Validation Policy

Qualified Service of Validation of signatures and stamps

Qualified Electronics (QES)

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

Telephone: 902 902 172 (Calls from Spain)

International +34 933 935 946

Web: www.anf.es

Security level

Public Document

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

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

Web: www.anf.es

INDEX

1. Introduction

1.1. Overview

This document is the Validation Policy of ANF Certification Authority [ANF AC], it establishes the validation rules for qualified and advanced electronic signatures (QES / AES), and for qualified and advanced electronic seals (QEseal / AESeal). It is in accordance with theRegulation (EU) n ° 910/2014of the European Parliament and of the Council, and with section i.6 of the IMPLEMENTING DECISION (EU) 2015/1506OF THE COMMISSION of September 8, 2015 (in accordance with paragraph 5 of article 27 and paragraph 5 of article 37 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council):

> *"Advanced electronic signatures and advanced electronic stamps are technically similar, so the standards for advanced electronic signature formats should apply mutatis mutandis to advanced electronic stamp formats."*

This Validation Policy is subordinate to what is established in the Certification Practice Statement of ANF Certification Authority.

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

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

This document has been prepared in accordance with current Spanish legislation and pan-European standards and specifications for the provision of trust services. Its structure follows the recommendation of Annex A ETSI TS 119 441.

This signature validation policy establishes the set of restrictions processed or to be processed by the validation service application (SVA) for signature validation, which works on the basis of a signature validation policy as input. The validation policy supported by the ANF AC SVA is defined in section 1.1.2 of this document.

ANF AC is the Qualified Provider of the Electronic Signature and Stamp Validation Service (QSVSP) and provides this qualified validation service (QSVS).

This service verifies that the signed / sealed files submitted for validation meet the requirements of the eIDAS Regulation and standards on the matter, using operational procedures and information security management procedures that exclude any probability of data manipulation:

- Check the validity of QES / AES and QEseal / AESeal.
- Validate qualified certificates: verifying qualification, integrity, authenticity and validity;
- Validate qualified electronic time stamps: verifying qualification, integrity, authenticity and validity.

The ANF AC Validation service has been designed and developed in accordance with the standards:

- **ETSI EN 319 401:** General Policy Requirements for Trust Service Providers;
- **ETSI TS 119 441:** Policy requirements for TSP providing signature validation services;
- **ETSI TS 119 101:** Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for applications for signature creation and signature validation;
- **ETSI TS 119 442:** Protocol profiles for trust service providers providing AdES digital signature validation services;
- **ETSI TS 119 172-4: (**Draft) Signature policies, Part 4: Signature validation policy for European qualified electronic signatures / seals using trusted lists;
- **ETSI EN 319 102-1:** Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation;
- **ETSI TS 119 102-1:** Procedures for Creation and Validation of AdES Digital Signatures- Part 1: Creation and Validation;
- **ETSI TS 119 102-2:** Procedures for Creation and Validation of AdES Digital Signatures, Part 2: Signature Validation Report;
- **ETSI EN 319 122-1:** CAdES digital signatures, Part 1: Building blocks and CAdES baseline signatures;
- **ETSI EN 319 122-2:** CAdES digital signatures, Part 2: Extended CAdES signatures;
- **ETSI EN 319 132-1:** XAdES digital signatures, Part 1: Building blocks and XAdES baseline signatures;
- **ETSI EN 319 132-2:** XAdES digital signatures, Part 2: Extended XAdES signatures;
- **ETSI EN 319 142-1:** PAdES digital signatures, Part 1: Building blocks and PAdES baseline signatures;
- **ETSI EN 319 142-2:** PAdES digital signatures, Part 2: Additional PAdES signatures profiles;
- **ETSI EN 319 412: (**Electronic Signatures and Infrastructures (ESI): Certificate Profiles);
- **IETF RFC 3647: "**Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- **RFC 3739: (**Internet X.509 Public Key Infrastructure: Qualified Certificates Profile);
- **ETSI TS 119 172-1:** Signature Policies, Part 1: Building blocks and table of contents for human readable signature policy documents;
- **ETSI TS 119 172-2:** Signature Policies, Part 2: XML format for signature policies;

1.1.1. TSP identification

ANF Certification Authority [ANF AC], is the provider of the qualified service for the validation of qualified electronic signatures and stamps. It is a legal entity established under Organic Law 1/2002 of March 22 and registered in the Ministry of the Interior with the national number 171,443 and NIF G-63287510.

ANF AC uses OID's according to the ITU-T Rec. X.660 standard and the ISO / IEC 9834-1: 2005 standard and has been assigned the private company code (SMI Network Management Private Enterprise Codes) 18332 by the organization international IANA (Internet Assigned Numbers Authority), under the branch iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA –Registered Private Enterprise-).

ANF AC is a qualified provider in the following eIDAS trust services:

- Qualified electronic signature certificates
- Qualified electronic seal certificates

- Qualified web authentication certificates (SSL / TLS - QWAC)
- Qualified time stamp service
- Qualified service for the validation of qualified electronic signatures and stamps
- Qualified service for the preservation of qualified electronic signatures and seals
- Qualified certified electronic delivery service

ANF AC, is certified in accordance with international standards:

- ISO 9001 for Cas
- ISO 27001 ISMS
- ISO 14001 Environment

In addition, as a member of the UN Global Compact, ANF AC respects the 10 established principles and assumes the ISO 26000 standard. ANF AC systems are subject to compliance with the PCI-DSS standard.

1.1.2. Supported Validation Service Policy (s)

The QSVS works on the basis of a validation policy of signatures as input, that is, the validation of signatures / stamps, is always performed against a validation policy. Supported validation policies and whose requirements are used to carry out the process are:

ANF AC Validation Policy	OID 1.3.6.1.4.1.18332.56.1.1
Conforms to the ETSI TS 119 441 validation criteria	OID 0.4.0.19441.1.1
Conforms to the ETSI TS 119 441 qualified validation criteria	OID 0.4.0.19441.1.2

This Validation Policy of ANF AC permanently updated and published in https://www.anf.es

The validation report specifies the key and level of the validated electronic signature / seal. The trusting third party is responsible for determining its applicability to the commercial purpose and, therefore, its acceptance or rejection.

1.2. Validation service components

1.2.1. SVS actors

The validation service includes the participation of:

- The signer can restrict / limit the signature (for example, by means of a signature policy (creation), a standard commitment) and this can influence the validation of the signature.
- TSPs related to the signer:
  - or The TSP has issued the signer certificate (CA);
  - or Any TSP that may be implicit in the generation of signatures:
    - the TSP managing the (Q) SCD on behalf of the signer;
    - the TSP that generates the signature;
    - TSA;
    - VA, OCSP answer,
    - etc.
- Other TSPs:

or TSA;
or other SVSPs to whom the SVSP may transmit a request; -
or etc.

