Electronic signature and electronic seal policy

of

ANF Certification Authority

Security level

Public Document

Important announcement

This document is the property of ANF Certification Authority

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

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

Web: www.anf.es

Index

Index 3

1 Introduction..... 6

1.1 General description 6

1.2 Commercial domain and applications 7

1.2.1 Scope and limits of the electronic signature policy 7

1.3 Document identification 7

1.3.1 Name and version of the document 7

1.3.2 Document identifier 8

1.3.3 Compliance rules 8

1.3.4 Distribution points 8

1.4 Document management 9

1.4.1 Body responsible for the administration of the document 9

1.4.2 Contact persons 9

1.4.3 Approval procedure 9

1.5 Definitions and abbreviations 10

1.5.1 Definitions..... 10

1.5.2 Abbreviations 12

2 Application Security Practice Statement 14

2.1 Control requirements 16

2.1.1 Personal information..... 16

2.1.2 Electronic signatures 16

2.1.3 Business continuity 17

2.2 Security of the information 17

2.2.1 Security policy..... 17

2.2.2 Network protection 17

2.2.3 Protection of information systems 17

2.2.4 Software and application integrity 17

2.2.5 Security of audit trails 17

2.3 Requirements for the signature creation and validation processes 17

2.3.1 Signature creation processes and systems 17

2.3.2 Signature validation processes and systems, ... 18

2.4 Development and Coding Requirements 19

2.5 General requirements 19

3 Business scope parameters ....twenty

3.1 Related to the signature application processes .... twenty

3.1.1 Workflow (*sequencing and time)* of signatures .... twenty

3.1.2 Data to sign .... twenty

3.1.3 List of signed data and signature .... twenty-one
3.1.4 Target 27
3.1.5 Assignment of responsibility for validation and increase 28
3.2 Related to the signature application processes 29
3.2.1 Legal type of signatures 29
3.2.2 Commitment assumed by the signatory 29
3.2.3 Security level of chronological evidence 31
3.2.4 Signature formalities 33
3.2.5 Longevity and resistance to change 3. 4
3.2.6 Archive 36
3.3 Actors involved in creating / increasing / validating signatures 36
3.3.1 Identity and attributes (roles) of the signers 36
3.3.2 Security level required for the authentication of the signer 37
3.3.3 Signature Creation Devices 37
3.4 Other business parameters 38
3.4.1 Other information that will be associated with the signature 38
3.4.2 Cryptographic components 38
3.4.3 Technological environment 39

4 Technical mechanisms and implementation of standards 41
4.1 Related to the signature application processes 41
4.2 Entry and exit restrictions -creation, augmentation and validation- 44
4.2.1 Entry constraints - generate, increase and validate -..... 44
4.2.2 Exit restrictions to be used when validating signatures 58
4.2.3 Exit restrictions to be used to augment signatures 58

5 Other commercial and legal matters 59
5.1 Consent to accept signatures 59
5.2 Condition to trust electronic signatures 59
5.3 Applicable rates 59
5.4 Financial responsibility 59
5.5 Confidentiality of information 59
5.6 Privacy of personal information 59
5.7 Intellectual Property Rights..... 59
5.8 Representations and warranties 60
5.9 Disclaimers of warranties 60
5.10 Limitations of liability 60
5.11 Compensation 60
5.12 Term and termination 60
5.13 Notices and individual communications with participants 60
5.14 Amendments 60

5.15 Dispute resolution procedures 60
5.16 Applicable law 61
5.17 Compliance with applicable law 61

6 Compliance audit and other evaluations 62
6.1 Compliance audits -scope and frequency- 62

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 the national number 171.443 and NIF G63287510.

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 branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA –Registered Private Enterprise-)

This document is ANF AC's electronic signature policy. This policy determines the general and particular conditions applicable to the electronic signature for its creation, validation and increase.

ANF AC, administers this document in accordance with Regulation [EU] 910/2014 of the European Parliament (eIDAS), and with national legislation.

This policy has a standardized structure in accordance with ETSI TS 119 172-1.

This Electronic Signature Policy assumes that the reader knows the concepts of PKI, X-509 v3 certificates, electronic signature and validation. Otherwise, it is recommended that the reader be trained in the knowledge of the above concepts before making use of the services referred to in this document.

1.1 General Description

Regarding the electronic signature and the electronic seal, advanced or qualified, 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).

The basic functions of the electronic signature (*definition, ITU-T X.509 | ISO / IEC 7488-2)*are:

> Identity. Identify the signer unequivocally.
> Integrity. It guarantees that the content of the signed data object has remained complete and unaltered, any manipulation is detected. (*ITU-T X.509 | ISO / IEC 9594-8)*
> I do not repudiate. It ensures that the signer cannot repudiate what was signed.

The purpose of this policy is to guarantee the full consent and free will of the signer, thereby reinforcing the legal security and efficacy of the signed acts. To this end, this policy establishes certain procedures, conditions for the generation and validation of the signature.

Prior to the act of signing, the signer must have the possibility of verifying the data to be signed and even establishing general and specific conditions applicable to the electronic signature. This policy establishes, among other security measures, requirements like WYSIWYS '*what you see is what you sign*'and contemplates inclusion, if it is

will of the signer, of a signature policy, one or more commitments, mentions and exceptions in a signed field, within the signature or implicitly in the data object to be signed.

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 specific semantics or meaning and, therefore, it will be necessary to derive the meaning of the signature from the context, especially from the semantics of the signed document.

1.2 Commercial domain and applications

1.2.1 Scope and limits of the electronic signature policy

This policy is limited to the creation of an electronic signature / electronic seal, although the obligation of the signer and the third parties who trust to validate it before placing their trust is expressly established, as well as certain aspects of the signature increase (*long-term preservation).*

This document covers the requirements and procedures for the elaboration of electronic signatures and electronic seals that include the submission to this policy through the review of OID 1.3.6.1.4.1.18332.27.1.1.

The requirements for the increase of signatures are detailed in the Policy of the Qualified Service for the Preservation of Qualified Electronic Signatures and the Qualified Service for the Preservation of Qualified Electronic Seals, OID 1.3.6.1.4.1.18332.61.

The requirements for the validation of signatures are detailed in the Policy of the Qualified Validation Service of Qualified Electronic Signatures and Qualified Electronic Seals, OID 1.3.6.1.4.1.18332.56.1.1

These creation, validation and preservation policies can be applicable to any domain of use, eg. *B2B, B2C, Gov2B, Gov2C, Legal / Justice, Financial / Banking, Medicine / Health... etc.*

The electronic signatures subject to this policy can be used to subscribe all types of electronic documents, in accordance with the limitations of use established by current legislation, and the restrictions derived from the Certification Policy to which the electronic certificate used in its creation.

1.3 Document identification

1.3.1 Name and version of the document

Document name	Electronic Signature and Electronic Seal Policy

Version	1.4
Policy status	PASSED
Publication date	December 1, 2020
Approval date	December 1, 2020
Posted in	https://www.anf.es

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

Version	Changes	Approval	Publication
1.3	Technical fixes	06/1/2016	06/1/2016
1.4	Technical fixes	12/1/2020	12/1/2020

Review and approval		
Reviewed by:	Department legal / Responsable of normative compliance	November 18, 2020
Approved by:	PKI Governing Board	November 18, 2020

1.3.2 Document identifier

Document / OID reference	1.3.6.1.4.1.18332.27.1.1

There are no subordinate policies.

1.3.3 Compliance rules

This policy will be reviewed at least once a year, and whenever there are changes that require it.

The version of this policy will only be changed if there are substantial changes that affect its applicability.

1.3.4 Distribution points

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. Can be requested by email or in person.

Web	http://www.anf.es
Email	info@anf.es
Address	Paseo de la Castellana, 79 - Madrid - 28046 - Spain

This policy is available in PDF format (*electronically signed),* and printed on paper.

1.4 Document management

1.4.1 Body responsible for document administration

The body in charge of reviewing and approving this policy, if applicable, is the PKI Governing Board, the highest authority in the organization ANF AC.

Organism	PKI Governing Board
Email	juntapki@anf.es
Address	Paseo de la Castellana, 79 Town Madrid - 28046 - Spain
National contact phone	902 902 172 (*Calls from Spain)*
International contact phone.	(+34) 933 935 946

1.4.2 Contact persons

Legal department	Maricarmen Mateo	mcmateo@anf.es
Business development	Alvaro Diaz	adiaz@anf.es
Technology and regulatory compliance	Pablo Diaz	pablo@anf.es
Data protection officer	Yohana Lema	yohana@anf.ac
Documentation and training	Paula Jordan	paula.jordan@anf.es

1.4.3 Approval procedure

The request for revision of the electronic signature and electronic seal policy is made by the General Directorate of ANF AC to the Governing Board of the PKI. The request will state the reasons for requesting changes or new text inclusions, and will include a proposal for a new text.

The Governing Board of the PKI analyzes the request for review, assessing the need, adequacy and checking that the changes are in harmony with the Declaration of Certification Practices (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1 of ANF AC and your addendum.

1.5 Definitions and abbreviations

1.5.1 Definitions

Acceptance of the signature: technical verification to be carried out on the signature itself or on the attributes of the signature.

Trust anchor: In cryptographic systems with a hierarchical structure, a trust anchor is a certificate authority whose trust is assumed and not derived. In the X.509 architecture, a root certificate would be the trust anchor from which the entire chain of trust derives.

Signature / validation application = suite of utilities that allow the creation of AdES electronic signatures and the validation of electronic signatures and seals (SVA)

Signature validation application: An application that validates a signature against a signature validation policy, and that issues a status indication (that is, the signature's validation status) and a signature validation report. The ANF AC validation application is in compliance with ETSI TS 119 102-1.

Signature increase: process of incorporating certain information into a signature in order to maintain the validity of that signature in the long term.

> NOTE: The increase of signatures is a collateral process to the validation of signatures, that is, the process by which certain material (*e.g. timestamps, validation data, and even file-related material)*
> it is incorporated into signatures to make them more resistant to change or to increase their longevity.

Signature validation client: software component that implements the signature validation protocol to the user.

Electronic signature creation device: A configured computer or computer program that is used to create an electronic signature.

Qualified electronic signature creation device: a qualified device (*QSCD)* that meets the requirements listed in Annex II of the eiDAS Regulation.

Qualified electronic stamp creation device: a device that complies *mutatis mutandis* the requirements listed in Annex II of the eiDAS Regulation.

Secure electronic signature creation device: an electronic signature secure device (*SSCD).*

Signature validation status: one of the following indications: TOTAL-PASS, TOTAL-FAILURE, or UNDETERMINED.

Serial PDF signature: the second (and subsequent) signers of a PDF not only sign the document but also the signature of the previous signer and any modifications that may also have taken place (*for example, when filling out the form).*

Signature validation report: full validation report prepared by the signature validation application. It allows you to inspect the details of the assessments taken during the validation and to investigate the status indications detailed by the validation application. The report prepared by the ANF AC validation service meets the requirements established by ETSI TS 119 102-1 and the report is prepared in accordance with ETSI TS 119 102-2.

Signing PoE: the proof of signature existence is the signature data object which is outlined in the validation report.

Signature validation policy: set of signature validation constraints that are processed by the validation application that determine the result of the validation (PASS, FAIL, or UNDETERMINED).

Qualified validation service provider: SVSP that provides a qualified validation service for qualified electronic stamps and / or qualified validation service for qualified electronic signatures. For the purposes of this Policy, the provider is ANF AC.

Proof of existence: evidence that proves that an object existed at a specific date / time.

EIDAS regulation: Regulation (EU) 910/2014, July 23, 2014, regarding electronic identification and trust services for electronic transactions in the internal market. (eIDAS)

Signature applicability rules: A set of rules, applicable to one or more electronic signatures, that defines the requirements for determining whether a signature is suitable for a particular business or legal purpose.

