Policy for electronic signature based on certificates issued by the hierarchies of ANF Autoridad de Certificación

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 · Website: www.anf.es/en

Security Level

Public Document

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/en

Index

1 Introduction

ANF Certification Authority (henceforth, ANF AC) is a corporate entity, constituted under Organic Law 1/2002 March 22nd, and written in the Ministry of the Interior with national number 171.443 and company tax code G-63287510.

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-).

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

When signing data, the signatory indicates the acceptance of general conditions and particular conditions applicable to the electronic signature. This acceptance is done by the inclusion in the signature of an OID field. This object identifier specifies a particular electronic signature policy univocally.

If the field corresponding to the electronic signature regulation is absent and no applicable regulations are identified, then it must be assumed that the signature has been generated without any normative restriction, and consequently, that it has not been assigned any specific legal or contractual meaning. It would be a signature that does not explicitly specify any semantics or concrete 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 has been defined in a generic form in the Certification Practices 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 technical standards of reference and current legal standards, specifies details of all those contemplated in the References section of this document.

This Electronic Signature Policy assumes that the reader knows the concepts of PKI, certificate and electronic signature; Otherwise the reader is recommended to be trained in the knowledge of the above mentioned concepts before continuing with the reading of this document.

1.1 Purpose of the document

This policy represents the set of criteria assumed by ANF Autoridad de Certificación (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 Spanish Law 59/2003, of December 19th, on electronic signature (hereinafter, LFE) Art.18.b).2 this document reports on the mechanisms that ANF AC makes available to its subscribers to guarantee the reliability of the electronic signature of a document over time.

1.2 Legal definition of the electronic signature

Spanish Law 59/2003, of December 19th, on electronic signature (hereinafter, LFE), and the Regulation (UE) 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, that can be used as a means of identifying the signatory".

- **Advanced electronic signature**:
  "It is the electronic signature that allows to identify the signatory and to detect any subsequent changes of the signed data, which is linked to the signatory in a unique way and to the data to which it refers and which has been created by means that the signatory can maintain under its 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"

In order for an electronic signature to be considered an advanced electronic signature, the following requirements are inferred:

- **Identity:**
  Guarantees the identity of the signatory in a unique way.
- **Integrity:**
  It ensures that the content of a data message has remained complete and unaltered regardless of the changes that the means containing it may have suffered as a result of the communication, storage or presentation process.
- **Non-repudiation:**
  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 containing them, are detailed in the Certification Practices Statement and the Certification Policies of ANF AC.

1.3 Identification of the document

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

Name of the document	Policy for Electronic Signature
Version	1.3
Policy State	APPROVED
Document Reference / OID	1.3.6.1.4.1.18332.27.1.1
Publication date	June 1st, 2016
Expiration date	Not applicable
Related CPS	Certification Practices Statement (CPS) of ANF AC
Location	https://www.anf.es/en

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 y 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 the CAdES signatures profile (advanced signatures built on CMS signatures) suitable for being used within the scope of the Services European 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, y 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 XAdES signatures profile suitable for being used within the scope of the Services European 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 (Associated Signatures Container: Container that includes in a single package a set of electronic documents and a set of XAdES or CAdES electronic signatures on one, several or all documents) container profile, suitable for being used within the scope of the Services European Directive, 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 PAdES signatures profile (advanced signatures for PDF documents) suitable for being used within the scope of the Services European 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 y 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). Queda definida en las normas* 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. actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 y 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 basic applicable normative:

- Regulation (UE) 910/2014 of the European Parliament and of the Council of July 23rd, 2014, on electronic identification and trustworthy services for electronic transactions in the internal market and repealing Directive 1999/93/CE.
- Spanish Law 59/2003, of December 19th, on Electronic Signature.
- Spanish Law 11/2007, of June 22nd, on Electronic Access of Citizens to Public Services.
- Spanish Law 56/2007 or Law for the Impulse of the Information Society.
- Spanish Royal Decree 1671/2009, of November 6th, partially developing Spanish Law 11/2007, of June 22nd, on Electronic Access of Citizens to Public Services.
- Spanish Royal Decree 3/2010, of January 8th, which regulates the Security National Scheme in the field of Electronic Administration.
- Spanish Royal Decree 4/2010, of January 8th, which regulates the National Scheme of Interoperability in the Field of Electronic Administration.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/ EC (General Data Protection Regulation)
- Spanish Organic Law 15/1999, of December 13, on the Protection of Personal Data.
- Spanish Royal Decree 1720/2007 of December 21st, approving the Regulation of Development of Spanish 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 detailing the general conditions associated with them.

