to be signed. It is mandatory according to the PAdES standard.

Message-digest: identifies the encryption of the content signed OCTET STRING on encapContentInfo. It is mandatory according to the PAdES standard.
ESS signing-certificate or **ESS signing-certificate-v2** is a tag that allows the use of SHA-1 (only for *ESS signing-certificate)* and the SHA-2 family of algorithms as a security algorithm. It is a mandatory label according to the PAdES standard.
The field will not be specified **Cert** from the dictionary *Signature.*
Signature-policy-identifier: identifies the signature policy on which the electronic signature generation process is based. The document must include the OID of the particular signature policy applied.

The attribute will not be specified **Content-hints.**
The attribute will not be specified **SigningTime.** The signature time must be indicated in the M field in the Signature dictionary, a specific attribute of the PDF.
Commitment-type-indication: this label indicates the action of the signer on the signed document (approves it, informs it, receives it, certifies it, etc.) According to the PAdES standard, it must be indicated in the Reason field of the PDF itself.
Signer-attributes: indicates the role of the person in the electronic signature. At least one of these ClaimedRoles or CertifiedRoles elements must be present in this field.
Content-time-stamp: It allows a time stamp, before the generation of the signature, on the data to be signed, to be incorporated with the signed information.
For the place of signature, the entrance will be used **Location** in the signature dictionary, instead of the element *signer-location* mentioned in the CAdES heading.

Attribute **Counter-Signature,** endorsement of the electronic signature, it is not allowed in this type of signatures. The following signatures will be added according to the PAdES standard, according to the document ETSI TS 102 778-3 and part 4, version 1.1.2.

2.4 Storage of the original signed document

In all signature formats, the signature document can be separate or attached to the original signed document.

When the original document is included in the signature:

or In the case of CAdES these signatures are called implicit signatures.

The Signed Data type is adopted. For the structure of the original signed document, as specified in the CMS (IETF RCF 5652) and CAdES (ETSI TS) standards 101 733), which keeps the original document and the signature in the same file.

The PAdES and PDF Sign formats follow the CAdES model.

or In the case of XAdES firms, the standard establishes different modalities:

enveloping. Include the original document in your signature. In this model, the signature XML structure is the only one in the signature document, and it contains the original signed document internally. In this case, the signed data is in the "Object" node, and if the data is not XML, it is not possible to insert it directly into an XML structure, so it is previously encoded in Base64.

enveloped. An XML content self-contains its own digital signature, inserting it in its own internal node, therefore, unlike in the previous formats, it is not possible to sign content that is not XML.

When the original document is not included in the signature:

or In the CAdES case these signatures are called explicit signatures. The signature and the signed document are different files.

The PAdES and PDF Sign formats follow the CAdES model.

or In the case of XAdES signatures, these signatures are “dettached” mode.

2.5 Creation of the electronic signature

The electronic signature creation devices approved by ANF AC check the validity of the certificate before allowing its use. If the result is that the certificate is not current, the signing process is interrupted.

The electronic signature devices approved by ANF AC meet the requirements established in Art. 24 of the Law 59/2003, of December 19, on electronic signature (hereinafter, LFE), specifically:

1. *Signature creation data is the unique data, such as private cryptographic codes or keys, that the signer uses to create the electronic signature.*

2. *A signature creation device is a computer program or system used to apply the signature creation data.*

3. *A secure signature creation device is a signature creation device that offers at least the following guarantees:*

to) *That the data used for the signature generation can be produced only once and reasonably ensures its secrecy.*

b) *That there is reasonable assurance that the data used to generate the signature cannot be derived from the signature verification or from the signature itself and from*

that the signature is protected against forgery with existing technology at all times.

c) *That the signature creation data can be reliably protected by the signer against its use by third parties.*

d) *That the device used does not alter the data or the document to be signed, nor does it prevent it from being shown to the signer before the signing process.*

The list of approved devices, their technical specifications and qualification are published in http://www.anf.es

ANF AC is a qualified provider of trust services, which issues recognized electronic certificates. The creation of a recognized / qualified electronic signature requires:

Have been created with a recognized / qualified certificate, and
Have used a secure / qualified signature creation device.

2.6 Verification of the electronic signature

To verify the electronic signature, an electronic signature verification device approved by ANF AC must be used.