- The owner of the firm's enforceability rules is usually the relying party and these rules can be shared by a community. Signature applicability rules can be handled by an extension of the service provided by the QSVSP that will offer applicability verification.

Creation restriction (signature): criteria used when creating a digital signature.

Signature validation restriction: technical criteria with which an electronic signature can be validated. ANF AC's validation service follows the specifications of ETSI TS 119 102-1

Certification path: An ordered list of one or more public key certificates, starting with a root CA certificate (*self-signed)* and ends with the public key certificate to be validated. Defined in ITU-T X.509 | ISO / IEC 9594-8.

Validation service: system accessible through a communication network, which validates an electronic signature.

Qualified validation service for qualified electronic stamps: as specified in Regulation (EU) No. 910/2014, Article 40. For the purposes of this Policy, the service is provided by ANF AC.

Qualified validation service for qualified electronic signatures: as specified in Regulation (EU) No. 910/2014], article 33. For the purposes of this Policy, the service is that provided by ANF AC.

Signature validation service server: computer equipment that implements the signature validation protocol and processes the electronic signature / seal validation.

Subscriber: Corresponds to the client, natural or legal person, who hires the validation service and submits signatures and / or electronic seals to validation.

Type of commitment (signature): indication selected by the signer that establishes the exact implication of a signature.

User: Application or human interacting with a signature validation client.

Signature validation: verification and confirmation process that an electronic signature is valid.

Signature validation: verification and confirmation process that a digital signature is technically valid.

Validation of the qualified electronic signature: as specified in article 32 of Regulation (EU) No. 910/2014.

Qualified electronic seal validation: as specified in article 40 of Regulation (EU) No. 910/2014.

Applicability check: verification parameters to determine if a signature conforms to the signature applicability rules can be provided as a complement to the defined signature validation service ETSI TS
119 441. It has a greater scope than the validation specified in the aforementioned ETSI TS-

Signature verification: process of verifying the cryptographic value of a signature using signature verification data.

Checker: entity that wants to validate or verify an electronic signature.

1.5.2 Abbreviations

ANF AC:	ANF Certification Authority.
AV:	Validation Authority.
AC / AC:	Certification Authority. Business
BSP:	scope parameters. List of
CRL:	revocation certificates.
GIVES:	Signature application that includes an interface for the end user. Data
DTBS:	to be signed.
OCSP:	protocol for checking the status of an online certificate. Object
OID:	Identifier.
PCSC:	Qualified Trust Services Provider. proof of
PoE:	existence.
WHAT IS IT:	Qualified electronic signature certificate. Qualified
QEseal:	certificate of electronic seal. Qualified electronic
QSCD:	signature device. Qualified Service of Validation of
QSVS:	signatures / stamps.
QSVSP:	Qualified Provider of Signature / Stamp Validation Services.
QTSP:	Qualified Trust Services Provider.
LoA:	Guarantee level.

SCA:	Signature creation application.
SD:	Signatory's document.
SDO:	Signed data object.
SSCD / HSM:	Cryptographic Security Module certified Common Criteria ISO 15408 EAL 4+ or FIPS PUB 140-2 level 3.
SVA:	Electronic signature and stamp validation application.
SVP:	Signature validation protocol.
SVR:	Signature validation report.
SVS:	Signature validation service.
SVSServ:	Signature validation service server. Trust
TA:	anchor.
TSA:	Time Stamping Authority. Trust
TSP:	Service Provider. Time stamping unit.
TSU:	
VPR:	Signature validation process.
WYSIWYS:	'What you see is what you sign.'
XMP:	eXtensible Metadata Platform.

2 Application Security Practice Statement

ANF AC signature applications have been designed and developed in accordance with the requirements established in this document:

Safe Box ®. Application with end-user shell extension for electronic signature and validation. Critical Access®. Desktop application suite that includes electronic signature and validation. BlackBoxSign®. Signature and validation server. Sign to sign®. Signature and validation workflow. Legal Snap Scan®. Certified digitization service. Remote signing server for centralized certificates.

Creation of electronic signatures / electronic stamps

Electronic signature applications, electronic signature creation and electronic signature creation devices have to use qualified certificates of electronic signature or current electronic seal, to create advanced electronic signatures (AdES) or qualified (QAdES), in accordance with the eIDAS Regulation ,

Article 26. Advanced, must meet the following requirements:

to) be uniquely linked to the signer; allow the

b) identification of the signer;

c) have been created using electronic signature creation data that the signer can use, with a high level of confidence, under his / her exclusive control, and

d) be linked with the data signed by it in such a way that any subsequent modification of the same is detectable.

Article 3. Qualified:

An advanced electronic signature that is created by a Qualified Electronic Signature Creation Device (QSCD -*Qualified Signature Creation Devic*e-) and which is based on a qualified electronic signature certificate.

According to the signature context, the following restrictions will be taken into account:

- *ConstraintsOnCertificateMetadata:*
  This set of restrictions indicates requirements on specific certificates. The semantics are defined as follows:

  - *LegalPersonSignerRequired:* The subject identified in the signer's certificate must be a legal person, expressed as *boolean.*
  - *LegalPersonSignerAllowed:* The subject identified in the signer's certificate can be a legal person, expressed as *boolean.*

And, the set of restrictions ETSI TS 119 172-1 Annex C is assumed, the semantics of which are applied in the field of EU legislation, specifically:

- *EUQualifiedCertificateRequired:* This restriction indicates that the signer's certificate must be a qualified certificate of electronic signature / electronic seal, as defined in the applicable EU legislation; expressed as a *boolean.*
- *EUQualifiedCertificateSigRequired:* This restriction indicates that the signer's certificate requires that the signature be prepared in accordance with the ETSI standards on the matter; expressed as a *boolean.*
- *EUQualifiedCertificateSealRequired:* This restriction indicates that the signer's certificate must be a qualified electronic seal certificate, as defined in applicable EU legislation; expressed as a *boolean.*
- *EUSSCDRequired:* This restriction indicates that the private key corresponding to the public key of the signer's certificate must reside in a secure signature creation device; expressed as a *boolean. EUAdESigRequired:* This
- restriction indicates that the signature must be an advanced electronic signature as specified.
  defined in applicable EU law; expressed as a *boolean. EUAdESealRequired:* This restriction indicates that the
- signature must be an advanced electronic seal as defined in the reference ETSI standards; expressed as a *boolean. EUQSigCDRequired:* This restriction indicates that the private key corresponding to the public key of
- the signer's certificate must reside in a qualified signature creation device (*certified as QSCD);*

  expressed as a *boolean.*
- EUQSealCDRequired: this restriction indicates that the private key corresponding to the public key of the signer's certificate must reside in a qualified stamp creation device (*certified as QSealCD published in accordance with Art. 39 3) eIDAS Regulation);* expressed as a *boolean.*

Certificates can be stored in cryptographic software, or in a physical QSCD device, or in a centralized remote signature service, in which case they must meet the following requirements:

> In the event that the signer has entrusted to a third party the qualified devices for the creation of electronic signatures, the third party must be a qualified provider of trust services in accordance with the provisions of the eIDAS Regulation Annex II 3),
> The certificate used must have been issued with the qualification of qualified, and have been generated in a qualified device for the creation of electronic signature, and
> The device has to use the appropriate procedures and mechanisms to guarantee that the signer has exclusive control over the use of his data to create the electronic signature, and that the use of the device meets the requirements of the qualified electronic signature.

In any of the cases, the electronic signature / electronic seal creation devices must use components whose cryptographic security is in accordance with ETSI TS 119 312.

As established in Art. 29 of the eIDAS Regulation, compliance with the requirements to be considered a qualified signature creation device (QSCD) will be presumed, when there is a certification issued by a European body (*Art. 30).* Therefore, the signature creation device to be qualified as QSCD must be included in the list of qualified devices that have been notified to the European Commission by the Member States under article 31 of Regulation (EU) 910/2014 , published in,

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

A qualified electronic seal creation device is one that meets, mutatis mutandis, the indicated requirements in Annex II of Regulation (EU) 910/2014.

The signing applications will determine if the generation and management of the signature creation data corresponding to the certificate used to sign is a QSCD device, verifying if in the QcStatement extension, it includes the QSCD value.

Long-term electronic preservation of electronic signatures and stamps

In order to ensure long-term preservation of electronic signatures and seals, it is recommended to use a qualified long-term electronic preservation service with the capacity to increase cryptographic security.

Either party may delegate the responsibility for increasing the signature to the qualified service of signature preservation and qualified electronic seals of ANF AC OID 1.3.6.1.4.1.18332.61

Signature validation and electronic seals

To carry out the validation of the electronic signature / electronic seal, a qualified validation service of qualified electronic signatures and seals must be used that is registered in the EU TSL.

Any of the parties may delegate the responsibility of signature validation to the qualified service of signature validation and qualified electronic seals of ANF AC OID 1.3.6.1.4.1.18332.56.1.1.

2.1 Control requirements

2.1.1 Personal data

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.1.2 Electronic signatures

The signature applications, signature creation applications, electronic signature services and, the implementers of electronic signatures subject to this policy, will take into account, whenever possible, that the signatures satisfy the legal requirements that may be enforceable depending on the type. of business in which they intervene. For this they must ensure the quality of the signatures by controlling the following elements:

to) Firing devices used. Certificates that
b) have been used. Qualification of
c) instruments a) and b). Cryptographic
d) signature suite.
and) Desired longevity of electronic signatures. Desired
F) protection characteristics (signature level).
g) Qualification of the attributes obtained from third parties, in relation to point f).

h) Qualified validation prior to placing your trust.

2.1.3 Business continuity

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2 Information security

2.2.1 Security Policy

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2.2 Network protection

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2.3 Protection of information systems

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2.4 Software and application integrity

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.2.5 Security of audit trails

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

2.3 Requirements for the signature creation and validation processes

2.3.1 Signature creation processes and systems

a) Management of the type of data content. The signature application (*GIVES)* It must include a control of the type of data object to be signed, checking:

i. adaptation of the signature format selected with the format of the document to be signed, and warn the
ii. signer (*or prevent)* in case the format of the document to be signed may include macros or links that can show the human eye objects that are not actually signed.

b) Signature attribute viewer.

The signature will show the user the attributes that will be included in the fi rma.

c) The signature creation system manages a time and sequence control process.

d) Includes explicit invocation of signature.

and) Includes signature longevity level selection.

F) Includes authentication procedure and access control to the signature system.

g) Preparation of the data object to be signed (DTBS).

The signer selects the DTBS and the application determines the format, origin and guarantees the integrity, in the event that the signer generates the hash of the document, the application records that the hash has been elaborated by the signer.

h) DTBS representation.

The signer must have the ability to access and view the DTBS before preparing the signature, in the event that the DTBS is not accessible to the human eye, *eg an exe,* the signer is aware. Management of signature creation

i) devices.

In accordance with what is described in section 2 of this document.

j) Protection of communication between the signature creation device and the

SCA. Communication between both systems has to be protected; Cryptographic

k) suite security.

The systems must use cryptographic resources that are in compliance with ETSI TS 119 312.

l) The signature creation process and systems must have the capacity to adapt to the use of the community. To do this, they can offer the possibility of including:

- *commitments*

  That determine the scope of the signature and restrictions (*see section*

- *3.2.2). Target community restrictions*

  This set of constraints identifies the community to which each document and its signature (s) are

  (n) addressed and indicates the requirements in that community.

