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

Index **3**

1 Introduction **4**

2 Object **5**

3 Identification of the document **6**

3.1 Organization managing documentation 7

3.1.1 Contact 7

4 Scope of the signature policy **8**

4.1 Users Community 8

4.2 Supported signature formats 8

4.3 Area of application 8

5 Commitment **9**

6 General and specific conditions for the validation of the electronic signature **10**

7 Electronic Signature Preservation **11**

1 Introduction

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

This document determines the creation and validation of the electronic signature subject to this policy, according to the European technical standards eIDAS, describing the scope and use of the electronic signature with the intention of complying with current legal conditions.

The Public Key Infrastructure (PKI) of ANF AC is administered in accordance with the legal framework of Regulation [EU] 910/2014 of the European Parliament, and with Law 6/2020, of November 11, regulating certain aspects of the trusted electronic services from Spain.

Regarding the electronic signature and the advanced or qualified electronic seal, in accordance with the eIDAS Regulation and with this Policy, the general result of the application of this policy does not change, regardless of whether it is an advanced electronic signature / seal or qualified, provided that it has been prepared using a Qualified Certificate of Signature (QES), or a Qualified Certificate of Electronic Seal (QEseal).

This document is ANF AC's Electronic Signature Policy (hereinafter, PFE). The purpose of this policy is to strengthen confidence in electronically signed acts through certain conditions for a given context.

This Electronic Signature Policy assumes that the reader knows the concepts of PKI, X-509 v3 certificates and electronic signature. Otherwise, the reader is recommended to learn the above concepts before continuing with the reading of this document.

2 Object

When the signer includes the OID 1.3.6.1.4.1.18332.27.1.1 in the electronic signature / electronic seal, it means that the signer establishes that the conditions for its validation and use are those established in this policy.

The use of this object identifier OID 1.3.6.1.4.1.18332.27.1.1. that unequivocally specifies this policy, means that the signer accepts what is established in this document.

If the field corresponding to the electronic signature policy is absent, and there are no commitments, mentions or exceptions, that is, no context applicable to the signature is identified, then it must be assumed that the signature has been generated without any regulatory restriction, consequently, no specific legal or contractual meaning has been assigned to it. It would be a signature that does not expressly 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).

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	1.4
Policy State	APPROVED
Document Reference / OID	1.3.6.1.4.1.18332.27.1.1
Publication date	1st December 2020
Expiration date	1st December 2020
Location	https://www.anf.es/en

The identifier of this Certification Policy will only be changed if there are substantial changes that affect its applicability.

The entry into force of a new version occurs at the time of its publication.

Version	**Changes**	**Approval**	**Publication**
1.3	Technical fixes	01/06/2016	01/06/2016
1.4	Technical fixes	01/12/2020	01/12/2020

Review and Approval		
Checked by:	Álvaro Díaz MCarmen Mateo	November 18th 2020
Approved by:	Junta Rectora de la PKI	November 18th 2020

The body in charge of reviewing and approving this policy, if applicable, is the PKI Governing Board, the highest authority in the ANF AC organization. This policy will be reviewed at least once a year, and whenever changes are required, verifying that it is in harmony with the ANF A Certification Practices Statement and its addendum, especially with the OID 1.3 Validation Policy. 6.1.4.1.18332.56.1.1.

This policy is published on the corporate website of ANF AC in the Spanish and English language versions in the different versions that have been approved, in case of discrepancy, the Spanish language version prevails.

3.1 Organization managing documentation

The Governing Board of the PKI is responsible for the administration of this Policy and the set of certification practices of ANF AC,

Department	Junta Rectora de la PKI (Governing Board of the PKI)
Email	juntapki@anf.es
Address	Paseo de la Castellana 79 – Madrid – 28046 – España
National contact Telephone	902 902 172 (Calls From Spain)
International contact Telephone	+34 933 935 946 (International Calls)

3.1.1 Contact

Legal Department	Mª Carmen Mateo	mcmateo@anf.es
Bussiness Development	Álvaro Díaz	adiaz@anf.es
Technology & Compliance	Pablo Díaz	pablo@anf.es
Data Protection Officer	Yohana Lema	yohana@anf.ac

4 Scope of the signature policy

This electronic signature policy details the general conditions for the generation, validation and conservation of the electronic signature and a list of binary object formats and reference files that must be accepted by the corresponding electronic services.

For its unique identification, the signature policy will be identified with the unique identifier OID: 1.3.6.1.4.1.18332.27.1.1, which must be included in the electronic signature for the signature to be considered subject to the commitment, to the general conditions and application-specific for its validation, determining the conditions that the electronic signature must meet at a certain time according to the applicable version of this document.

4.1 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 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.

4.2 Supported signature formats

The formats of electronic signatures / electronic stamps supported are,

• XAdES - in accordance with ETSI EN 319 132 "XAdES Advanced Electronic Signature Profiles". In any of the modalities: detached, enveloped, enveloping.

• CAdES - in accordance with ETSI EN 319 122 "CAdES Advanced Electronic Signature Profiles". In any of the modalities: implicit or explicit.

• PAdES - in accordance with ETSI EN 319 142 "PAdES Advanced Electronic Signature Profiles". In enveloped mode.

and levels according to the BASELINE base profile,

• XAdES - B - T - LT and LTA

• CAdES - B - T - LT and LTA

• PAdES - B - T - LT and LTA

4.3 Area of application

This electronic signature policy can be used by any natural or legal person who voluntarily wishes to accept it.

5 Commitment

The signatory who includes this electronic signature policy, assumes that the electronic signature that he prepares is intended to be used in a legal and contractual framework, in which he wishes to prove with probative force and full legal validity, that he agrees, except in those issues in which you have expressed mention or exception, with the commitments and conditions that are implicitly or explicitly outlined in the signed data and in the signature document itself.

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.

6 General and specific conditions for the validation of the electronic signature

Before trusting the signed document, trusting third parties must proceed to validate the electronic signature.

To carry out the validation of the electronic signature / electronic seal, the qualified validation service of ANF Certification Authority (ANF AC) must be used, applying the requirements established in the Validation Policy of ANF AC OID 1.3.6.1.4.1. 18332.56.1.1.

7 Electronic Signature Preservation

The long-term preservation of electronic signatures requires determining at all times to guarantee 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 issued. keys and associated cryptographic material are vulnerable.

To determine the cryptographic security status, the guidelines of ETSI TS 119 312 must be followed