- European or foreign trusted list providers; Y
- The European Commission provides the list of trusted lists.

1.2.2. Service architecture

The signature validation service server (SVSServ) implements the SVA, that is, the application performs verification of the format, the identification of the signer's certificate, the validation context, the validation X.509, cryptographic validation, signature acceptance (i.e., signature validation requirements), etc. According to ETSI TS 119 102-1 specification.

ANF AC's signature / validation (DA) applications (Safe Box and critical Access) can be configured to operate exclusively on the client side (e.g. when they do not have an internet connection), or shared in client and server mode (through Internet connection to the Signature Validation Service (SVSServ) server.

Validation services are divided into the following components:

- The signature validation client is a component or piece of software that implements signature validation. In particular:
  or In exclusive configuration (**unqualified report)**
    - It requests a signature validation to the ANF CT component (CryptoAPI of the DA.
    - The DA allows you to request validation of a signature or multiple signature validations.
    - The DA executes the signature validation protocol exclusively on the user side;
    - The DA prepares the validation report;
    - The validation report is presented;
    - The client has:
      - A user interface to manually enter the request.
      - A user interface to present the report.

  or In shared configuration (**qualified report)**
    - Request a signature validation to the SVSServ
    - The service allows you to request validation of a signature or multiple signature validations.
    - Execute the Signature Validation Protocol (SVP) on the user side;
    - Where appropriate, it is responsible for the presentation of the validation and signature report;
    - The client has:
      - A user interface to manually enter the request.
      - A machine interface for automated requests.

- A user interface to present the report and validate the signature that authenticates it.

- The signature validation service server (SVSServ) implements the signature validation protocol by the SVSP. In particular:
  - or Runs the signature validation service protocol and processes signature validation on the SVSPl;
  - or Run the Signature Validation Application (SVA) as defined in ETSI TS 119 102-1, which implements the validation algorithm defined in ETSI TS 119 102-1. For this, the service consults among others:
    - The CA that issued the signer's certificate (for certificate (s) status information services (OCSP responder).
    - The CA of the TSA (s) that have provided timestamps within the signature.
    - Other SVSPs for complementary controls.
    - The European Member States' Trust Lists, the European Commission's Trust Lists List, and / or other trust lists.
    - etc.
  - or Creates the qualified signature validation reports related to the request;
  - or Create the signature validation response.

1.2.3. Parties involved

- **Qualified provider of validation services (QSVSP).** In the context of this document ANF AC. ANF AC assumes the general responsibility of the validation service, even when some functions are assumed by contracted third parties,
- **Subscriber**. It is the responsibility of the client who hires the validation service and submits signatures and / or electronic seals to validation.
- **User.** Application or human interacting with a signature validation client.
- **Trusting third party.** Third parties that without being the subscriber or the user, are authorized to access the qualified validation reports and trust them.

1.3. Definitions and abbreviations

1.3.1. Definitions

- Signature acceptance, technical verification to be carried out on the signature itself or on the attributes of the signature.
- 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, application that validates a signature against a signature validation policy, and that issues a status indication (that is, the signature validation status) and a signature validation report. The ANF AC validation application is in compliance with ETSI TS 119 102-1.
- Signature validation client, software component that implements the signature validation protocol to the user.
- Validation data, data that is used to validate an electronic signature.
- Signature validation status, one of the following indications: TOTAL-PASSED, TOTAL-FAILED or UNDETERMINED
- Signature validation report, complete 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.
- Signature PoE, the signature existence test, 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 (PASSED, FAILED, 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.
- Signature Applicability Rules, set of rules, applicable to one or more electronic signatures, that defines the requirements to determine whether a signature is suitable for a particular business or legal purpose.
  or The owner of the firm's enforceability rules is usually the relying party and these rules they 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
- 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 [i .1], Article 40. For the purposes of this Policy, the service is that provided by ANF AC.
- Qualified validation service for qualified electronic signatures, as specified in Regulation (EU) No. 910/2014 [i .1], 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.
- SubscriberCorresponds to the client, natural or legal person, who hires the validation service and submits signatures and / or electronic seals to validation.

- Commitment type, indication accepted by the signer of the exact implication of an electronic signature.
- User, Application or human being that interacts with a signature validation client.
- Validation, process of verification and confirmation of the validity of a certificate or an electronic signature.
- Signature validation, process of verification and confirmation that a digital signature is technically valid.
- Qualified electronic signature validation, 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 checkVerification parameters to determine if a signature conforms to the signature applicability rules can be provided as a complement to the signature validation service defined 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.

1.3.2. Abbreviations

ANF AC:	ANF Certification Authority
AV:	Validation Authority
HSM:	Cryptographic Security Module in accordance with a Common Criteria ISO 15408 EAL 4+ or FIPS PUB 140-2 level 3 certification
OCSP:	protocol for checking the status of an online certificate
PCSC:	Qualified Trust Service Provider
PoE:	proof of existence
WHAT IS IT:	qualified certificate of electronic signature
QEseal:	qualified certificate of electronic seal
QSVSP:	Qualified Provider of Signature / Stamp Validation Services
QSVS:	Qualified Signature / Stamp Validation Service
SD:	signer's document
SDO:	signed data object

SVA: electronic signature and stamp validation app

SVP: signature validation protocol

SVR: signature validation report

SVS: signature validation service

SVSServ: signature validation service server

TSA: Time Stamping Authority

TSU: time stamping unit

TSP: Trust Service Provider

VPR: signature validation process

1.4. Policies and practices

1.4.1. Organization that manages the TSP documentation

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

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

1.4.2. Contact person

Department	Legal department
Email 1	support@anf.es
Email 2	mcmateo@anf.es
Department	Technology and regulatory compliance
Email 3	pablo@anf.es
Address	Paseo de la Castellana, 79
Location	Madrid
Postal Code	28046
Phone number	902 902 172 (Calls from Spain) International (+34) 933 935 946

1.4.3. Applicability of public documentation

Document name	Validation Policy of the Qualified Service for the Validation of qualified electronic signatures and seals		
Version	2.6.		
OID	1.3.6.1.4.1.18332.56.1.1		
Approval date	04/12/2021	**Publication date**	04/12/2021