  E.g. These rules can establish the conditions under which a particular signature can be trusted, or include provisions regarding the expected effectiveness of signatures, where multiple signatures are required.

m) The signature creation devices, if they include a massive signature operation, must include processes and systems that guarantee the security requirements indicated in this section:

BulkSigningRelevance:

This restriction indicates the requirement to reference data signed through automated mechanisms, especially for massive signatures. Or, on the contrary, its prohibition. The values used to express these requirements are:

or mandatedBulkSigning

or forbiddenBulkSigning

ConstraintsOnTheNumberOfDOTBS:

This restriction indicates the requirement to reference the number of data objects that a signature can sign. The semantics to express a possible set of values is defined as follows

minValue {<, ≤, =} x {=, ≥,>} maxValue

2.3.2 Signature validation processes and systems,

The process and system for validating electronic signatures and seals, defined in the Validation Policy of ANF AC OID 1.3.6.1.4.1.18332.56.1.1, must be used. that, among other issues, guarantees:

a) validation rules apply

b) the user has a validation interface;

c) the signature format is checked for appropriateness;

d) the useful life of the signature is verified;

e) Conformance is indicated relative to the validation input / output.

2.4 Development and coding requirements

A policy must be in place that establishes development and coding requirements, in particular with:

1) Security of software development methods,
   As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. and its addendum, in particular what is defined in the OID Software and Hardware Life Cycle Policy: 1.3.6.1.4.1.18332.57.1.1
2) Verification of regulatory compliance and interoperability,
   As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. and its addendum.

2.5 General requirements

Control measures must be in place in relation to:

1) User interface,
   As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. and its addendum, in particular what is defined in the OID Software and Hardware Life Cycle Policy: 1.3.6.1.4.1.18332.57.1.1
2) Intervention with other trusted service providers, as defined in the
   Certification Practices Statement addendum. (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. and his

3) General security measures,
   As defined in the Certification Practice Statement addendum. (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1. and his

3 Business scope parameters

This section covers the rules or requirements established by this policy based on the business scope parameters (BSP), which are:

- parameters mainly related to the application and / or business process for which the implementation of the signature (s) are required;
- parameters mainly influenced by legal provisions associated with the application and / or business context;
- parameters related to the actors involved in the creation / validation of signatures; and
- other signature parameters.

3.1 Related to the signature application processes

ANF AC signature applications have been designed and developed in accordance with the requirements established in this document:

Safe Box ®. Application with end-user shell extension for electronic signature and validation.
Critical Access®. Desktop application suite that includes electronic signature and validation.
BlackBoxSign®. Signature and validation server. Sign to sign®. Signature and validation workflow. Legal Snap Scan®. Certified digitization service. Remote signing server for centralized certificates.

The signature tokens and stores used in the process of creating an electronic signature / seal accepted by this policy are:

All devices qualified with QSCD certification.
All HSM devices (Common Criteria ISO 15408 certificate EAL 4+ level or higher). Token USB Plug and Sign® of ANF AC.
Cryptographic software in compliance with the PKCS # 12 standard. Windows / Mozilla / Linux certificate store.

3.1.1 Workflow (*sequencing and time)* of signatures

This signature policy addresses a set of signatures.

3.1.2 Data to be signed

Signature applications must have the ability to manage the following requirements:

Set of restrictions that establishes which properties should or should not be signed (*ContentRelatedConstraintsAsPartOfSignatureElements):*

- *MandatedSignedQProperties-DataObjetFormat*
  It requires a specific format for the content that the signer signs.
- *MandatedSignedQProperties-content-hints*
  Specific information requirements that is encapsulated in the data object, the set being signed. E.g. *XMP for certified digitization of invoices. MandatedSignedQProperties-content-reference*
-
  To require the incorporation of information, in such a way that it links the request and response of the message in an exchange between two parties, or other forms of links. E.g.*certified delivery. MandatedSignedQProperties-content-identifier*
- *content-identifier*
  To require the presence of a specific value of an identifier that can be used as a signed qualification attribute "content-reference". E.g.*QSCD in the signing of employment contracts.*

This restriction indicates whether all the data or only a part of it has to be signed (*DOTBSAsAWholeOrInParts).* It is defined as follows:

- integer: all data must be signed;
- parts: only certain parts of the data need to be signed. In this case, additional information must be used to express which parts have to be signed.

3.1.3 List of signed data and signature

Signing applications that get the hash of the data objects to be signed and identify all relevant aspects of the data objects to be signed. These aspects include:

1) The nature and format of the data to be signed (*for example, binaries, structured data, XML, PDF document, documents such as Word or ODF, multimedia packages, images, etc.).* The signature format must be appropriate to the format of the data object to be signed. In addition, other crucial aspects must be taken into account, for example, the threat of existence of corruption agents (*any code that changes the display of the data object to be signed: a PHP page or a macro in a word),* or data objects that are impossible to visualize, eg. *an executable * .exe*
   In these cases it is convenient to warn the signer of the inherent risk that these objects entail.
2) The signature applications will use by default the natural signature format according to the syntax of the data. Specific.
   to. XML syntax, XAdES format is used.
   b. PDF syntax, PAdES format is used.
   c. Binary data objects, CAdES format is used.

   However, in certain circumstances, the selection of a signature format not initially considered "the natural choice" could be justified.

3.1.3.1 Signature format and levels to use

The supported electronic signature / electronic stamp formats are:

ETSI EN 319 132 "*XAdES Advanced Electronic Signature Profiles*".
ETSI EN 319 122 "*CAdES Advanced Electronic Signature Profiles*".

ETSI EN 319 142 "*PAdES Advanced Electronic Signature Profiles*".

The levels admitted according to the BASELINE base profile are:

- XAdES - B - T - LT and LTA
- CAdES - B - T - LT and LTA
- PAdES - B - T - LT and LTA

3.1.3.1 Relative location of signatures and signed data objects

Three relative locations of signatures and signed data objects can be distinguished:

- Envelope. The signature contains the signed document,
  In the case of CAdES they are called signatures *implicit,* Y
  in XAdES they are firms *enveloping.*
- Wrapped. The signature included within the signed document,*enveloped.* They can be PAdES or XAdES.
  Regarding CAdES signatures, although they can be embedded within objects whose structure is defined in ASN.1 (*as long as this structure defines fields to embed),* o Within S / MIME messages, neither the CMS nor CAdES specifications define a mechanism for explicitly referring to signed data objects that are external to the signature.
- Separated. The signature is separate from the signed document.
  In the case of CAdES they are called signatures *explicit,* and in XAdES they are firms *detached.*

This policy only supports:

XAdES. In any of the modalities:

or *enveloped*

XAdES signatures can be embedded in XML documents.

or *Enveloping*

XAdES can also wrap the signed data object. When this is a binary object, it is previously encoded to base64, and encapsulated within an element*ds: Object.*

CAdES. In the modality:*implicit.*

CAdES signatures, since they are based on CMS signatures, can wrap the signed data object, encapsulating in the field *encapContentInfo 's eContent.*

PAdES. In the modality:*enveloped.*

The signatures will be PAdES NoXML which, by their very document-centric nature, are embedded within the PDF document they sign.

3.1.3.2 Multiple simultaneous relative positions

In some usage scenarios, highly complex processes are necessary.

XAdES: Due to the referencing mechanism inherited from XML Signature, an XAdES signature can, at the same time, wrap one of the data objects that it signs, and be wrapped by another data object that signs, and separated from another data object that signs.

PAdES-XML-EMB: This mode of PAdES can be, at the same time, wrapped inside a signed XML document and separated from another signed data object.

3.1.3.3 Number of signatures and data objects signed

Possible options:

to. *parallel (or independent) signatures (that is, signatures applied to the exact same data);*

b. *Serial signatures (that is, signatures applied to different data and serialized).* The data object can be a form that will be previously filled in by each signer;

c. *counter-signatures (that is, signatures applied successively to the set of previous signatures, and optionally to the same original data);* or

d. *Sequential / hierarchical (that is, the service subscriber establishes a certain order of signature by which signer 2 cannot sign until signer 1 has signed).* In this scenario, the signature can be serial, counter-signature or a combination of both.

and. Act unit (*that is, several signatories in the same act –moment in time- must sign p.je. dual authentication mode).*

Multiple signatures and data objects. Supported signature formats: CAdES, XAdES and PAdES

i. *Document signed by a single signature:* all three formats allow this situation.

ii. *Document signed by more than one signature.* Depending on the format, the following considerations must be taken into account:

Counter-signatures

The signatures PAdES, CAdES and XAdES allow counter-signature. In all cases, the contra-signatures can in turn be PAdES, CAdES or XAdES signatures respectively.

Serial and parallel signatures

PAdES

- Serial signatures. PAdES-NoXML signs any other PAdES-NoXML signature that is already present in the document when it is created: they are always serial signatures;
- Parallel signatures. PAdES-NoXML do not allow the generation of parallel signatures;
- PAdES XML signatures allow combination of serial and parallel signatures

XAdES

- It is capable of managing any number of signatures that sign an XML document (*Totally or partially),* with any combination of serial and parallel signatures, and without any restriction on the relative location of the signatures and the signed data object.

CAdES

- Parallel signatures: can incorporate signatures as an unsigned attribute, which allows a sequence of countersignatures in one of the parallel signatures. It should be taken into account that CAdES lacks mechanisms to make explicit reference to objects of

signed data and consequently applications must be configured to properly handle each specific combination.

iii. A signature requires signing more than one data object

PAdES

PAdES-NoXML only sign a PDF container. Everything inside the PDF container is signed, but nothing else.

PAdES-XML being XAdES signatures, you can sign more than one data object within the XML content of the PDF container.

PAdES-XML-EMB can sign data objects that are outside the PDF container.

CAdES

They cannot, by themselves, sign more than one data object.

XAdES

Incorporates native mechanisms to sign more than one data object.

3.1.3.4 Electronic time stamps

ETSI EN 319102-1 calls time signatures those that result from incorporating a timestamp token in the basic signature.

The PAdES, CAdES and XAdES signatures provide containers that allow the time stamp token to be included within an electronic signature. Possible modalities:

1) Include one or more timestamp token (s) in the data objects to be signed, before the signature is actually generated. This procedure makes it possible to demonstrate that certain data objects have been generated before a certain point in time.
2) Include within a signature a timestamp made by the signer. This timestamp does not generally deserve the same trust as an electronic timestamp generated by a timestamp service provider. ANF AC applications, except Legal Snap Scan®

   (invoice digitization service in XMP Metadata tax regulations on the matter), does not allow the inclusion of timestamp.
3) Include one or more timestamp tokens within an electronic signature. Each time stamp proves that the signature was generated before the time indicated within the time token. This modality is strongly related to the longevity of electronic signatures *.

A timestamp token has a limited validity period, to protect the signature timestamp token itself, it may be necessary to use another timestamp token to protect the first, which in turn increases the longevity of the signature*see point 3.1.3.7 of this document).*

* *The longevity of a signature is the period of time during which the ability to reassess its validity is ensured. technique. In fact, the first measure within the ETSI electronic signature formats to allow the technical validity of a signature to be reassessed for a period of time that goes beyond the expiration or revocation of any of the certificates within the path of certification of the signer's certificate, and beyond the breaking of any of the algorithms (including summary algorithms) used for its generation, it is the incorporation of a timestamp token in the signature before any of the events occur aforementioned.*

3.1.3.5 Include long-term validation material

ETSI EN 319102-1 names signatures with long-term validation material, those resulting from incorporating validation elements to signatures with time stamps (*AdES Level LT).*

XAdES and CAdES LT level, specify containers for references to validation data. PAdES signatures do not incorporate this type of references, since this format is intended to be an autonomous package in terms of validating a signature in the long term.