For univocal 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 policy, framework and the general and specific conditions of application for its validation.

The present signature policy is available in a readable format, so that they can be applied in a specific context to comply with the requirements of creation and validation of electronic signature.

2.1 Users Community

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

- **Signatory:** Is the person who has a signature creation device and acts on his own behalf or on behalf of a natural or legal person to which he represents.
- **Relying third party:** natural or legal person receiving the electronic signature that before entrusting it, validates or verifies the electronic signature based on the conditions required in this document.
- **Issuer of the electronic certificate:** is the certification entity issuing the electronic certificate on which the creation of the electronic signature is based.
- **Issuer of the signature policy:** is the entity that is responsible for generating and managing the signature policy document, which governs the signatory and the relying third party on the processes of generation and validation of electronic signature.

2.2 Scope of application

2.2.1 Allowed 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 evidential force and full legal validity, that the signatory agrees, except in those matters in which it has expressed a mention or exception, with the commitments and conditions that are implicitly or explicitly outlined in the signed data.

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

2.2.2 Restricted uses

The scope of application of this Electronic Signature Policy is exclusively limited 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

It is forbidden the creation of electronic signatures subjected to this Electronic Signature Policy in order to perform tests without legal value.

2.3 Common signature formats

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

For purposes of clarification, not limitation, 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 is embedded in the signature itself: *Attached/implicit signature*: the two elements (document and signature) are in the same file, and the whole 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 files *.xml. The end result is a *.xml file.
  The signed electronic document may be included in the signature, the rules include the following options:
    - *Attached*: although the signature and the document are returned in a single XML file both are separated within the same and only the part where the document is found is signed.
    - *Enveloped*: if you have signed a part of the XML document that contains it, it is called an *enveloped* signature.
    - *Enveloping*: if it contains the signed data within itself it is called a *enveloping* signature.

  According to technical specification ETSI TS 101 903.

- **PAdES Format** (PDF AdvancedElectronicSignatures).
  Basically it is an implementation of the 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 document structure itself, as specified by the standard ISO 32000-1:2008.
  PAdES Format according to technical specification ETSI TS 102 778-3.

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

2.3.1 Validity of the electronic signature

According to international standards, the term "long term validity of the signature - XL" must be established, as long as the requirements that **maintain its validity** and the ability **to verify it over time** are met.

The verification process aims to determine:

- The integrity of the signed data ensuring that they have not undergone any modification.
- The authenticity of certificates that have been used to sign, and
- Verify that the status of the certificate with which it was signed was in force at the time of signature.

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

To solve this problem it must be included in the electronic signature the information of the date of its creation (*Time Stamping*) and of the validity of the certificate at that moment (*OCSP response signed by the CA issuing the certificate used*). Thus is achieved that the validity of the signature last beyond the validity of the certificate.

All signatures created with devices approved by ANF AC, are **AdES** (**Ad**vanced **E**lectronic **S**ignature) **XL** (e**X**tended **L**ong term = Long-term signatures**)** signatures.

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

- **Basic Signature**
  - **AdES - BES**, is the basic format to meet the requirements of the advanced electronic signature. Provides basic authentication and integrity protection, it does not contemplate "non-repudiation" or long-term validation.
  - **AdES – EPES**, is an AdES-BES to which is added information about the signature policy, such as information about the certificate used and the CA that issued it.
- **AdES T**, (T of TimeStamp). Is an AdES-EPES to which a time stamp is added in order to place in time the moment in which a document is signed. This is a second signature made by ANF TSA CA (Time Stamp Authority).
- **AdES C**, (C of Chain). Is an AdES-T to which is added references about the certificates and the validation source used to confirm the validity of the certificate used. This mode is the basis for long-term verification.
- **AdES X**, (X of eXtended). Is an AdES-C to which is added information about the date and time of the data entered in the extension C to the references created in the AdES-C model.
- **AdES XL**, (XL of eXtended Long-term). Is an AdES-X to which is added the certificates (only public key) and the validation sources that were used. Unlike the -C, where only a 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 event that the CA that issued the certificate, or the validation source (OCSP Responder or CRL), is no longer available. That is to say, **it guarantees long-term off-line validation**.
- **AdES A**, (A of Archive). This format includes all of the above mentioned information but includes meta-information associated with remittance policies. A policy of reaffirmation establishes a period of expiration of the digital signature, and after this time, it is proceeded to a reaffirmation. 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 the signature formats