Version	**Changes**	**Approval**	**Publication**
2.6.	Annual review	04/12/2021	04/12/2021
2.5.	Technical corrections alignment ETSI TS 119 441	11/18/2020	11/18/2020
2.4.	Technical corrections	01/15/2020	01/15/2020
2.3.	Annual review	02/23/2019	02/23/2019
2.2.	Annual review	06/05/2018	06/05/2018
2.1.	Annual review	08/12/2017	08/12/2017
2.0.	Annual review	03/16/2016	03/16/2016

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

The entry into force of a new version occurs at the time of its publication, the policy is published on the corporate website of ANF AC www.anf.es

- OID Certification Practice Statement 1.3.6.1.4.1.18332.1.9.1.1
- Terms and Conditions OID 1.3.6.1.4.1.18332.5.1.5
- Contract for the Provision of Services OID 1.3.6.1.4.1.18332.5.1.4
- OID Risk Assessment 1.3.6.1.4.1.18332.80.6.3
- OID Risk Analysis Matrix 1.3.6.1.4.1.18332.13.2.1
- Business continuity and disaster recovery plan OID 1.3.6.1.4.1.18332.13.1.1
- Qualified Validation Service - Procedure - Interpretation - Evidence - Battery of tests
- OID 1.3.6.1.4.1.18332.56.1.2

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

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.

2. Management and operation of the trust service

2.1. Internal organization

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.1.1. Organization reliability

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.1.2. Segregation of functions

As defined in the CPS of ANF AC regarding the signatories of the certificates.

- Provider of the qualified validation service, in the context of this ANF AC document.
- Subscribers, corresponds to third parties who trust the validation service and submit signatures and / or electronic seals to validation.
- Users, corresponds to the application or human being that interacts with the signature / validation application on a signature validation client.

2.2. Human Resources

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.3. Asset Management

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.4. Access control

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.5. Cryptographic controls

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.6. Physical and environmental security

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.7. Operational safety

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.8. Network security

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.9. Incident management

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.10. Evidence gathering

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.11. Business continuity and disaster recovery plan

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.12. Cessation plan

As defined in the CPS of ANF AC regarding the signatories of the certificates.

2.13. Accordance

As defined in the CPS of ANF AC regarding the signatories of the certificates.

3. Design of the signature validation service

3.1. Validation process requirements

When the signature validation service aims to validate qualified electronic signatures or stamps as defined in Article 32.1 of Regulation (EU) No 910/2014, the validation process will follow the requirements of ETSI TS 119 172-4 (*draft phase).*

3.1.1. Signature validation process to the SVSServ follows the ETSI TS 119 102-1 algorithm

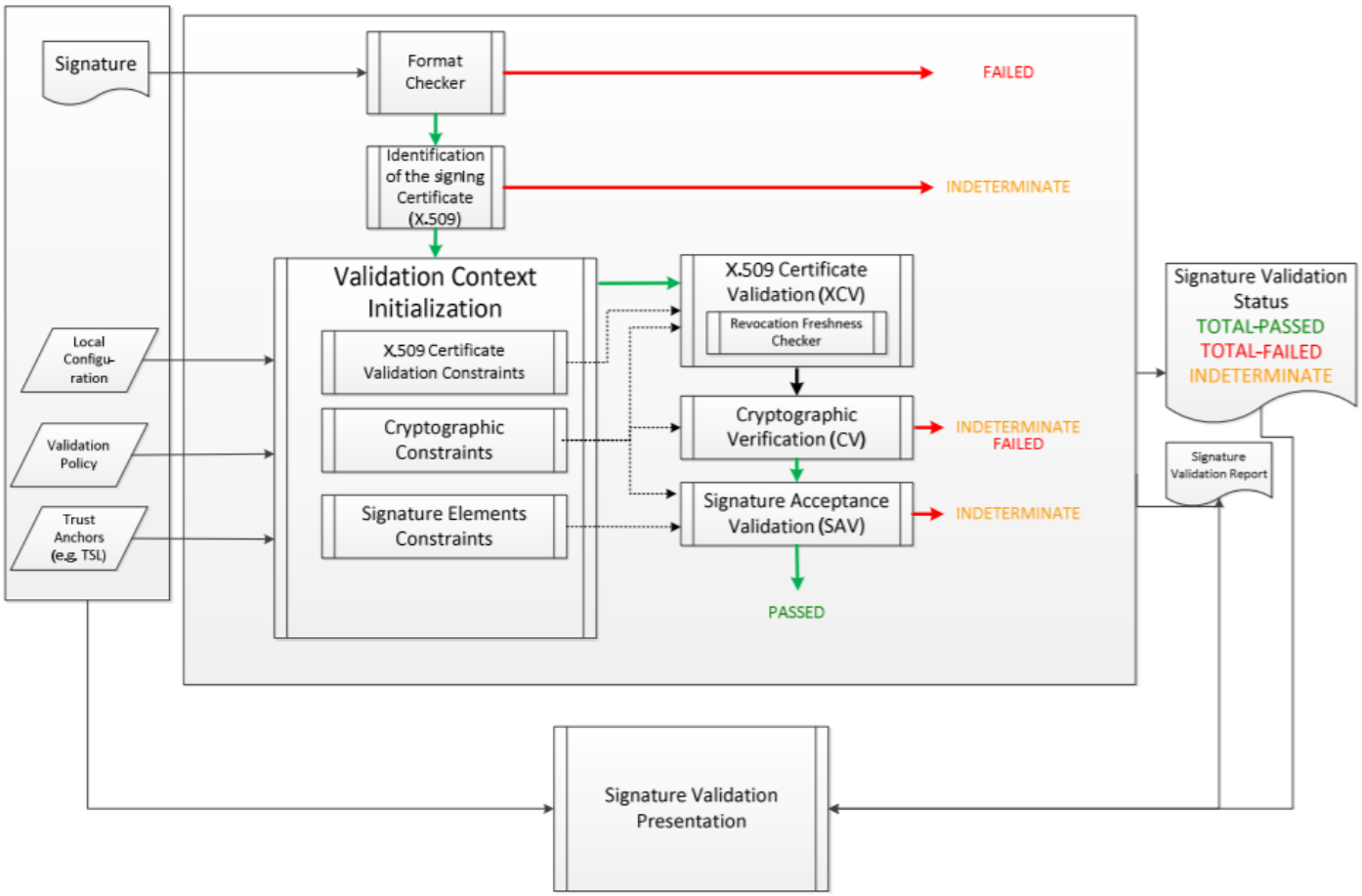

Illustration 1 Basic Signature Validation ETSI TS 119 172-1

Functional procedure of the validation service:

Step 1	The client generates and sends a signature validation request to ANF AC. The protocols supporting the request and the response correspond to the ETSI TS 119 442 specification. The request includes: 1. The signed document / s (SD) and the signature / s (SDO) that signs them; or

	2. the signed documents / representation / s (SDR) and the signatures that sign them, to avoid exposing the content of the document to the validation service. Mapping between signed documents and their summaries used within signatures is essential when verifying a signature. In accordance with Regulation (EU) No. 910/2014, the link between the signed document and the signature is part of the conditions for an advanced electronic signature / stamp. However, due to confidentiality or performance reasons, there are use cases where it is preferable to send only the hashed summaries of signed documents. In this case, the verification of the integrity of the signed document and its correspondence with the signature is beyond the control and responsibility of the SVSServ. In other cases, it is the ANF AC component that calculates the hash value of the signed documents, or any attribute such as file attributes. In this case, ANF AC guarantees that the integrity of the documents has not been compromised during the process. In any of the cases, the expected hashes are calculated with the same hash functions as those used in the signature.
Step 2	**SVSServ performs the validation process.**
	The validation process corresponds to the ETSI TS 119 102-1 specification]. Validation is performed by the SVSP in accordance with this signature validation policy. The signature of the validation process follows the provisions of ETSI TS 119 102-1].
Step 3	**The SVSServ prepares and sends the validation response.**
	The protocols that support the request and the response are those specified in ETSI TS 119 442. The validation response includes the validation reports. It includes the OID of the Service Policy and the OID of the signature validation policy used. The validation report corresponds to the ETSI TS 119 102-2 specification, and is signed by the electronic seal of ANF AC.
Step 4	**Presentation of the validation report**
	The client can offer a signature validation presentation module to present the validation report that specifies the result and provides detailed report of each of the signed attributes. The user, under his responsibility, decides whether to accept the signature or not.

3.2. Validation protocol requirements

The validation protocol used by ANF AC complies with ETSI TS 119 442 *"Protocol profiles for trust service providers providing AdES digital signature validation services."*

3.2.1. Validation of electronic signatures and stamps

ANF AC's Qualified Validation Services allow you to confirm the validity of a QES / QEseal, provided that:

- The certificate that supports the electronic signature / seal at the time of signature has been qualified (QC) in accordance with Annex I of the eIDAS Regulation.

- The qualified certificate has been issued by a Qualified Trust Services Provider and is valid at the time of signature.
- The signature validation data correspond to the data provided by the User Party.
- The unique set of data that represents the Subject of the electronic signature in the certificate has been duly delivered to the User Party.
- If at the time of signing a pseudonym has been used, and this has been clearly indicated to the User Party.
- The electronic signature / seal has been created by a qualified electronic signature / seal creation device.
- The electronic signature / seal has been created using cryptographic components classified as secure.

- If the electronic signature / seal when creating it has been subjected to a certain electronic signature policy not authorized by this policy.
- The integrity of the signed data has not been compromised.
- The requirements for an advanced electronic signature (article 26 of the Regulation) have been met at the time of signature.
- Provides the User Party with the correct result of the validation process (status indication and report) and lets them know about any security-related problems.
- The service gives the User Parties the opportunity to receive the result of the validation process in an automated, reliable and efficient manner, which includes a qualified signature (or seal) of ANF AC as QTSP.
- The signed data object must contain the necessary certificates in its attributes.

In addition, in accordance with ETSI TS 119 172-1, the possible inclusion of signature commitments will be taken into account and will be recorded in the validation report. Specifically, the accepted signature commitments (may include one or more) are:

- OID 1.2.840.113549.1.9.16.6.1 - the signature is intended for data authentication purposes only. 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 - as 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.

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.
ANF AC, in accordance with the provisions of Annex B of ETSI 119 172-1, has created the following proprietary OIDs:

OID 1.3.6.1.4.1.18332.27.1.9 - Use of the signature as a 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 legal certification of an original document. The signature is intended solely to certify that the signer guarantees that the signed document is an authentic 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.

OID 1.3.6.1.4.1.18332.27.1.1 - Full legal effects according to OID Signature Policy 1.3.6.1.4.1.18332.27.1.1.

Indicates that the signature is intended to be used in a legal and contractual framework, in which it is desired to prove with probative force and full legal validity, that the signer agrees, except in those matters in which a mention has been made, or exception, or commitment to 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 subscribe all types of electronic documents, in accordance with the use limitations established by current legislation, and the restrictions derived from the Certification Policy to which it is submitted the electronic certificate used in its creation.

The technical validity of the QES / QESeal is verified according to the process described in the ETSI EN 319 102-1 document and confirmed by issuing qualified electronic status certificates.

The following sections describe the validation service concept model, the validation process selection, and the result (status and report) of the validated qualified certificate for QES / QESeal.

In the event that there is no specific requirement indicated on the Service in this document, the requirements of point i.5 of ETSI EN 319 102 will apply.

If this document indicates specific requirements and rules, they will prevail over the pertinent ones of ETSI EN 319 102-1.

In the event that there is a discrepancy between the requirements and rules of this document and those of ETSI EN 319 102, the contents of this document will prevail.

The SVSServ manages event logs (LOGs) that allow proof of services provided and the time they occurred. In addition, the types of validation services that have been requested, the result of the request (success or failure) are recorded. and the identity of the subscriber who has requested them in order to manage consumption. Access to this information is restricted to expressly authorized personnel.

3.2.2. TSP validation

SVSServ manages a repository with the Trusted Lists (TSL) published by each of the member countries of the Union and versioning control. Before use, it is verified that the version to be used is the latest version published.

The interpretation of the TSL is carried out by SVSServ in accordance with the provisions of ETSI TS 119 612.

3.2.3. OCSP service

The SVSServ proceeds to verify the validity status of the certificates used in the elaboration of the electronic signature / seal by means of OCSP consultation. The OCSP response is required to comply with the IETF RFC 6960, X.509, Internet Public Key Infrastructure Online Certificate Status Protocol –OCSP standard.

OCSP Responders must attend queries in real time, directly on the repositories of the issuing entity of the certificates used, either in the preparation of the signature, seal, or issuance of a time stamp. OCSP responses must be electronically signed by the QTSP. The validation process includes the certificate submitted for consultation and the entire chain of the Certification Hierarchy up to the first level (excluding Root CA).