PAdES LT allows to incorporate validation material within the PDF object of the DSS dictionary and optionally within the objects of the VRI dictionary (ETSI EN 319 142-2)

The ETSI formats allow you to increase the signature by incorporating the following references:

the sequence of references to the full set of CA certificates used to validate the digital signature up to *(but not including)* the signer's certificate;
the sequence of references to the complete set of revocation data used in the validation of the signer and CA certificates;
references to the full set of certificates required to verify any time stamp token embedded in the signature at the time the unsigned attribute / property encapsulating these references is embedded;

references to the full set of revocation data necessary to verify any timestamp token embedded in the signature at the time the unsigned attribute / property encapsulating these references is embedded;

references to the full set of certificates used to validate attribute certificates or signed assertions, if present;

references to the full set of revocation data used in validating attribute certificates or signed assertions, if present.

The Most PKI systems use two procedures to manage revocation data: CRLs and CRLs.
responses from online certificate status servers, obtained through protocols designed for these purposes, such as the OCSP protocol.

This signing policy requires that the OCSP responses must be signed by the CA that issued the certificate, and the verification must have a full scope of the route in accordance with RFC 6960.

3.1.3.6 Include material to augment long-term validation data

An electronic signature requires that it be reassessed over a period of time that goes far beyond its expiration or revocation and even the lack of availability of state information services (CRL / OCSP). In addition, the signature must be protected in the event of a possible violation of some of the cryptographic algorithms used by stronger algorithms.

ETSI EN 319102-1 for this level of AdES LTA signatures, requires incorporating a qualified time stamp token that covers the content of the signature with long-term validation data.

CAdES, XAdES and PAdES signatures provide means to protect even augmented signatures and consequently to increase their longevity. Requirements:

1) Incorporate any missing validation material into the signature, including previously incorporated timestamp token validation material.
2) Protect all the material necessary to validate the signature (*including signed data objects, even if they are separated from the signature and validation material)* generating a new timestamp token using a stronger digest algorithm if needed. This timestamp token actually provides proof of the existence of the timestamp and at the same time protects its integrity.
3) Incorporate the new timestamp token into the signature encapsulated in a suitable container.

These types of timestamp tokens are known as timestamp tokens for long-term availability and integrity of material validation.

3.1.3.7 Indication of commitment / s assumed by the signer

The CAdES, PAdES and XAdES firms provide mechanisms to indicate the commitment assumed by the signer. Detail of standardized commitments in section 3.2.2 of this document.

3.1.3.8 Protect the indication of the identity of the signer

All electronic signature formats standardized by ETSI, with the exception of PAdES-CMS *, require protecting both the signer's certificate or the signer's certificate summary with the signature itself.

The indication of the identity of the signer must be protected.

* *ETSI EN 319142-2 [i.7], clause 4 for PAdES-CMS does not require the inclusion of ESS-signing-certificate or ESS-signing-certificate-v2*

3.1.3.9 Inclusion of roles and attributes of the signer

The CAdES, PAdES and XAdES signatures provide mechanisms to indicate the role played by the signer, which gives the right to include certain attributes.

Within the scope of this policy, if this indication is included, it contemplates the following options:

a declaration "*certified ",* issued by an attribute authority (*for example, attribute certificate: affirmation signed by an attribute authority that assumes the veracity of the information) *;*
attribute included in the body of the certificate whose responsibility for veracity is assumed by the issuer of the certificate.
or OID 2.5.4.12 Title (T) compliant [RFC 5280]

* *Attribute certificates should not be included within PAdES-CMS signatures (ETSI EN 319 142-2, clause 4.2.1)*

3.1.3.10 Inclusion identifier of the Signature Policy

The CAdES, PAdES and XAdES firms provide mechanisms to incorporate explicit information from the signature that regulate its generation and validation.

3.1.3.11 Inclusion of the indication of the data object format signed

The CAdES, XAdES, and PAdES-XML-EMB digital signatures provide mechanisms for incorporating an indication of the format of the signed data object as signed information.

3.1.3.12 Signature increase -life cycle-

Electronic signatures go through more complex stages than the simple initial generation and validation phase. It is necessary for firms to extend their longevity beyond the validity period of the certificates that have intervened in their creation, and the effective life of the cryptographic components used.

The life cycle of an electronic signature until the moment it is discarded, comprises the following stages: *generation, validation and increase of signature.*

The CAdES, XAdES and PAdES formats satisfy these types of requirements, allowing additional data to be added to the signatures to support their life cycles. The process of incorporating additional data into a generated signature is called signature augmentation.

This additional data can be validation data, that is, data necessary to validate the signature (*e.g. CRL certificates, OCSP responses, etc.),* and can also be data to increase the longevity of signatures (*for example, time stamp tokens as detailed in clause 3.1.3.5 of this document).*

NOTE.- more information in section 3.2.5.1 "Increased longevity and resistance to change".

3.1.3.13 Include references to certificates

Both CAdES and XAdES signatures define containers to include references to:

1) CA certificates within the certification path of the signer's certificate;
2) attribute authority certificates and the certificates within your certification path;
3) assertions signing certificates (*required when signer signs signed assertions)* and the certificates within their certification routes; Y
4) certificates of timestamp tokens already present in the signature at the time of generating these containers, and the certificates within their certification paths.

Each reference contains the summary value calculated in the referenced certificate using a specific summary algorithm and an identifier (*optional).* Relying parties can use the digest value to verify that the retrieved certificate is actually the referenced one.

3.1.4 Objective

This signature policy establishes the following requirements:

1. The signature must be in one of the formats established in section 3.1.3, advanced electronic signatures (AdES) or qualified (QAdES)

2. The signature must have been created using a qualified certificate of signature (QES) or a qualified certificate of electronic seal (QEseal), which is in accordance with the eIDAS Regulation.
3. General condition: the signature must include this policy by including the OID 1.3.6.1.4.1.18332.27.1.1

Description:

The signer makes the signature with full consent and free will, knows and accepts that the signature is intended to be used in a legal framework in which it is desired to prove with evidentiary force and full legal effectiveness that the signer agrees with the signed data , unless you have indicated commitment / s, have noted a mention or exception that may limit the scope of the agreements and conditions that are implicitly or explicitly outlined in the signed data. The electronic signatures generated within the scope of this Electronic Signature Policy can be used to sign all types of electronic documents, in accordance with the limitations of use or requirements established by current legislation,

4. Particular conditions: the signatory can indicate the type of commitment / s that determine the scope of the signature. The type indicated by the signer is specified by a specific OID and is included in the signature. The commitments allowed by this policy are detailed in section 3.2.2.
5. Mentions / exceptions: when necessary, the signer can include a text that is included in the signature. It will be necessary to derive the meaning of the signature from the text written by the signer.

3.1.5 Assignment of responsibility for validation and augmentation

The relying parties, prior to placing their trust in the electronic signature / seal, must carry out the validation process using a qualified electronic signature and seal validation service registered in the EU TSL.

Parties that trust the firm:

- or The signer,
- or Trusting third parties,
- or Automatic processes that corroborate / ratify signed documents, or counter-sign before counter-signing as part of the data flow, or publish signed documents.

Any of the parties may delegate the responsibility of signature validation to the qualified service of signature validation and electronic seals of ANF AC OID 1.3.6.1.4.1.18332.56.1.1.

The validity of the signature is associated with the ability to validate it over time, for this it is necessary to apply techniques to increase cryptographic security. The augmentation of an electronic signature is the process by which certain material (*e.g. timestamps, validation data, etc.)* is incorporated into signatures to make them more resistant to change or to extend their longevity (*re-stamped / re-stamped).*

To carry out a suitable resealing, cryptographic components accepted by ETSI TS 119 312 must be used and in accordance with the ETSI reference standards on the matter (*list of standards in section 3.1.3.1 of this document).*

Any of the parties may delegate the responsibility of increasing the signature in the qualified service of conservation of electronic signatures and long-term electronic seals of ANF AC OID 1.3.6.1.4.1.18332.61.

3.2 Related to the signature application processes

3.2.1 Legal type of signatures

In accordance with Regulation (EU) No. 910/2014 [eIDAS], this signature policy covers the following types of signature:

qualified electronic signature,
advanced electronic signature backed by a qualified signature certificate,
qualified electronic seal,
Advanced electronic seal backed by a qualified electronic seal certificate.

Whenever possible, the signature workflow must take into account the legal requirements that may be required depending on the type of act (*eg employment contracts must be formalized with a qualified electronic signature).*
In addition, it may be the case that certain legal acts cannot be formalized by electronic signature (*e.g. the signing of a deed of purchase and sale of a property)*

The use scenarios are innumerable, the market reality is that only in certain processes the signature application can determine the type of act to be formalized, therefore, the relying parties assume the responsibility of verifying that the type of signature It is the appropriate one and, even if possible, the formalization by means of an electronic signature / stamp.

ANF AC, makes available to its subscribers a free legal support service:

e-mail. mcmateo@anf.es
Phone 902 902 172

3.2.2 Commitment assumed by the signatory

Whenever possible, implementers should identify and describe the expected purpose of each signature and, therefore, the meaning and precise nature of the responsibility assumed by the signer, that is, the type of commitment of each electronic signature according to the business scenario and the flow of signatures. Additionally, signature commitment types can be helpful in avoiding potential ambiguities due to the fact that electronic signatures may not provide contextual information equivalent to that of the paper world, creating uncertainty about the signer's intent.

The general condition corresponding to this policy is included in section "3.1.4 Objectives", with the OID 1.3.6.1.4.1.18332.27.1.1. If one or more of the following particular conditions is specified, and any of them contradicts the general condition, the particular condition prevails over the general condition. If the signer has written any mention or exception, and the text written by the signer shows any contradiction with the condition
general or particular, the mention or exception prevails over the previous ones.

Each type of commitment is expressed by a unique identifier (OID or URI), it can include one or more.

The particular commitments accepted by this policy are:

- Commitments published in ETSI 119 172-1 (*Annex B)*
- Standardized commitments referenced with OID owner of ANF AC.

Particular commitments:

OID 1.2.840.113549.1.9.16.6.1 - proof of origin.

Indicates that the signer acknowledges having created, approved and sent the signed data. The URI of this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin. OID 1.2.840.113549.1.9.16.6.2 - as acknowledgment of receipt.

Indicates that the signer acknowledges having received the content of the signed data; The URI of this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt. OID 1.2.840.113549.1.9.16.6.3 - proof of delivery.

Indicates that the TSP providing this indication has delivered signed data in a mailbox accessible to the recipient of the signed data.

The URI of this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery . OID 1.2.840.113549.1.9.16.6.4 - sender proof.

Indicates that the entity providing that indication has submitted the signed data (but did not necessarily create it).

The URI of this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfSender.

OID 1.2.840.113549.1.9.16.6.5 - approval test.

Indicates that the signer has approved the content of the signed data. The URI of this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfApproval. OID 1.2.840.113549.1.9.16.6.6 - creation test.

It indicates that the signer has created the signed data (but not necessarily approved, nor sent that). The URI of this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfCreation.

Proprietary commitments:

OID 1.3.6.1.4.1.18332.27.1.9 - Credential in an access control.

The signature is intended solely for the authentication of entities in order to leave evidence of the access request made by the signer.

OID 1.3.6.1.4.1.18332.27.1.12 - Intermediate authorization

The signature is intended only as an intermediate approval as part of a decision process; OID 1.3.6.1.4.1.18332.27.1.14 - Seen, read mark.

The signature is intended solely to indicate having reviewed a document;

OID 1.3.6.1.4.1.18332.27.1.15 - Intervention in the certified digitization of an original document.

The signature is intended solely to certify that the signer guarantees that the signed document is a certified copy that fully corresponds to an original .;

OID 1.3.6.1.4.1.18332.27.1.16 - Intervention as a witness.

It indicates that the signature is intended solely to indicate having witnessed the signature of another person on the same document (signed data) who has read the document in its entirety, and has signed it as proof of their compliance with them.