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

The particularly relevant information according to the signature format is:

2.3.2.1 XAdES Format

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

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

- **SigningTime:** It 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:** It identifies the signature policy on which the electronic signature generation process is based.
- **DataObjectFormat:** It defines the format of the original document.
- **SignatureProductionPlace**: It defines the geographical place where the document was signed.
- **SignerRole:** It defines the role of the person in the electronic signature. At least one of these elements, ClaimedRoles or CertifiedRoles, must be present in this field.
    - In the case of its use in an invoice in eInvoice format, it must contain one of the following values in the field ClaimedRoles:
        - "supplier": when the signature is performed by the issuer.
        - "customer": When the signature is performed by the receiver.
        - "third party": When the signature is made by a person or entity other than the issuer or receiver.
    - In the case of using certificates of attributes to certify the role of the signatory the field CertifiedRoles will contain the encoding in base-64 of one or more attributes of the signatory certificates.
- **CommitmentTypeIndication:** It defines the action of the signatory on the signed document (approves it, informs it, receives it, certifies it, ...)
- **AllDataObjectsTimeStamp:** Contains a time stamp, calculated before the generation of the signature, 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 which may be included in the *UnsignedProperties* field. The following signatures, whether serial or parallel, will be added as indicated by the XAdES standard, according to the document ETSI TS 101 903 v1.4.2 (being allowed implementations according to v1.2.2 and subsequent).

Unsigned properties of the XAdES-C mode.

- **CompleteCertificateRefs** which contains references to all the certificates in the chain of trust necessary to verify the signature, except the signatory certificate.
- **CompleteRevocationRefs** which contains references to CRLs and/or OCSP responses used in the certificate verification.

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

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

- CertificateValues.
- RevocationValues.

These properties allow to include, not only the references to the validation information but also the complete trust chain 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:** it identifies the encryption of the *signed* content *OCTET STRING* in *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 algorithms family as security algorithm. It is a mandatory label according to the CAdES standard.
- **Signing-time:** Indicates the date and time of signature. This label is only included if the signature has a Digital Time Stamp.
- **SignaturePolicyIdentifier:** it indicates the signature policy on which the generation of the electronic signature will be based. The document must incorporate the reference (OID) to the particular signature policy applied and the digital fingerprint of the corresponding signature policy document and the algorithm used, in the digital element *SigPolicyHash* of the corresponding signature policy document and the algorithm used, in the element *SigPolicyHash*, so that the verifier can verify, in turn, this value, that the signature is generated according to the same signature policy that will be used for validation.
- **Content-hints:** it 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**: it contains an identifier that can be used in the previous attribute.
- **Commitment-type-indication:** it indicates the action of the signatory on the signed document (approves it, informs it, receives it, certifies it...).
- **Signer-location:** it allows to indicate the geographical place where the document has been signed. At least one of these ClaimedRoles or CertifiedRoles elements must be present on this label.
- **Signer-attributes:** it 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 that are going to be signed, to incorporate it with the signed information.
- **CounterSignature**, endorsement of the electronic signature. The following signatures will be added as indicated by the CAdES standard, according to the document ETSI TS 101 733 v2.2.1 (being allowed implementations according to v1.6.3 and subsequent).

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

- **complete-certificate-references** that contains references to all the certificates in the chain of trust necessary to verify the signature.
- **complete-revocation-references** that contains references to the CRLs and/or OCSP responses used in the verification of the signature.

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

It is recommended to use the following formats:

- In case the validation is carried out by 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 validation cannot be performed through OCSP and is performed 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-C signature, that is to say, to the references to queried CRLs and trusted chain certificates , it is not recommended to include the certificate-values and revocation-values attributes as they can be very bulky.