The electronic signature verification devices approved by ANF AC meet the requirements established in Art. 25 of Law 59/2003, of December 19, on electronic signature (hereinafter, LFE), specifically:

1. *Signature verification data is the data, such as public cryptographic codes or keys, that are used to verify the electronic signature.*
2. *A signature verification device is a computer program or system used to apply signature verification data.*

3. *The electronic signature verification devices will guarantee, whenever technically possible, that the verification process of an electronic signature satisfies, at least, the following requirements:*

to) *That the data used to verify the signature correspond to the data shown to the person who verifies the signature.*
b) *That the signature is reliably verified and the result of that verification is correctly presented.*

c) *That the person who verifies the electronic signature can, if necessary, reliably establish the content of the signed data and detect whether they have been modified.*
d) *That both the identity of the signer or, where appropriate, the use of a pseudonym is clearly shown, as well as the result of the verification.*
and) *That the authenticity and validity of the corresponding electronic certificate are reliably verified.*

F) *That any change related to your security can be detected.*
Four. *Likewise, the data referring to the verification of the signature, such as the moment in which it occurs or a verification of the validity of the electronic certificate at that moment, may be stored by the person who verifies the electronic signature or by trusted third parties. .*

The list of approved devices, their technical specifications and qualification are found published in http://www.anf.es

2.7 Cryptographic elements

For generic security environments in accordance with the technical specifications ETSI TS 102 176-1 on "Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature ". In addition, the criteria that, in this regard, have been adopted in the National Security Scheme, developed from article 42 of Law 11/2007, by Royal Decree
3/2010, of November 6.

Any of the following algorithms are allowed:

Hash (Digestion), SHA-2withRSA (SHA224withRSA, SHA256withRSA, SHA384withRSA, SHA512withRSA)
Encryption, RSA

For high security environments, the criteria of the National Cryptological Center, CCN, will be taken into account, applying the revised recommendations of CCN-STIC 405. Likewise, the recommendation CCN-STIC 807 ("Employment Cryptography in the ENS "), as established in the National Security Scheme.

In general, any of the following algorithms can be used for the electronic signature:

RSA / SHA224, RSA / SHA256, RSA / SHA384 and RSA / SHA512 recommended for archiving electronic documents (very long term signatures).

Key lengths will be at least 2048 bits.

ANF AC constantly monitors the news that occurs in the field of cryptography. An updated report is kept of the validity status of the algorithms and key length it uses, which is publicly accessible at http://www.anf.es

The cryptographic surveillance service of ANF AC, takes among other references and security guides the technical specifications ETSI TS 102 176-1 on "Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signature ". And the criteria adopted in the National Security Scheme developed from article 42 of Law 11/2007.

In the event of an algorithm change or extension of the key length, users and trusted third parties have a special re-stamping service that allows the validity of the signatures produced up to that moment. In case of use, the rates published in each
moment.

2.8 Signatories

The following options are contemplated:

Simple signatures. Signature documents of a single signer.
Online signature. It is the multiple signature in which all the signers are at the same level and in which the order in which it is signed does not matter.
Counter-signature or cascading signature. Multiple signature in which the order in which it is signed is important. Each signature must endorse or certify the signature of the previous signer.

3 Electronic signature validation policy

This section specifies the conditions that must be considered by the signer, in the electronic signature generation process, and by the trusted third party, in the signature validation process.

3.1 Period of validity

This Electronic Signature Policy is valid from the date of issue until the publication of a new updated version.

3.2 Common rules

These rules make it possible to establish responsibilities regarding the electronic signature on the person or entity that creates the electronic signature, and the person or entity that verifies it, defining the minimum requirements that must be submitted.

3.2.1 Signer rules

Any electronic signature device approved by ANF AC, gives the signer the possibility of consulting the electronic document before processing its acceptance, even giving him the ability to review mentions or exceptions that will expand or delimit what is expressed in the document to be signed. .

The signer assumes the responsibility of checking whether the electronic document contains dynamic content. If the file to be signed has not been created by the signer, the signer must check its content before entering the signature activation data (PIN), assuming that by signing it, in addition to its acceptance, it expresses the tacit acknowledgment of having previously reviewed it. .

Unless the signer has contracted the Electronic Signatures Conservation Service from ANF AC, it is the signer's responsibility to preserve and safeguard the electronic signature.

3.2.2 Trusting third party rules

The relying party is responsible for verifying the electronic signature before proceeding with its acceptance. To carry out the corresponding validation, you must use a verification device approved by ANF AC.

In addition, the trusting third party, through its own resources, will check the adequacy of the type of electronic certificate used by the signer, as well as the limitations of use outlined in the "key usage", "Extended Key Usage", and those that may be outlined in other extensions of the certificate itself.

The trusting third party, accepting the electronic signature, makes a tacit acceptance of the liability limitations that ANF AC agrees to assume as specified in the body of the certificate itself,
and in its corresponding Certification Policy.