The fields contained in the OCSP response according to the RFC6960 specification:

Field	Definition
CertID.hashAlgorithm	Hash algorithm identifier
CertID. issuerNameHash	Sender DN hash (OCTET STRING)
CertID.serialNumber	Serial number of the certificate to be validated
CertID. issuerKeyHash	Hash of the issuer's public key (OCTET STRING)
nonce	Optional
certReq	All responses contain the ANF AC certification chain down to the root. Its presence and value is ignored.

An example of a query with OpenSSL is detailed below:

OpenSSL ocsp -CAfile <ca_certificate>
- issuer <certificate_ia> -cert <certificate_to_consult>
- url <verification_url>

The <verification_url> field must be the one indicated in the "Authority Information Access" field of the certificate.

Example to perform GET queries with open SSL:

The request is generated:

openssl ocsp

- noverify

- no_nonce

- respout ocsp.resp

- reqout ocsp.req

- issuer AssuredID64.cer

- cert rev64.cer

- url"http://ocsp.anf.es/spain/AV"

- header "HOST" "ocsp.anf.es"

- text

Converts to B64

openssl enc

- in ocsp.req

- out ocsp.req.b64 -a

Clarification: OpenSSL has been found to issue the following error responses:

1 / If the root CA has directly signed the end entity certificate, OpenSSL returns:

Response Verify Failure

Verify error: self signed certificate in certificate chain

2 / If the response from the OCSP responder is of a CRL type, OpenSSL returns:

Response Verify

Failure signer certificate not found

3 / The OCSP Responder servers of ANF AC support GET and POST queries.

3.3. Interfaces

According to the conceptual model of the electronic signature / stamp validation process in ETSI EN 319 102-1, the software with validation functions for QES / QESeal includes two components:

- SVA / Signature Validation Application;
- DA / Driving Application.

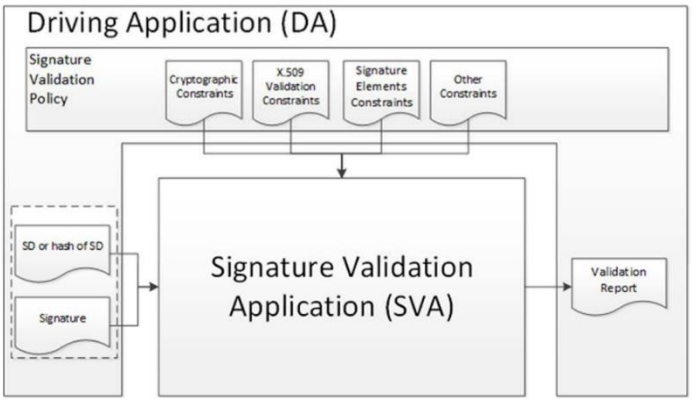

Figure: ETSI TS 119 102-1 signature validation model

ANF AC, makes three modalities available to its subscribers:

- **Safe Box.** It is an end-user application that, once installed, activates in the Shell context menu (right mouse button), making it possible to make command line calls to the SafeBox application. This application allows you to carry out electronic signatures and a qualified validation process for electronic signatures and stamps. Exclusively for SOWindows.
- **Critical Acces.** It is an end-user desktop application. Exclusively for Windows OS,

- **Web Service.** This service is available in two modalities:
  or Web client that allows human user validations through the browser.
  or No interface to perform automatic validations. Available for Linux OS.

In all modes the user can select the signed data object if it is not included in the SDO. But the user is not allowed to provide more inputs for the validation process (eg elements to parameterize the validation policy, signature class, etc)

In all the modalities, it is possible to validate multiple signatures, and validate all of them.

SVA activates the ANF CriptoToken library, a "Driving Application" (DA) component that receives the result of the validation process in the form of a qualified validation certificate (status and report) from the SVSServ.

The service supports signature and electronic stamp validation processes in different formats:

- Validation process for the basic signature / stamp format
- Validation process for Signatures with Electronic Time Stamp
- Validation process for Signatures with Electronic Time Stamp and verification of validity status at OCSP origin.

DA uses standardized libraries and components that have been tested. The latest versions classified for exploitation are kept.

SVA, maintains the integrity and confidentiality of all the information provided by the user and of any data that flows between the application and the user, even in the case of a public environment.

Unless the subscriber has contracted the qualified service of conservation of signatures and electronic seals of ANF AC, the SVSServ will not store the SD.

3.3.1. Communication channel

The communication channel between the client and the SVSServ carries the signature validation request (1.) and the response (3.). It can be synchronous or asynchronous. It covers SVSP (SSL Communications Protocol) authentication, to prevent false reporting, and can support client authentication.

When the SVSP requests the intervention of TSA (ANF AC TSA for time stamping) or, OCSP status request (ANF AC VA for OCSP responses) or, TSL request, etc. , SSL communication protocol is used.

The subscribers of the validation service are authenticated before the SvSServ using credentials provided by ANF AC.

3.3.2. SVSP - other TSP

ANF AC, to perform the service provision, may have to consult another PCSC, for example OCSP status query. In this case, the communication channel between ANFA C and other providers requires that the called PSC be qualified, the information received is signed and it is possible to validate it.

The validation service may be affected by the practices, policies and SLAs of other TSPs that are not under the control of ANF AC.

3.4. Signature Validation Report Requirements

The validation report includes information on ANF AC in accordance with ETSI TS 119 612 Section 5.5.2, and on the application used. The requirements established by ETSI TS 119 102-2 and ETSI TS 119 441 are followed. In the event that ANF AC decides to make any variation in them, this variation will be included in this policy,