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

2.3.2.3 PAdES Format

Main tags that can be included in the signature document:

- **Content-type:** it specifies the type of content to be signed. It is mandatory according to the PAdES standard.
- **Message-digest:** it identifies the encryption of the signed OCTET STRING content in encapContentInfo. it is mandatory according to the PAdES standard.
- **ESS signing-certificate** or **ESS signing-certificate-v2** it is a label that allows the use of SHA-1 (only for *ESS signing-certificate*) and the SHA-2 algorithms family as security algorithm. It is a mandatory label according to the PAdES standard.
- The **Cert** field of the *Signature* dictionary will not be specified.
- **Signature-policy-identifier:** identifies the signature policy on which the electronic signature generation process is based. The document must incorporate the OID of the applied private signature policy.
- The **Content-hints** attribute will not be specified.
- The **SigningTime** attribute will not be specified. 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 signatory on the signed document (approves it, informs it, receives it, certifies it, etc.). According to the PAdES standard, it must be indicated in the PDF's own Reason field.
- **Signer-attributes:** it indicates the role of the person in the electronic signature. At least one of these items, ClaimedRoles or CertifiedRoles, must be present in this field.
- **Content-time-stamp:** it allows a time stamp, before the generation of the signature, on the data that are going to be signed, to incorporate it with the signed information.
- For the location of the signature, the **Location** entry will be used in the signature dictionary, instead of the signer-location element mentioned in the CAdES.
- The **Counter-Signature** attribute, endorsement of the electronic signature, is not allowed in this type of signatures. The following signatures will be added according to the PAdES standard according to 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 may be separated or attached to the original signed document.

- When the original document is included in the signature:
  - 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 standards CMS (IETF RCF 5652) and CAdES (ETSI TS 101 733), that maintain the original document and the signature in the same file.

    The PAdES and PDF Sign formats follow the CAdES model.
  - In the case of XAdES signatures, the standard establishes different modalities:
    - enveloping. It includes the original document in the signature. In this model the signature XML structure is the only one in the signature document, and it contains internally the signed original document. In this case, the signed data is in the "Object" node, and if the data are not XML, it is not possible to insert it directly into an XML structure, so they are previously encoded in Base64.
    - enveloped. An XML content auto-contains its own digital signature, inserting it in an internal own node, reason why, 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:
  - 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.
  - In the case of XAdES signatures these signatures are "dettached" modality.

2.5 Creation of the electronic signature

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

1. *Signature creation data are the unique data, such as private cryptographic codes or keys, that the signatory uses to create the electronic signature.*
2. *A signature creation device is a computer program or system that is used to apply signature creation data.*
3. *A secure signature creation device is a signature creation device that offers at least the following guarantees:*
   - ***a)*** *That the data used for the generation of a signature can be produced only once and reasonably ensures its secret.*
   - ***b)*** *That there is a reasonable assurance that the data used for signature generation cannot be derived from signature verification or from the signature itself and that the signature is protected against counterfeiting with the existing technology at all times.*
   - ***c)*** *That the signature creation data can be reliably protected by the signatory against its use by third parties.*
   - ***d)*** *That the device used does not alter the data or the document to be signed nor prevents it from being shown to the signatory before the signing process.*

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

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

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

2.6 Verification of the electronic signature

In order 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 comply with the requirements established in Article 25 of Spanish Law 59/2003, of December 19th, on electronic signature (hereinafter LFE), specifically:

1. *Signature verification data are data, such as public cryptographic codes or keys, which 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. *Electronic signature verification devices shall, where technically possible, ensure that the verification process of an electronic signature satisfies at least the following requirements:*
   - ***a)*** *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 verified reliably and the result of that verification is presented correctly.*
   - ***c)*** *That the person who verifies the electronic signature can, if necessary, reliably establish the content of the signed data and detect if they have been modified.*
   - ***d)*** *That both the identity of the signatory or, where appropriate, clearly show the use of a pseudonym, as the result of verification.*
   - ***e)*** *That the authenticity and validity of the corresponding electronic certificate are verified reliably.*
   - ***f)*** *That any changes related to their safety can be detected.*
4. *In addition, data relating to verification of the signature, such as when it occurs or a confirmation of the validity of the electronic certificate at that time, 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 published in http://www.anf.es/en.

2.7 Cryptographic elements

For generic security environments according to ETSI TS 102 176-1 on "Electronic Signatures and Infrastructures (ESI); Algorithms and parameters for secure electronic signature ". In addition, consideration will be given to the criteria adopted in the Security National Scheme, developed from article 42 of Spanish Law 11/2007, by Spanish Royal Decree 3/2010, of November 6th.