Unless the signer has contracted the Electronic Signatures Conservation Service from ANF AC, it is the signer's responsibility to preserve and safeguard the electronic signature.

3.2.3 Rules for time stamps

The time stamp ensures that the original signed data was generated before a certain date, and determines the moment in which the signer used his certificate to create the electronic signature.

The electronic signature devices approved by ANF AC obtain Electronic Time Stamping from the Time Stamping Units (TSU). The format of the electronic time stamp issued by the TSUs of ANF AC comply with the IETF recommendations, RFC 5816, "Internet X.509 Public Key Infrastructure; Time-StampProtocol (TSP) ", being electronically signed by electronic certificates from ANF AC TSA.

The basic elements that make up a digital time stamp are:

1. Data on the identity of the issuing authority (ANF AC TSA).
2. Sequencer parameters ("previous", "current", and "next" hashes).
3. Unique transaction number.
Four. UTC date and time.
5. The Time Stamping Unit (TSU) signs the TIMEStamping with a certificate issued by ANF TSA CA.

ANF AC has a date and time stamping service, in accordance with ETSI TS 102 023, according to the specifications defined in CPS OID 1.3.6.1.4.1.18332.5.1 of ANF Time Stamping Authority.

3.2.4 OCSP response rules

From the moment the signature is made and the electronic time stamp is stamped, it is, at a minimum, the maximum time for updating the status of the certificate in the OCSP online validation service.

ANF AC OCSP Responders comply with the IETC RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP reference standard. OCSP responses are dated and signed with certificates issued by ANF AC.

The electronic signature devices approved by ANF AC, validate the status of the certificate after the moment the electronic signature is generated, and after the digital time stamp is stamped.

Regarding the precautionary period or grace period, it should be noted that no period is set, considering that the OCSP response corresponds to the actual status of the certificate, at the time set in said status information.

3.2.5 Trust rules for long-lived firms

The CAdES (ETSI TS 101 733), XAdES (ETSI TS 101 903) and PAdES (ETSI TS 101 733) standards contemplate the possibility of incorporating additional information to electronic signatures to guarantee the validity of a signature in the long term, once it has expired. the period of validity of the certificate. The method for
Obtaining long-lived signatures is described in the AdES XL and AdES A modalities.

4 Preservation of electronic signatures

ANF AC, except for a specific contract in which this service is assumed, does not store and, therefore, does not assume the responsibility of safeguarding the signature documents generated by its subscribers.

The signatories and trusting third parties must be aware that the verification process of a signature must be able to be repeated years after its generation and with the passage of time, magnetic or optical media can degrade, and without forgetting that technology advances inexorably : the cryptographic components: *Keys and algorithms that are safe today, in the future may be considered obsolete, or even the file format has changed and we will not be able to access the information if we have not saved the necessary applications.*

For all these reasons, it is not enough to obtain an electronic signature that meets the requirements to be classified as a long-term electronic signature, this document must be kept properly, both from the point of view of physical security by storing it in a safe place, but rather In addition, the intrinsic characteristics of this instrument must be taken into account.

Technical security

The proper preservation of long-term electronic signatures requires determining at all times the cryptographic security status of the components used in their creation and, if they are at risk, the signatures must be re-stamped before they are created. keys and associated cryptographic material are vulnerable.

In the case of AdES Signatures, it is recommended to follow the AdES A format.

ANF AC's Electronic Signature Preservation service includes a Re-Stamping service. Through this re-sealing service, previously issued stamps are resealed in any of their modalities. The stamps are generated in binary format following the RFC 3161 standard "*Internet X.509 Public Key Infrastructure Time Stamp Protocols*", Standard defined by the Internet Engineering Task Force (IETF) for the Time Stamp protocol.

For the archiving and management of electronic documents, the electronic signature Preservation service follows the recommendations of the technical guides for the development of the National Scheme of Interoperability as well as that indicated in the ETSI TS 101 533 standard.

5 Signature policy management

This PFE details and completes what is stipulated in the "Certification Practices Statement" (CPS) of the PKI ANF AC.

The maintenance, updating and electronic publication of this document will correspond to the Governing Board of the PKI of ANF AC.

This Electronic Signature Policy is valid from the date of issue until the publication of a new version.

The loss of validity of an Electronic Signature Policy, does not affect the signatures that have been issued prior to their replacement, lasting effects on those signatures that have been issued, subject to that specific policy, within the validity period of the same.

5.1 Publication Procedure

ANF AC publishes this Electronic Signature Policy in its repositories http://www.anf.es