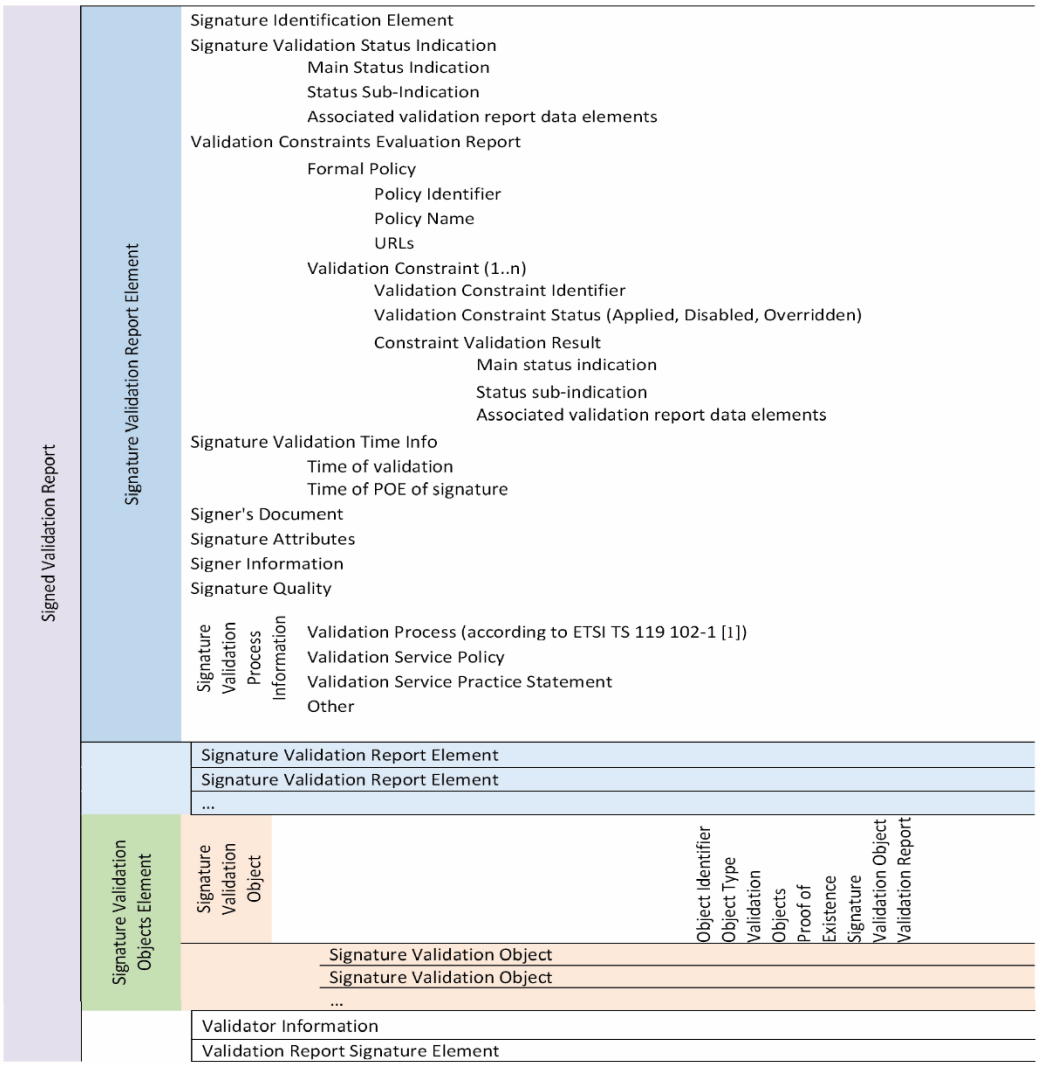

Illustration 2 Structure and elements of the validation report according to ETSI TS 119 102-2 v 1.2.1

3.4.1. Status indication of the validation process and the validation report

The service provides a validation report in PDF (signed PAdES LT) or XML (signed XAdES - A), which details the validation of the signature / stamp performed, allowing the DA to check in detail the decisions made during the validation and to establish / examine in detail the causes of the status indication provided.

The result of the validation process includes:

- A status indication of the results of the QES / QESeal validation process.
- An indication of the validation policy (s) whose requirements have been applied.
- Date and time of the validation status, including the data used for the validation.
- Additional reporting data for validation according to the following tables:

3.4.2. Status indication for the QES / QESeal validation process

Status indication	Semantics	Validation report data
TOTAL-CONFIRMED	The QES / QESeal validation process has a TOTAL-CONFIRMED: • checks cryptographic of QES / QESeal they have been correct (including verification of hashes of the different data objects, indirectly signed); • positively validated the certification of the identity of the signer (that is, the signing certificate is valid); Y • successfully validated QES / QESeal	The validation process confirms that the certification chain is validated, including the certificate for QES / QESeal, used in the validation process along with a specific signed / stamped attribute (if any), which is considered as proof of validation.
TOTAL-FAILURE	The QES / QESeal validation process has a FULL-FAIL result because the Cryptographic checks of the QES / QESeal They are unsuccessful (including Hashes controls of the different data objects, Indirectly signed / sealed) or it has been shown that the generation of the Signature / seal has occurred after Revocation / in suspension time of the QC .	The validation process explains the cause of issuing the report of TOTAL-FAILURE for each of the elements that are taken into account and that have given negative results.
INDETERMINATE	The information available is not enough to carry out the validation process and determine the QES / QESeal status indication: TOTAL CONFIRMED or TOTAL FAILED	The validation process provides information in order to explain the cause that results in "undetermined", and to help determine the missing data to complete the validation process.

The validation report includes the status indication corresponding to **TOTAL-FAILURE** and **INDETERMINATE.**
In validation, QES has a structure that is presented in the following table, and consists of main and auxiliary codes that provide the validation process.

Structure and semantics of the Validation report

Indication of condition	Stub code	Semantics	Report data from validation
TOTAL-FAILURE	HASH-FAILURE	The QES validation process / QESeal leads to TOTALFAILED, Because at minus a hash of an object that participates in the signature, does not correspond to the hash registered in QES / QESeal.	The validation process provides a identifier that Explicitly identifies a signature / stamp object causing the error in the QES / QESeal.
	FORMAT-FAILURE	QES / QESeal is not compatible with supported standards indicated in this document at a level that does not allow the block to be processed cryptographically.	The validation process provides information about the failed QES / QESeal process
	SIG-CRYPTO-FAILURE	The QES / QESeal validation process leads to FULL FAILED, because the signature value cannot be verified with the help of the public key of the QES / QESeal certificate.	The validation process is negative due to inconsistency of QES / QESeal certificate.
	POLICY-FAILURE	The validation process determines that the QES / QESeal is subject to a Signature Policy not authorized by this Validation Policy.	The validation process is negative because the Signature Policy is not authorized.
	REVOKED	The QES / QESeal validation process leads to FULL-FAIL because: the QES / QESeal certificate has been revoked, and there is a test based on a Timetamping that determines that the Signature / seal is developed after revocation of the certificate.	The validation process provides: · The validation of the certification chain. The date of revocation / suspension of the QES / QESeal certificate. · CRL where applicable. · Electronic QES / QESeal time stamp.
INDETERMINATE	SIG_CONSTR AINT_FAILURE	The QES validation process / QESeal leads to UNDETERMINED, because one or more QES / QESeal attributes are not correspond to the elements validation.	The validation process provides: • The chain of certification used in the validation process. • Additional information about the cause