The OID uniquely identifies each particular commitment and its description can even be included in the electronic signature or implicitly in the semantics of the signed data object. If it is included in the electronic signature, it must be outlined in the field "*type of commitment*"As specified in the reference ETSI EN standard.

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 specific semantics or meaning and, therefore, it will be necessary to derive the meaning of the signature from the context, especially from the semantics of the signed document.

Definitions to be used in the inclusion of commitments:

CommitmentTypesRequired:

It establishes the set of values required for the commitment expressed by the signer and if this expression is required to be part of the signature properties. The semantics is:

- **MandatedSignedQProperties-commitment-type-indication:** This restriction indicates whether the expression of the commitment by the signer must be part of the signed qualified properties; expressed as *boolean.*
- **MandatedCommitmentTypeValues:** This restriction indicates the possible values required for the type of commitment to be expressed by the signer. The semantics is defined as follows:
  - or **MatchingValuesIndicator:** how the commitment type values are matched in the signature, against the possible required commitment values. It can have the following values:
    "all" if all values must be met;
    "atLeastOne" if at least one of the values must be met;
    "none" if not all values are met.
  - or **CommitmentTypeValues:** a non-empty commit sequence that reviews type identifiers (OID or URI), associated with its description.

3.2.3 Security level of chronological evidence

Implementers must differentiate:

Timestamp

It is the assignment by electronic means of the date and time to a document. It can be generated by any application, without meeting any legal or technical requirement. It does not offer legal certainty.

It can only be used for technical purposes and when required by a standard (*eg service digitization of invoices in XMP Metadata)*

Qualified Electronic Time Stamp

It offers legal effectiveness. It is prepared according to ETSI technical standards and in accordance with the eIDAS Regulation.

The qualified electronic time stamp certifies the existence of an object in a moment of time, it has a legal presumption of certainty. It must be issued by a Qualified Trust Service Provider (PCSC), accredited for the provision of this service and registered in the EU TSL.

Whenever reliable evidence of time is required, a qualified electronic time stamp must be used, issued by a PCSC registered in the EU TSL as qualified in the provision of the electronic time stamping service.

Signature applications must use (*except applicable legal or fiscal regulation)* qualified electronic time stamps. To determine the qualification of an electronic stamp, the signature application will verify that the stamp is signed by a PCSC that has used a qualified certificate to sign the time stamp (*id-pe-qcStatements = "1.3.6.1.5.5.7.1.3"),* and that includes the OID 0.4.0.19422.1.1 (*id-qcs-pkixQCSyntax-v2 - in accordance with the ETSI EN 319 412-1 standard).* By including this OID, the issuer asserts that the timestamp token is issued as a qualified electronic timestamp according to the eIDAS Regulation (EU).

The qualified electronic time stamp is a required attribute in T, LT and LTA level signatures.

The definitions of how the evidence of time has to be are,

- *MandatedSignedQProperties-signing-time*
  Indication of the time and day on which the signature was generated is required.
- *MandatedSignedQProperties-content-time-stamp*
  Requires a qualified electronic time stamp on all signed data, as part of qualified signed properties.

- *MandatedUnsignedQProperties-signature-time-stamp*
  Requires a qualified electronic time stamp on the signature.
- *MandatedUnsignedQProperties-archival-form*
  It requires a timestamp on the file.

Definitions regarding the level of assurance required are,

LoAOnTimingEvidences:
This set of constraints indicates the level of assurance required (*LoA)* in the evidence of time. The semantics are defined as follows:

- *LoA-on-signing-time*
  This restriction indicates the required LoA in the time signature.
- *LoA-on-content-time-stamp*
  Indicates the required LoA in the content of the timestamp.
- *LoA-on-signature-time-stamp*
  Indicate the required LoA in signing the time stamp.
- *LoA-on-archival-time-stamp*
  Indicates the required LoA in the timestamp file.
- *LoA-on-time-in-OCSP-response*
  Indicates the LoA required in the time expressed in the OCSP response.
- *LoA-on-time-in-CRL*
  Indicates the LoA required in the time expressed in the CRL

3.2.4 Signature formalities

One of the most important characteristics of a signature is the way it is created. Often referred to as "*signing ceremony ",* It is the way in which the signatory's attention is drawn to the meaning of the commitment that is being assumed through the act of signing. The quality of the signing ceremony is directly related to the "*consent and will*"Of the signer.

Implementers should identify requirements on any type of evidence related to free will or intention to sign (*e.g. depending on the importance and significance of the act, 2FA could be used to reinforce the evidence).*
Signature applications need to draw the signer's attention to the importance of the commitment being made when applying their signature creation data. All these requirements are materialized by providing the signer with a suitable signature interface.

Main requirements to consider:

1. In a WYSIWYS environment, "*what you see is what you sign*". Definitions indicating the required measure:

   WYSIWYSRequired

   Indicates the requirement to have a "*what you see is what you sign ";* expressed as a *boolean.*

   WYSIWHBSRequired

   Indicates the requirement to have a "*what you see is what has been signed ";* expressed as a *boolean.*

   ProperAdviceAndInformationRequired

   Indicates if it is required to provide the user (*signer or verifier)* advice and adequate information on the creation of the signature, the application process and on the legal consequences, as well as a user interface that guarantees, as far as possible, a valid legal signature with full guarantees of consent and will; expressed as*boolean. UserInterfaceDesignConstraints*

   Indicates whether it is necessary to design the user interface to meet the warranty requirements expressed in this clause 3.2.4; expressed as*boolean. CorrectValidationAndArchivalProcedures*

   This restriction indicates whether the SCA and SVA should show the relying party (*including the signer)* the correct procedures for validation and archiving of the signature and associated validation data; expressed as a tuple made of a*boolean* and an optional character string.
2. Provide users with adequate advice, information and advice on the application signing process:

   i) adequate advice and information on the signature application process;
   ii) adequate advice and information on legal consequences;
   iii) a user interface that allows meeting the legal requirements regarding the expression of will or intentions of the signers (signature commitments); Y
   iv) design the user interface in a way that ensures a legal signature environment, including:
      Implementation that allows and demonstrates a clear expression of the will to sign and the user's intention to be bound by the signature.
      Implementation allowing and demonstrating informed consent.

Consistency between the use of the appropriate signature creation and the verification data, signature creation device, the data to be signed and the scope and expected purpose of the signature (or the act of signing)

3. Provide users with an environment of "*what you see is what you sign.* "To do this, it is verified that the format is a secure format or, if it is a format that allows macros or includes objects visible to the human eye but that will not be signed, the signer is warned and they are not displayed. In the same way if the data object cannot be reproduced to the human sense (sight or hearing). The signer is recommended to previously review the data object to confirm that it is the data object of interest.
4. In order to avoid uncertainty for the signer or relying parties, the signature application and the validation report include an explicit description that avoids possible ambiguities when the signatures do not provide contextual information equivalent to that of the world of paper.
5. Help information on signature types, levels, and modalities is included.

The definition to use is:

LoAOnLongevityAndResilience: -
This restriction indicates the required LoA on the longevity and strength of the evidence provided by the firm.

ANF AC, makes available to all signatories who submit to this signature policy, a legal support service gratuitous:

e-mail. mcmateo@anf.es
Phone 902 902 172

A qualified service of validation of signatures and electronic seals of ANF AC is made available to all parties that trust the signature.

ANF AC signature creation applications are annually subjected to a compliance audit in order to confirm the adequacy of the protection profiles.

3.2.5 Longevity and resistance to change

The passage of time has two different effects on electronic signatures:

First, the certificates used may expire, have been revoked or even the issuer's validation service may no longer be available;
second, cryptographic algorithms (*also including digestion algorithms - hash summary-),*
they may weaken as cryptanalysis techniques and computing capabilities improve.

Longevity and resilience to change (*understood as such, the resistance of firms to the discovery of weaknesses in their algorithms)* they are, consequently, closely related to each other.

The expected longevity and the resistance to change of the signature so that it is verifiable up to a certain period of time, is closely associated with the "*level*"Of signature in which it has been drawn up, in addition, taking into account whether a signature increase has been applied to it (*re-ringing).*

In the case of signatures according to the Baseline level B format that do not have a signature increase, the longevity period is reduced to the validity time of the certificate used (*expiration or revocation),* and security validity status of the cryptographic components. The validity period can be less than one day.

In the case of signatures that include a qualified electronic time stamp (*level T format)* but it does not have a signature increase, the longevity period extends beyond the validity status of the certificate but is limited to the availability of the OCSP or CRLs service of the certificate issuer, and the security validity status of the cryptographic components. The period of validity can be considered medium term, two years.

In the case of signatures that include a qualified electronic time stamp and verification of the validity status of the certificate (*LT level format)* but it does not have a signature increase, the longevity period extends beyond the validity status of the certificate even if the availability of the OCSP or CRLs service of the certificate issuer has been lost, but it is limited to the validity status of the security of the components cryptographic. The period of validity can be considered long-term, six years.
In the case of signatures that include a qualified electronic time stamp, verification of the validity status of the certificate and are stored in a qualified long-term conservation service (*LTA level format),* the guaranteed longevity period is very long-term, at least 15 years.

The relying parties have to take into account the need for longevity and resilience that the firm must offer in accordance with the scope required according to the business scenario.

3.2.5.1 Increase longevity and resistance to change

CAdES, XAdES and PAdES signatures provide means to protect augmented signatures and consequently to increase their longevity. Steps necessary to carry out the increase:

1) Incorporate any missing validation material into the signature, including missing validation material from any previously embedded timestamp token.
2) Protect all the material necessary to validate the signature (*including signed data objects, even if they are separated from the signature and validation material)* generating a new timestamp token using a stronger digest algorithm if needed. This timestamp token actually provides proof of the existence of all items and at the same time protects their integrity.
3) Incorporate the new timestamp token into the encapsulated signature in a suitable container.

These types of timestamp tokens are known as timestamp tokens for long-term availability and integrity of material validation. At a minimum, these signatures will incorporate all the validation data necessary for their validation and one or more of these types of timestamp tokens. Consequently, these firms will require at least two specific components:

1) Containers for validation data values.
2) Containers for archive timestamp tokens.

The ETSI specifications allow complex attribute / property combinations that can be time-stamped.

The following CAdES, PAdES and XAdES firms incorporate this type of time stamp tokens:

XAdES- LTA signatures,

CAdES- LTA signatures,

PAdES- LTA signatures.

NOTE.- more information in section 3.1.3.13 "Increase of signature -life cycle-".

3.2.6 File

The file is related to the longevity of the signatures, and the parties must take into account the scope of security required according to the business scenario, and legal, fiscal or sector regulations that affect it.

The definition to use is:

ArchivalConstraints

This restriction indicates the requirements regarding the signature file and associated validation data.

Either party can delegate the responsibility of filing documents and signatures in the qualified service of conservation and storage of electronic signatures and long-term electronic seals of ANF AC OID 1.3.6.1.4.1.18332.61.

3.3 Actors involved in creating / augmenting / validating firms

3.3.1 Identity and attributes (roles) of the signers

A signature has no value if it cannot be attributed to the signer. As a general rule, the signature applications outlined in this document use qualified certificates in their creation, therefore, the identity of the signer is obtained from the signature certificate / seal used to sign, which guarantees full legal effectiveness on the identity of the signer.

The qualified certificate used to create the signature is subject to the identification requirements established in the Certification Practice Statement of the certificate issuer, Certification Policy to which the certificate is submitted, to Regulation (EU) 910/2014 (eIDAS), national legislation and ETSI technical standards on the matter.