It is allowed to use any of the following algorithms:

- 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 and the revised recommendations of the CCN-STIC 405 will be applied. CCN-STIC 807 ("Cryptography of Employment In the ENS "), as established in the Security National Scheme.

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

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

The key lengths shall be at least 2048 bits.

ANF AC keeps a constant follow-up of new developments in the field of cryptography. An updated status report is kept of the algorithms and key length used, publicly accessible in http://www.anf.es/en.

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

In case of a change in algorithm or extension of the key length, trusted users and third parties have a special re-stamping service that allows the validity of the signatures up to that point to be maintained. In case of use the rates published at any time will be applied.

2.8 Signatories

The following options are considered::

- **Simple signatures**. Signature documents of a single signatory.
- **Online signature**. It is the multiple signature in which all the signatories are at the same level and in which it does not matter the order in which it is signed.
- **Counter signature or cascade 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 signatory.

3 Electronic signature validation policy

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

3.1 Validity period

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 allow to establish responsibilities with respect to 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 presented.

3.2.1 Rules of the signatory

Any electronic signature device approved by ANF AC, gives the signatory the possibility to consult the electronic document before processing the acceptance of the same, even granting him the ability to describe mentions or qualifications that will expand or delimit what is expressed in the document to be signed.

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

Unless the signatory has contracted to ANF AC the Service of Conservation of electronic signatures, it is the responsibility of the signatory the conservation and custody of the electronic signature.

3.2.2 Rules of the Relying Third Party

The relying third party is responsible for verifying the electronic signature before proceeding to its acceptance. To carry out the corresponding validation he/she must use a verification device approved by ANF AC.

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

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

Unless the signatory has contracted to ANF AC the Service of Conservation of electronic signatures, it is the responsibility of the signatory the conservation and custody of 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 determine the instant in which the signatory used his certificate to produce the electronic signature.

The electronic signature devices approved by ANF AC, obtain stamping of Electronic Time Stamp of Time Stamping Units (TSU). The electronic time stamp format issued by the ANF TSUs comply with IETF recommendations, RFC 5816, "Internet X.509 Public Key Infrastructure; Time-StampProtocol (TSP) ", being electronically signed by electronic certificates of 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 (hash values " previous ", " present " and " following ").
3. Univocal transaction number.
4. 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 DPC OID 1.3.6.1.4.1.18332.5.1 of ANF Time Stamping Authority.

3.2.4 OCSP Responses rules

From the moment the signature is made and the electronic time stamp is stamped it is, at least, the maximum time to update 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) 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 of generating the electronic signature, and after the time of stamping the digital time stamp.

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

3.2.5 Confidence rules for long-term signatures

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

4 Conservation of electronic signatures

ANF AC, unless specific agreement in which this service is assumed does not store and, therefore, does not assume the responsibility of guarding the signature documents generated by its subscribers.

Signatories and trusted third parties need to be aware that the verification process of a signature must be repeated years after its generation and over time, magnetic or optical media can be degraded, and without forgetting that technology is inexorably advancing : the cryptographic components: *Keys and algorithms that are now safe, in the future can be considered obsolete, or even the format of files has changed and we will not be able to access the information if we have not saved the necessary applications*.

Therefore, it is not sufficient to obtain an electronic signature that meets the requirements to be classified as a long-term validity electronic signature, this document must be adequately preserved, from the point of view of physical security storing it in a safe place, in addition, the intrinsic features of this tool must be taken into account.

Technical security

The proper conservation of long-term validity electronic signatures requires that the cryptographic security status of the components used in its creation to be determined at all times and, in case of risk, a signatures re-stamp must be made before the keys and associated cryptographic material are vulnerable.

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

The service of Conservation of electronic signatures of ANF AC, includes a Re-Stamping service. By this re-stamping service the seals previously issued in any of its modalities are stamped another time. The stamps are generated in binary format following the standard RFC 3161 "*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 storage and management of electronic documents, the Electronic Signature Conservation service follows the recommendations of the technical guides for the development of the National Interoperability Scheme as well as the outlined by the standard of ETSI TS 101 533.

5 Management of the signature policy

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

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

This Electronic Signature Policy is valid from the date of issue to 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, and the effects on those signatures that have been issued being subjected to that policy, within the validity period of the same.

5.1 Publication Procedure

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