	CHAIN_CONSTRAINTS_FAILURE	The QES / validation process QESeal leads to UNDETERMINED, because the certification chain used in the validation process does not correspond to the elements related to the certificate of validation	The validation process provides: • The chain of certification used in the validation process. • Additional information about the cause
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The QES / validation process QESeal leads to UNDETERMINED, because the verification of the chain of certification shows an error due to no reason established.	The validation process provides: Additional Information about why.
	CRYPTO_CONSTRAINTS	The QES / validation process QESeal leads to INDETERMINATE, because at least one of the algorithms used or the size of the keys used with these algorithms is below the required level of security cryptographic and also: The QES / QESeal certificates will be generated after a moment until which these algorithms / keys are they considered safe; plus: QES / QESeal is not protected by a timestamp stamp sufficiently reliable before the time until which the algorithms / keys are considered safe.	The validation process provides: A identification / designation of actual QES / QES or of a certificate generated with a algorithm or a key size below the level security required cryptographic.
	EXPIRED	The QES / validation process QESeal leads to UNDETERMINED, because the signature time stamp is after the expiration date (notAfter) of the certificate	The validation process provides: the validated certification chain
	NO_SIGNING_CERTIFICATE_FOUND	The QES / QESeal certificate cannot be identified	

	NO_CERTIFICATE_CHAIN_FOUND	An element of the certification chain to identify the QES / QESeal certificate has not been found.	
	REVOKED_NO_POE	The corresponding certificate has been revoked / suspended during validation. The SVA cannot establish whether the certificate was used before or after the time of revocation / suspension	
	OUT_OF_BOUNDS_NO_POE	The certificate has expired or is not yet valid on the validation date / time and SVA cannot determine if it is within the range of certificate validity At least	
	CRYPTO_CONSTRAINT_FAILURE_NO_POE	one of the algorithms used in the QES / QESeal or in the corresponding certificates that participate in its validation or key size is below the required level of security cryptographic and there is also no proof that the signatures / seals or these certificates have been generated before the time up to which this algorithm / key has been considered secure	The validation process provides: Identification of QES / QESeal or the corresponding certificate Generated with Unacceptable Key Length or with an algorithm does not meet security requirements cryptographic.
	NO_POE	Evidence is missing to show that the signature / seal was generated prior to the recognition of a compromising event (i.e. broken algorithm).	
	TRY_LATER	Not all checks can be done with the information available. Despite this, the process is possible if the validation uses additional information about the Revocation / Suspension that	

		it will be available at a later stage.	
	SIGNED_DATA_NOT_FOUND	Data for signature / stamp cannot be received	The validation process provides: The identifier (for example URI) of the data for the signature / stamp that caused the error
	GENERIC	other reasons.	The validation process provides: Additional information showing why the status of validation is INDETERMINATE

3.4.3. Certificate validation limitations

Restrictions for the validation of X.509 certificates in the certification chain verification process according to ETSI TS 119 172-1, clause A.4.2.1., Table A.2. Row (m).

Restriction	**Constraint value in the QES / QESeal validation (SVA or DA)**
(M) 1. X509 Certificate validation restriction: This set of restrictions refers to the requirements in the certification chain validation process in accordance with IETF RFC 5280. The restrictions may be different for different types of certificates (eg signing certificates. For OCSP responses, for CRL lists, electronic time stamps / TST). The semantics of a possible set of required values that is used to present these requirements is determined as follows:	
(M) 1.1 SetOfTrustAnchors: This restriction indicates a set of trustworthy REPUBLICA Certifying Authorities (TA) acceptable in order to limit the validation process. MEXICO (TSL) ARGENTINA	EU (TSL) ECUADOR (TSL) PERU (TSL) DOMINICANA (TSL) (TSL)
(M) 1.2 CertificationPath: This constraint shows the certification path used by the SVA for QES / QESeal validation. The certification path It has "n" length from the beginning / Trusted Authority (VA) towards the QES / QESeal certificates used when validating the signature. The restriction may include the path or indicate the need to include the path provided through the QES / QESeal, if there is one.	

(m) 1.3. *user-initial-policy-set:* Pursuant to IETF RFC 5280 clause 6.1.1 (c) (m) 1.4. *initial-policy-mapping-inhibit:* Pursuant to IETF RFC 5280 clause 6.1.1 (e) (m) 1.5. *initial-explicit-policy:* Pursuant to IETF RFC 5280 clause 6.1.1 (F) (m) 1.6. *initial-any-policy-inhibit:* Pursuant to IETF RFC 5280 clause 6.1.1 (g) (m) 1.7. *initial-permitted-subtrees:* Pursuant to IETF RFC 5280 clause 6.1.1 (h) (m) 1.8. *initial-excluded-subtrees:* Pursuant to IETF RFC 5280 clause 6.1.1 (i) (m) 1.9. *path-length-constraints:* This limitation refers to the number of Certification Authority (CA) certificates within the certification chain. (m) 1.10. *policy-constraints:* This restriction refers to the policy (s) in the QES / QESeal certificate.	100 Mb.
(M) 2. RevocationConstraints: This set of restrictions refers to the verification of the status of QES / QESeal certificates during the validation process. These restrictions may be different for different types of QES / QESeal certificates.	
(M) 2. Revocation restrictions: This set of restrictions refers to QES / QESeal (m) 2.1. RevocationCheckingConstraints: This restriction refers to the requirements to verify the QES / QESeal certificate for revocation / suspension. These restrictions specify whether the revocation / suspension check is necessary or not and whether OCSPresponses or issued CRLs must be used. The semantics for a possible set of required values used to present these requirements is defined as follows: - ClrCheck: Checks are performed based on the current CRL; - OcspCheck: The revocation / suspension status is checked via OCSP IETF RFC 6960; - BothCheck: Both checks are performed through OCSP and CRL; - EitherCheck: Checks are made through OCSP or through CRL; - NoCheck: No checks	eitherCheck
(M) 2.2. RevocationFreshnessConstraints: This restriction indicates the timing requirements of the revocation / suspension information. The restrictions can indicate the maximum acceptable difference between the date of issuance of the information on the status of revocation / suspension of the QES / QESeal certificate and the time of validation or require that SVA accept only the information for revocation / suspension.	DO NOT

issued at a specified time after the creation / generation of QES / QESeal.	
(M) 2.3. RevocationInfoOnExpiredCerts: This restriction imposes that the QES certificate used in its validation be issued by a Certificate Authority (CA), which supports the updates of certificates NOT revoked / suspended even after they have expired for a period longer than a certain lower limit.	
(M) 3. LoAOnTSPPractices: This restriction indicates the level of agreement (LoA) regarding the practices of TSP (s), which issue the QES / QESeal certificate to be confirmed during the validation process in the way of certificates.	DO NOT
EUQualifiedCertificateRequired	YES
EUQualifiedCertificateSigRequired	YES
EUQualifiedCertificateSealRequired 1	YES

3.4.4. Cryptographic limitations

Cryptographic restrictions on the algorithms and parameters used in the creation of QES / QESeal, as indicated in ETSI TS 119 172-1, clause A.4.2.1, Table A2, row (p).