The signature processes must take into account that in some usage scenarios the attributes that a signer has or the role played by a signer are at least as important as their identity. E.g. *The document must be signed by a certain person (a contract), or it can be sealed by one of the computer applications of one of the departments of an organization (a guarantee), or it must be signed by a doctor (electronic prescription), or associated with a certain hierarchical authority (Commercial Director)*

Implementers must take into account not only the values contained in the certificate, they also have to take into account other requirements, stating the set of attributes, authorities and responsibilities that are associated with each signer, their access rights or authority to sign. on behalf of the organization that intends

represent, etc. The inclusion of attributes or roles implies that you must have a certified accreditation that legally guarantees such mention, eg.

proof that an employee or representative is authorized to transact on a specific security;

proof of authorization of delegation to sign, etc.

The definition to use is:

MandatedSignedQProperties-signer-attributes:

This restriction indicates whether the signer must have a qualification. The attribute is required and the restrictions associated with the attributes are required. This can be expressed as a tuple made from a Boolean associated with a sequence of identifiers that express constraints on the required attributes of the signer. Said restrictions on the attributes or roles of the signer may cover:

- what roles / attributes are required;
- identification of the roles / attributes that need to be certified or present within signed assertions;
- restrictions on the type of roles / attributes; and
- restrictions on role / attribute values.

When necessary, this constraint can be used to express whether an attribute is required and the associated requirements.

3.3.2 Level of security required for the authentication of the signer

Certificates (*electronic signature or electronic seal),* are issued as qualified by a Qualified Trust Service Provider accredited and registered on the EU Trust List.

Implementers must identify what is the level of guarantee required for the authentication of the signer in each signature that will be generated within the business process, that is, what are the expectations in terms of trust that the use scenario requires. *E.g. if 2FA is required, or if there are restrictive measures in terms of time or computer terminal, etc.*

The definition to use is:

NameConstraints:

These restrictions indicate requirements on distinguished names for issued certificates (*p. e.g. to signer, CA, OCSP responders, CRL issuers, Time Stamping Units)* as defined in IETF RFC 5280

3.3.3 Signature creation devices

In accordance with the provisions of the eIDAS Regulation, an "electronic signature creation device" is a piece of equipment or computer program used to create an electronic signature. The signature creation devices recognized by this policy are:

All ANF AC applications and platforms outlined in this document. Specifically:

or Safe Box ®.

or Critical Access ®.

or BlackBoxSign.®

or Legal Snap Scan ®.

or Sign to sign®.

or Remote signing server for centralized certificates.

Signature tokens and stores that are used in the process of creating an electronic signature / seal recognized by this policy:

All devices qualified with QSCD certification. All HSM devices (*Common Criteria ISO 15408 certificate EAL 4+ level or higher).*

Token USB Plug and Sign ® of ANF AC.

Token in cryptographic software with ANF AC middleware and in accordance with the PKCS # 12 standard. Windows / Mozilla / Linux certificate store.

3.4 Other business parameters

3.4.1 Other information to be associated with the signature

No requirements are foreseen in this matter.

3.4.2 Cryptographic components

They have to comply with the provisions of ETSI TS 119 312 "*Cryptographic Suites*"

Implementers will know and follow the guidelines of ETSI TR 119 300 "*Guidance on the use of standards for cryptographic suites*".

The definition to use is:

NameConstraints:

These restrictions indicate requirements on distinguished names for issued certificates,

p. e.g .: to signer, CA, OCSP responders, CRL issuers, Time Stamping Units as defined in IETF RFC 5280

X509CertificateValidationConstraints

This set of restrictions indicates the requirements to carry out the validation process of the certification path according to IETF RFC 5280. These restrictions may be different for different types of certificates (*eg certificates issued to signer, CAs, OCSP responders, CRL issuers, time stamp units).* The semantics are as follows:

SetOfTrustAnchors

This constraint indicates a set of acceptable trust hierarchies (*TA)* as a constraint to the validation process. Such *TA* must be provided in the form of self-signed certificates (*root certificate) (clause 6.1.1 of IETF RFC 5280)* and a time until these trust hierarchies were considered reliable.

Eg: The TA package can be provided in the form of:

- Trust points specified in signature validation policies;
- Trusted CA sets, for example, represented by their root certificates stored in the environment (*like the Windows or Mozilla store);*
- trusted service status lists;
- EU trust lists as defined in eIDAS.

CertificationPath

This restriction indicates a certification path required to be used by the SVA for signature validation. The certificate path has a length 'n' from the trust anchor (*TA)* down to the certificate used to validate a signed object (*for example, the time-stamped certificate).* This restriction may include the path to consider or indicate the need to consider the path provided in the signature, if any.

- *user-initial-policy-set:* this restriction is as described in IETF RFC 5280 clause 6.1.1 point (c).
- *initial-policy-mapping-inhibit:* this restriction is as described in IETF RFC 5280 clause 6.1.1 point (and).
- *initial-explicit-policy:* this restriction is as described in IETF RFC 5280 clause 6.1.1 point (f).
- *initial-any-policy-inhibit:* this restriction is as described in IETF RFC 5280 clause 6.1.1 point (g).
- *initial-permitted-subtrees:* this restriction is as described in IETF RFC 5280 clause 6.1.1 point (h).
- *initial-excluded-subtrees:* This restriction is as described in IETF RFC 5280 clause 6.1.1 point (i).
- *path-length-constraints:* indicates restrictions on the number of CA certificates in a certification path. This may need to define initial values or handle such constraint differently (*for example, ignore it).*

- policy-constraints: This restriction indicates requirements for the certification policies referenced in the certificates. This may need to define initial values for this or handle the constraint differently (*for example, ignore it).* This should also allow the ability to require an end-entity certification policy extension.

3.4.3 Technological environment

The electronic signature applications identified in this policy are functional in Windows operating systems from version 7 and Linux, they are not functional in Apple's Mac OS.

In the case of mobile applications, they are functional in Android and iOS operating systems. Implementers must clearly identify what type (s) of document (s) and what signatures within them will be managed. Depending on the usage scenario, it may require specific services to support these tasks and, consequently, use specific sets of standards.

3.4.3.1 Selection of standards

The formats of electronic signatures / electronic stamps accepted will be in accordance with the standardized structure by,

ETSI EN 319 132-1 and ETSI EN 319 132-2 "*XAdES Advanced Electronic Signature Profiles*". ETSI EN 319 122-1 and ETSI EN 319 122-2 "*CAdES Advanced Electronic Signature Profiles*". ETSI EN 319 142-1 and ETSI EN 319 142-2 "*PAdES Advanced Electronic Signature Profiles*".

Process,

ETSI TS 119 172-1 "Part 1: *Building blocks and table of contents for human readable signature policy documents*"ETSI TS 119 101

"*Policy and security requirements for applications for signature creation and signature validation*"ETSI EN 319 102-1

"*Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation*"ETSI TR 119 001

"*The framework for standardization of signatures; Definitions and abbreviations*"

Time stamps,

ETSI EN 319 422-1 "*Time-stamping protocol and time-stamp token profiles*"

OCSP responses,

RFC 6960

"*Online Certificate Status Protocol - OCSP*

"Certificates X509 v.3,

RFC 5280

"*Online Certificate Status Protocol - OCSP*

"ETSI EN 319 401

"*General Policy Requirements for Trust Service Providers*

"ETSI EN 319 412-5

"*Part 5: QCStatements*"

Cryptographic Suites Procedure,

ETSI TS 119 312

"*Cryptographic Suites*

"ETSI TR 119 300

"*Guidance on the use of standards for cryptographic suites*"

Trusted Services List (TSL)

ETSI TS 119 612 *"Trusted Lists"*

4 Technical mechanisms and implementation of standards

4.1 Related to the signature application processes

Table 1: Signature Policy Statement Summary

Signature Policy Authority: ANF Certification Authority NIF G63287510 **Signature Policy:** Electronic Signature and Electronic Seal Policy OID 1.3.6.1.4.1.18332.27.1.1 **Identifier of the signature (s) in the workflow:** AdES / QAdES signatures			
BSP	**BSP title**	**Statement summary deal**	**Counterpart technical statement**
(to)	Work flow *(sequencing and weather)* of signatures	1. Safe Box®. 2. Critical Access ®. 3. BlackBoxSign®. 4. Sign to Sign®. 5. Remote signature server	1. Application with end-user shell extension for electronic signature and validation. 2. Suite of desktop applications that includes electronic signature and validation. 3. Signature and validation server. 4. Signature and validation workflow. 5. For centralized certificates. In all cases: The use of a current qualified certificate issued by the PCSC registered in the EU TSL is required. the responsibility of obtaining the hash of the data object lies with the signing application of ANF AC.
(b)	Data to sign (*DTBS)*	1. Safe Box®. 2. Critical Access ®. 3. BlackBoxSign®. 4. Sign to Sign®. 5. Remote signature server	1. Application for Windows environment, includes Shell Extension. Developed in Java, it uses CryptoAPI B &, interoperates with ANF AC middlware, and centralized remote signature platforms, credentials and certificates. 2. Windows desktop application. Developed in Java, it uses CryptoAPI B &, interoperates with ANF AC middlware, and centralized remote signature platforms, credentials and certificates. 3. Hybrid platform: *Cloud (docker / S3 bucker) and CPD Java, Python, C ++, PHP (Laravel framework).* Four. Cloud platform developed in PHP (Laravel framework), interoperates with BlackBoxSign®. 5. Hybrid platform: *Cloud (docker / S3 bucker) and CPD Java, Python, C ++, PHP (Laravel framework).*
(c)	Relationship between DTBS and signature / s	Accepted signature / stamp formats AdES / QAdES in accordance with: 1. ETSI EN 319 132 2. ETSI EN 319 122 3. ETSI EN 319 142	Permitted levels according to the BASELINE base profile: 1. XAdES - B - T - LT and LTA 2. CAdES - B - T - LT and LTA 3. PAdES - B - T - LT and LTA Supported signature modalities: 1. XAdES: enveloped or enveloping.

			2. CAdES: implicit. 3. PAdES: enveloped.
(d)	Target community	The community of signers or trusting third parties is not restricted. **General conditions:** The signature is intended to be used in a legal and contractual framework. They can be used to subscribe all kinds of electronic documents, in accordance with the Use limitations established by current legislation, and the restrictions derived from the Certification Policy to which the electronic certificate used in its creation is subject. **Particular conditions:** Commitments are defined under which a certain signature is trusted or include, when it is necessary, provisions relating to the intended effectiveness of the firms.	In all cases, the general conditions and particular conditions are uniquely identified by OID and a description of scope and use is made.
(and)	Assignment responsibility for validation and signature augmentation	Parties that trust the firm: - The signer, - trusting third parties, - automatic processes that corroborate / ratify signed documents, or countersign before counter-sign them as part of the data flow, or they publish documents signed. Before placing your trust, it is required validation of electronic signatures / stamps.	To carry out the validation, the qualified service of signature validation and electronic seals of ANF AC must be used.
(F)	Legal type of signature	In accordance with Regulation (EU) No. 910/2014 [eIDAS]	qualified electronic signature, advanced electronic signature backed by a qualified signature certificate, qualified electronic seal, Advanced electronic seal backed by a qualified electronic seal certificate.
(g)	Commitment assumed by the signer	Each type of commitment and the signature policy itself is expressed as a unique identifier (OID or URI)	The Signature Policy is recorded with the OID 1.3.6.1.4.1.18332.27.1.1, and commitments defined by ETSI TS 119 172-1 ANNEX B and proprietary commitments defined in this document are recognized.

(h)	Security level about the evidence chronological	As defined in the ETSI standards in this matter	1. Verification of condition (OCSP). Certificate validity. 2. Verification of the qualification and suitability of the certified type. 3. Hash generation of the data object, path, name and format. Four. Request to the signer for the data of signature activation. 5. Elaboration of signature. 6. Construction of the firm. Depending on the level of obtaining the OCSP response, and / or TimeStamping.
(i)	Formalities of the firm	Help and adequate security measures when signing process.	1. WYSIWYS environment (What You See Is What You Get). 2. The signer provides: i) advice and information on the application signature process; ii) advice and information on legal consequences; Y iii) a user interface that allows meeting the legal requirements regarding the expression of will or intentions of the signers
(j)	Longevity and resilience to change	The expected longevity and resistance to change of the signature so that it is verifiable up to a period of time determined.	Baseline level B format. The validity period may be less than one day. Baseline level T format. The validity period can be up to 2 years. Baseline format LT level. The period of validity can be considered long-term, six years. Baseline format LTA level. The period of validity can be considered very long-term, at least 15 years.
(k)	Archive	To guarantee the archiving of documents signed is required use a service qualified of conservation and long-term electronic signature and stamp storage.	Requirements included in the Policy for the conservation of signatures and electronic seals of ANF AC, OID 1.3.6.1.4.1.18332.61
(l)	Identity of the signers	The use of qualified identity certificates is required, issued by a Qualified Trust Services Provider accredited for the issuance of said certificates, and registered in the EU Trust List.	Subject to the identification requirements established in the Certification Practice Statement and Certification Policy to which the certificate is submitted. It must include the information required by the eIDAS Regulation, national legislation and ETSI technical standards on the matter.

(m)	Security level required for authentication of signatory	Certificates are required to be Qualified certificates, issued by a Qualified Trust Service Provider accredited for the issuance of said certificates, and registered on the EU Trust List.	In accordance with the eIDAS Regulation, and national legislation.
(n)	Devices signature creation	All QSCD-HSM devices and those listed in section 3.3.3	ANF AC applications and platforms: Safe Box®. Critical Access ®. BlackBoxSign®. Sign to Sign®. Remote signature server Tokens: QSCD devices. HSM devices. USB Plug and Sign token with ANF AC middleware. Token in cryptographic software PKCS # 12 with ANF AC middleware. Windows / Mozilla / Linux certificate store.
(or)	Other information that will be associated with the firm	No requirements are foreseen in this matter.	No requirements are foreseen in this matter.
(p)	Crypto suites	ETSI TS 119 312	ETSI TS 119 312
(q)	Technological environment	operating systems Windows version 7 or higher, and Linux,	They are not functional in Apple OS
Creation / Application Practice Statements signature validation		OID Validation Policy 1.3.6.1.4.1.18332.56.1.1.	OID Validation Policy 1.3.6.1.4.1.18332.56.1.1.
Summary of the signature formats selected according to section 3.1.3.1, which includes details about the format of the signed data, the relative location of the signature and the signed data (i.e. wrapped, enveloping, implicit), the specific attributes of the signature and the expected level of the selected signature format:			

4.2 Entry and Exit Restrictions -creation, augmentation and validation-

4.2.1 Input constraints - generate, augment and validate -

Table 2

Signature Policy Authority: ANF Certification Authority NIF G63287510 **Signature Policy:** Electronic Signature and Electronic Seal Policy OID 1.3.6.1.4.1.18332.27.1.1 **Identifier of the signature (s) in the workflow:** AdES / QAdES signatures							
BSP	**BSP title**	**Summary statement deal**	**Counterpart statement technique**	**Restriction (s)**	**Value of restriction on the creation of the signature (SCA or DA)**	**Value of restriction on increasing of signatures (SCA, SVA or GIVES)**	**Value of restriction on validation of the signature (SVA or DA)**
(to)	Workflow (sequencing & timing) See table 1	see Table 1	see Table 1	**(a) 1. OrderInSequence:** The workflow contemplates multiple possibilities of signature sequence and multiple signers.	AdES / QAdES See section 3.1.1	Politics OID 1.3.6.1.4.1.18332.61	Politics OID 1.3.6.1.4.1.18332.56.1.1
				(a) 2. SequencingNature: Signature characteristics related to sequencing: **(a) 2.1 Mandated-independent:** Independent signatures are defined as signatures applied to the exact same data. This restriction indicates that the firm must necessarily be independent. **(a) 2.2 Mandated-serial:** Serial signatures are defined as signatures applied to different data and serialized. This restriction indicates that the signature is required to be serial. **(a) 2.3 MandatedUnsignedQProperties-counter-signature:** Counter-signatures are defined as signatures applied successively to the set of previous signatures and, optionally, to the same data originals. This restriction indicates that unsigned rated property must be present at the signature.	See section 3.1.1.1		

BSP	BSP title	Summary statement statement deal	Counterpart statement technique	Restriction (s)	Value of restriction on the creation of the signature (SCA or DA)	Value of restriction on increasing of signatures (SCA, SVA or GIVES)	Value of restriction on the validation of the signature (SVA or DA)
				(a) 3. Relevance of time: **(a) 3.1 TimingRelevanceOnSequencing:** This restriction indicates the required relevance of synchronization with respect to the signature sequence. The semantics is defined as follows: - [no] before a certain date, [no] after a certain date, - [no] before a certain period of time, exactly in a - certain amount of time, [no] after a certain period of - time. - **(a) 3.2 TimingRelevanceOnEvidence:** Define how the evidence of time has to be. Specifically: **(a) 3.2.1 MandatedSignedQProperties-signing-time** It requires indication of the time and day on which the signature was generated. Qualified electronic time stamp. **(a) 3.2.2 MandatedSignedQProperties-content-time-stamp** Requires a qualified electronic time stamp on all signed data, as part of qualified signed properties. **(a) 3.2.3 MandatedUnsignedQProperties-signature-time-stamp** Requires a qualified electronic time stamp on the signature. **(a) 3.2.4 MandatedUnsignedQProperties-archival-form** It requires a timestamp on the file.	See section 3.1.1.1 See section 3.2.3		
				(a) 4. MassSigningAcceptable (yes / no): This restriction indicates if the massive signature is accepted with respect to the type of signature. Expressed in boolean.	See section 3.1.1.1		

BSP	BSP title	Summary statement statement deal	Counterpart technique	Restriction (s)	Value of restriction on the creation of the signature (SCA or DA)	Value of restriction on increasing of signatures (SCA, SVA or GIVES)	Value of restriction on the validation of the signature (SVA or DA)
(b) DTBS				**(b) 1. ConstraintOnDTBS:** This restriction indicates requirements on the type of data that the signer must sign.	See section 3.1.1.1		
				(b) 2. ContentRelatedConstraintsAsPartOfSignatureElements: Set of restrictions that establishes which properties should or should not be signed: **(b) 2.1 MandatedSignedQProperties-DataObjetFormat** It requires a specific format for the content that the signer signs. **(b) 2.2 MandatedSignedQProperties-content-hints** Specific information requirements that is encapsulated in the data object, the set being signed. **(b) 2.3 MandatedSignedQProperties-content-reference** To require the incorporation of information, in such a way that it links the request and message response in an exchange between two parties, or other forms of links. **(b) 2.4 MandatedSignedQProperties-content-identifier** To require the presence of a specific value of an identifier that can be used as a signed qualification attribute "contentreference".	See section 3.1.2		
				(b) 3. DOTBSAsAWholeOrInParts: This restriction indicates whether all the data or only a part of it has to be signed. It is defined as follows: - integer: all data must be signed; - Parts: Only certain parts of the data need to be signed. In this case, additional information must be used to express which parts have to be signed. .	See section 3.1.2		

BSP	BSP title	Summary declaration on deal	Counterpart statement technique	Restriction (s)	Value of restriction on the creation of the signature (SCA or DA)	Value of restriction on increasing of signatures (SCA, SVA or GIVES)	Value of restriction on the validation of the signature (SVA or DA)
(c)	Relationship Between DTBS and sign			**(c) 1. BulkSigningRelevance:** This restriction indicates the requirement to reference data signed through automated mechanisms, especially for massive signatures. Or, on the contrary to its prohibition. The values used to express these requirements are: **(c) 1.1 mandatedBulkSigning** **(c) 1.2 forbidden Bulk Signing.**	See section 2.3.1 m)		
				(c) 2. ConstraintsOnTheNumberOfDOTBS: This requirement indicates the number of data objects that a signature can sign. The semantics to express a possible set of values is defined as follows minValue {<, ≤, =} x {=, ≥,>} maxValue	See section 2.3.1 m)		
				(c) 3. SignatureRelativePosition: This requirement indicates the relative position of the signature and the signed data. To express these requirements, they are defined as follows: • implicit; • enveloped; • enveloping	See section 3.1.3.1		
				(c) 4. MandatedSignatureFormat: The required signature format determines the required signature level and format.	See section 3.1.3		
(d)	Managed to community			**(d) 1. TargetedCommunityConstraints:** This set of constraints identifies the community to which each document and its signature (s) is (are) directed and indicates the requirements in that community. EXAMPLE: These rules, for example, can establish the conditions under which a particular signature can be trusted, or include provisions regarding the expected effectiveness of signatures, where multiple signatures are required.	See section 2.3.1		

BSP	BSP title	Summary statement deal	Counterpart and statement technique	Restriction (s)	Value of restriction on the creation of the signature (SCA or DA)	Value of restriction on increasing of signatures (SCA, SVA or GIVES)	Value of restriction on the validation of the signature (SVA or DA)
(and)	Assignment responsibility for validation and increase			**(e) 1. ValidationRequiredBeforeAugmenting:** This restriction indicates whether validation is required before increasing a signature to a higher level, expressed as a Boolean.		Poliethics OID 1.3.6.1.4.1.18332.61	
				(e) 2. AugmentToLevel: This restriction indicates the level of the signature format that must be reached after a signature has been augmented.		Poliethics OID 1.3.6.1.4.1.18332.61	
(F)	Legal type			**(f) 1. ConstraintsOnCertificateMetadata:** This set of restrictions indicates requirements on specific certificates. Semantics is defined as follows: **(f) 1.1. LegalPersonSignerRequired:**The subject identified in the signer's certificate must be a legal person, expressed as a boolean. **(f) 1.2. LegalPersonSignerAllowed:**The subject identified in the signer's certificate can be a legal person, expressed as a boolean. The set of restrictions of Annex C ETSI TS 119 172-1 are assumed, the semantics of which apply to the context of EU legislation.	See section 2		

(g) Commitment type				**(g) 1. CommitmentTypesRequired:** It establishes the set of values required for the commitment expressed by the signer and if this expression is required to be part of the signature properties. The semantics is: **(g) 1.1. MandatedSignedQProperties-commitment-type-indication:**This restriction indicates whether the expression of the commitment by the signer must be part of the signed qualified properties; expressed as*boolean.* **(g) 1.2. MandatedCommitmentTypeValues:**This restriction indicates the possible values required for the type of commitment to be expressed by the signer. The semantics is defined as follows: **MatchingValuesIndicator:** how the commitment type values are matched in the signature, against the possible required commitment values. It can have the following values: "all" if all values must be met; "atLeastOne" if at least one of the values must be met; "none" if not all values are met. **CommitmentTypeValues:** a non-empty commit sequence that reviews type identifiers (OID or URI), associated with its description.	See section 3.2.2		

(h) Level of security synchronization of evidences				**(h) 1. LoAOnTimingEvidences:** This set of constraints indicates the level of assurance required (LoA) in the evidence of time. The semantics are defined as follows: **(h) 1.1. LoA-on-signing-time:**This restriction indicates the required LoA in the time signature. **(h) 1.2. LoA-on-content-time-stamp:**indicates the LoA required in the time stamp content. **(h) 1.3. LoA-on-signature-time-stamp:**indicates the LoA required in signing the time stamp. **(h) 1.4. LoA-on-archival-time-stamp:**indicates the required LoA in the timestamp file. **(h) 1.5. LoA-on-time-in-OCSP-response:**indicates the LoA required in the time expressed in the OCSP response. **(h) 1.6. LoA-on-time-in-CRL:**indicates the LoA required in the time expressed in the CRL.	See section 3.2.3		
(i)	Formalities of signing			**(i) 1. WYSIWYSRequired:** Indicates the requirement to have a "what you see is what you sign"; expressed as a boolean.	See section 3.2.4		

				(i) 2. WYSIWHBSRequired: Indicates the requirement to have a "what you see is what has been signed"; expressed as a boolean.	See section 3.2.4		
				(i) 3. ProperAdviceAndInformationRequired: Indicates whether it is required to provide the user (signer or verifier) advice and adequate information on the creation of the signature, the application process and on the legal consequences, as well as a user interface that guarantees, as far as possible, a valid legal signature with full guarantees of consent and will; expressed as a boolean.	See section 3.2.4		
				(i) 4. UserInterfaceDesignConstraints: Indicates whether it is necessary to design the user interface to meet the warranty requirements expressed in clause 3.2.4; expressed as a boolean.	See section 3.2.4		

BSP	BSP title	Summary statement deal	Counterpart statement technique	Restriction (s)	Value of restriction in the creation of the signature (SCA or GIVES)	Value of restriction on increasing of signatures (SCA, SVA or GIVES)	Value of restriction in the validation of the signature (SVA or GIVES)
				(i) 5. CorrectValidationAndArchivalProcedures: This restriction indicates whether the SCA and SVA should show the relying party (*including the signer)* the correct procedures for validation and archiving of the signature and associated validation data; expressed as a tuple made of a boolean and an optional character string.	See section 3.2.4		
(j)	Longevity and resilience			**(j) 1. LoAOnLongevityAndResilience:** This restriction indicates the required LoA on longevity and strength than the evidence provided by the firm.	See section 3.2.5		
(k)	Archive			**(k) 1. ArchivalConstraints:** This restriction indicates the requirements regarding the signature file and associated validation data.	See section 3.2.6		
(l)	Identity and attributes of role of signatory			**(l) 1. ConstraintsOnCertificateMetadata-LegalPersonSignerRequired:**The The subject identified in the signer's certificate must be a legal person, expressed as a boolean.	See section 2		

				(l) 2. ConstraintsOnCertificateMetadata-LegalPersonSignerAllowed: The subject identified in the signer's certificate can be a legal person, expressed as a boolean.	See section 2		
				(l) 3. MandatedSignedQProperties-signer-attributes: This restriction indicates whether the signer must have a qualification. The attribute is required and the restrictions associated with the attributes are required. This can be expressed as a tuple made from a Boolean associated with a sequence of identifiers that express constraints on the required attributes of the signer. Said restrictions on the attributes or roles of the signer can cover: what roles / attributes are required; identification of the roles / attributes that need to be certified or present within signed assertions; restrictions on the type of roles / attributes; and restrictions on role / attribute values. When necessary this restriction can be used to express whether an attribute is required and the associated requirements.	See section 3.3.1		
				(l) 4. NameConstraints: These restrictions indicate requirements on distinguished names for issued certificates (*p. e.g. to signer, CA, OCSP responders, CRL issuers, Time Stamping Units)* as defined in IETF RFC 5280.	See section 3.3.2		

BSP	**BSP title**	**Summary statement d deal**	**Counterpart statement technique**	**Restriction (s)**	**Value of restriction n in the creation of the signature (SCA or GIVES)**	**Value of restriction on increasing of signatures (SCA, SVA or GIVES)**	**Value of restriction n in the validation of the signature (SVA or GIVES)**
(m) LoA about	authentication of signer			**1. X509CertificateValidationConstraints:** This set of restrictions indicates the requirements to perform the certification path validation process according to IETF RFC 5280. These restrictions may be different for different types of certificates (for example, certificates issued to the signer, to CAs, to OCSP responders, CRL issuers, time stamping units). The semantics are as follows: **(m) 1.1. SetOfTrustAnchors:** This constraint indicates a set of Acceptable Trust Hierarchies (TA) as a constraint for the validation process. Such TAs must be provided in the form of self-signed certificates (root certificate) (clause	See section 3.3.2		

				6.1.1 of IETF RFC 5280) and a time until these trust hierarchies were considered reliable. Eg: The TA package can be provided in the form of: - Trust points specified in signature validation policies; - Trusted CA sets, for example, represented by their root certificates stored in the environment (such as the Windows or Mozilla store); - trusted service status lists; - EU trust lists as defined in eIDAS. **(m) 1.2. CertificationPath:**this restriction indicates a route certification required to be used by the SVA for signature validation. The certificate path has a length 'n' from the trust anchor (TA) down to the certificate used to validate a signed object (for example, the time-stamped certificate). This restriction may include the path to consider or indicate the need to consider the path provided in the signature, if any. **(m) 1.3. user-initial-policy-set:**this restriction is as described in IETF RFC 5280 clause 6.1.1 point (c). **(m) 1.4. initial-policy-mapping-inhibit:**This restriction is as described in IETF RFC 5280 clause 6.1.1 point (e). **(m) 1.5. initial-explicit-policy:**this restriction is as described in IETF RFC 5280 clause 6.1.1 point (f). **(m) 1.6. initial-any-policy-inhibit:**this restriction is as described in IETF RFC 5280 clause 6.1.1 point (g). **(m) 1.7. initial-permitted-subtrees:**this restriction is as described in IETF RFC 5280 clause 6.1.1 point (h). **(m) 1.8. initial-excluded-subtrees:**This restriction is as described in IETF RFC 5280 clause 6.1.1 point (i). **(m) 1.9. path-length-constraints:**indicates restrictions on the number of CA certificates in a certification path. This may need to define initial values or handle such constraint differently (eg ignore it).			

BSP	BSP title	Summary statement d deal	Counterpart statement technique	Restriction (s)	Value of restriction n in the creation of the signature (SCA or GIVES)	Value of restriction on increasing of signatures (SCA, SVA or GIVES)	Value of restriction n in the validation of the signature (SVA or GIVES)
				(m) 1.10. policy-constraints: This restriction indicates requirements for the certification policies referenced in the certificates. This may need to define initial values for this or handle the constraint differently (*for example, ignore it).* This should also allow the ability to require an end-entity certification policy extension.	See section 3.3.2		

				(m) 2. RevocationConstraints: This set of restrictions indicates the applicable requirements when verifying the validity status of the certificate and the certificates that make up the certification path. These restrictions may be different for different types of certificate (*for example, certificates issued to signer, CAs, responding OCSPs, CRL issuers, timestamp units).* The semantics is as follows **(m) 2.1. RevocationCheckingConstraints: i**It indicates the requirements to verify the revocation of the certificate. Such restrictions can specify whether or not revocation verification is required and whether OCSP or CRL responses should be used. Semantics for a possible set of values is as follows: **clrCheck:** Checks will be made against CRLs current (or authority revocation lists); **ocspCheck:** Revocation status will be checked using OCSP IETF RFC 6960; **bothCheck:** OCSP and CRL controls will be carried out; **eitherCheck:** OCSP or CRL controls will be performed; **noCheck:** Verification is not required. **(m) 2.2. RevocationFreshnessConstraints:**This restriction indicates the time requirements in the revocation information. Restrictions may indicate the maximum accepted difference between the date of issuance of information about the revocation status of a certificate and the time of validation, or require that the SVA only accept revocation information issued a certain time after it has been issued. created the signature. **(m) 2.3. RevocationInfoOnExpiredCerts:**This restriction requires that the signer's certificate be issued by a certificate authority that maintains certified revocation notices even after they have expired.	See section 3.3.2		

BSP	BSP title	Summary statement deal	Counterpart dstatement technique	Restriction (s)	Value of restriction n in the creation of the signature (SCA or GIVES)	Value of restriction on increasing of signatures (SCA, SVA or GIVES)	Value of restriction n in the validation of the signature (SVA or GIVES)
				(m) 3. LoAOnTSPPractices: This restriction indicates the required LoA on the practices implemented by the TSP that has issued the certificates, that is, the certificates present in the path of the signer's certificate and, optionally, those present in all or some of the other validated certificate chains.			
(n)	Signature Creation Devices			**(n) 1. LoAOnSCD:** This restriction indicates the LoA required in the signature creation device in which the private key resides, that is, the certificates present in the certificate path of the signer's certificate and, optionally, those certificates present in all or some of the others. validated certificate chains.	See section 3.3.2		
(or)	Other information to be associated with signatures			**(or) 1. MandatedSignedQProperties-signer-location:** This restriction indicates that the signer location must be expressed as a signed qualifying property and can also express restrictions on the value.	See section 3.3.2		
				(or) 2. MandatedUnsignedQProperties-signature-policy-extension: This restriction indicates that the signature policy extension is required as a qualified unsigned property and can also express restrictions on the values.	See section 3.3.2		
				(or) 3. MandatedUnsignedQProperties-signature-policy-inclusion-inarchival-form: This restriction indicates the requirement to include the signature policy as part of the corresponding unsigned rated property.	See section 3.3.2		
(p)	Cryptographic suites			**(p) 1. CryptographicSuitesConstraints:** This restriction indicates requirements on algorithms and parameters used when creating signatures or when validating signed objects or augmentation (*for example, signature, certificates, CRL, OCSP responses, timestamps).*	See section 3.3.2		
(q)	Technological environment			**(q) 1. TechnologicalEnvironmentConstraints:** This restriction indicates the requirements of the technological environment in which the signatures are processed	See section 3.3.2		

Table A.3

(p) 1. Cryptographic restrictions				
Signature type	**Identifier algorithm**	**Minimum size of signing key**	**Minimum length of hash value**	**Date of Expiry**
Signature to validate	Sha256RSA	2048-bit	256-bit	Maximum 5 years
Signer Certificate	Sha256RSA	2048-bit	256-bit	Maximum 5 years
CA certificate in a valid chain	Sha256RSA	2048-bit	256-bit	Maximum 5 years
Time-Stamp Token	Sha256RSA	2048-bit	256-bit	Maximum 5 years
OCSP response	Sha256RSA	2048-bit	256-bit	Maximum 5 years
CRLs	Sha256RSA	2048-bit	256-bit	Maximum 5 years

4.2.2 Exit restrictions to be used when validating signatures

As established in the Validation Policy of ANF AC OID 1.3.6.1.4.1.18332.56.1.1.

4.2.3 Exit restrictions to be used to augment signatures

As established in the Policy for the Qualified Service for the conservation of qualified electronic signatures and for the Qualified Service for the conservation of qualified electronic seals of ANF AC OID 1.3.6.1.4.1.18332.61.

5 Other business and legal matters

5.1 Consent to accept signatures

Express consent is not required to accept electronic signatures.

5.2 Condition to trust electronic signatures

Before trusting an electronic signature / electronic seal, it is required to submit it to a qualified validation system that is in compliance with eIDAS and recognized in the EU TSL.

5.3 Applicable fees

The rates for ANF AC's trust services are published on the corporate website

Https://www.anf.es

5.4 Financial responsibility

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.5 Confidentiality of information

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.6 Privacy of personal information

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.7 Intellectual property rights

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.8 Representations and warranties

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.9 Disclaimers of warranties

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.10 Limitations of liability

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.11 Indemnification

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.12 Term and termination

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.13 Notices Y communications individual with the participants

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.14 Amendments

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.15 Dispute resolution procedures

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.16 Applicable law

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

5.17 Compliance with applicable law

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.

6 Compliance audit and other evaluations

6.1 Compliance audits -scope and periodicity-

As defined in the Certification Practice Statement (DPC) OID 1.3.6.1.4.1.18332.1.9.1.1.