Limitation	Constraint value in the QES validation / QESeal
(P) 1. CryptographicSuitesConstraints: This restriction indicates requirements for the algorithms and parameters used in the creation of QES / QESeal, or used in the validation of signatures / stamps of objects included in the validation process (for example QES / QESeal, certificates, CRLs, OCSP- Seal stamps / TSTs).	In accordance with ETSI TS 119 312

3.4.5. Limitations of the elements of the signature

Restrictions regarding QES / QESeal elements that indicate DTBS (Data To Be Signed) requirements, according to ETSI TS 119 172-1, clause A.4.2.1., Table A. 2, row (b).

Limitation	Constraint value in the QES / QESeal validation (SVA or DA)
B) 1. ConstraintOnDTBS: This restriction indicates the requirements on the type of data to be signed / sealed by the signer / sealing person.	DO NOT
(B) 2. ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints shows the NOT required information elements related to the content, in the form of the requirements	

signed or unsigned qualifications present in QES / QESeal. The set includes: (B) 2.1 MandatedSignedQProperties-DataObjectFormat requires a specific format of the content to be signed / stamped by the person signatory. (B) 2.2 MandatedSignedQProperties-content- requires information hints specific describing internal content signed / multilayer sealing Messages in which one content is encapsulated in another in order to be signed by the signer. (B) 2.3 MandatedSignedQProperties-content-reference requires the inclusion of information on how to connect a request and a message response within an exchange between both parties or how the connection should be made, etc. (B) 2.4 MandatedSignedQProperties-content-identifier requires the presence and eventually a specific value of an identifier to be used later in the signed attribute that qualifies "contentreference".	
(b) 3. DOTBSAsAWholeOrInParts: This constraint shows if the data or just a specific part / s of it should be signed. The semantics of a possible set of required values used to indicate these requirements is defined, as follows: • Whole: all data must be signed; • Parts: only certain part / s of the data must be signed. In this case, additional information is used to indicate which parts should be signed / sealed.	DO NOT

3.4.6. Limitations of formats and levels supported by QES / QESeal

The qualified service of validation of signatures / advanced / qualified electronic stamps (QSVS) of ANF AC, supports the following formats of QES / QESeal,

- XAdES - ETSI EN 319 132
- CAdES - ETSI EN 319 122
- PAdES - ETSI EN 319 142

and levels

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

3.4.7. Supported QES / QESeal restrictions

Signature / stamp position and signed data object	Value
Covering QES / QESeal - the signature / stamp covers the data object	YES
Covered (type "letter") QES / QESeal - The signed data object covers the signature / stamp	YES
Separate QES / QESeal - Signature / stamp and data object are separate (independent)	YES
Simultaneously, positions were repeatedly compared A	YES
document has more than one QES / QESeal	YES

3.4.8. Validation of qualified electronic signatures in accordance with eIDAS: Art. 32 and 33

Art. 32 and 33 of Regulation (EU) No. 910/2014 Art. 32. *Requirements*	**Execution of the Service**
for the validation of qualified electronic signatures	
1. In the process of validating a qualified electronic signature, the validity of the qualified electronic signature is confirmed, providing that:	
A) the certificate justifying the signature in the at the time of signing it was a qualified certificate for an electronic signature, which corresponds to the annex I.	The certificate validation process complies with the requirements described in EU 2015/1505 and ETSI 319 412-5 Annex A.1 for the QTSP that issues qualified certificates for electronic signature.
B) the qualified certificate has been issued by a qualified fiduciary service provider and has been valid at the time of signing.	The certificate validation process complies with the requirements described in EU 2015/1505 and ETSI 319 412-5 Annex A.1 for the QTSP that issues qualified certificates for electronic signature.
C) the signature validation data Correspond to the data provided by the relying party.	It is guaranteed through the QES / QESeal formats.
D) the unique set of data, representing the signer of the electronic signature on the certificate, will deliver to the trusting party.	The signing certificate for QES / QESeal is included in the answer by the validations for each protocol supported according to this document.
E) if at the time of signing a pseudonym, this has been clearly stated to the trusting part.	Subject is used only at the express request of the client and after a preliminary agreement between them and the QTSP, the requirements of ETSI EN319 4122 will apply in accordance with this document. Since the pseudonym indication in the field
F) the electronic signature has been created by a device for creating electronic signature qualified.	The certificate validation process complies with the requirements described in EU 2015/1505 for the QTSP that issues qualified certificates. Is done a check for the type of SSCD (QSCD) required.
G) the integrity of the signed data is not engaged.	It is guaranteed through the validation model supported indicated in this document.
H) the requirements cited in art. 26 have been fulfilled at the time of signing.	It is guaranteed through the validation model supported indicated in this document.

2. The system used for the validation of the qualified electronic signature provides the participant the correct result of the validation process and allows to find possible problems related to safety.	The QES / QESeal validation process and the statusindication after check are described in this document.
Art 33. *Qualified validation service for qualified electronic signatures*	
1. Only a qualified provider of trust services may provide a qualified validation service for qualified electronic signatures that:	
A) carry out the validation in accordance with article 32, paragraph 1, and	See previous table on Article 32 (1).
B) allow the user parties to receive the result of the validation process of a automated way that is reliable, efficient and include electronic signature advanced or advanced electronic seal of the qualified service provider of validation.	Users receive, in an automated way, a Qualified validation report stamped by ANF Certification Authority, using the certificate qualified electronic seal that identifies the service ("Digital identity") in the European TSL.
Art. 28. *Qualified certificates for electronic signatures*	
1. Qualified certificates for signatures electronic correspond to the requirements set out in Annex I.	It corresponds to the requirements of ETSI 119 412-5, Annex A.1.
2. Qualified certificates for electronic signatures are not subject to any mandatory requirement that exceeds the requirements established in Annex I.	The certificate validation process complies with the requirements described in EU 2015/1505 for trusted lists. No additional controls are required except those indicated in Annex I of the Regulation.
3. Qualified certificates for signatures electronic data may include additional data do not obligatory. These data do not affect the operational compatibility and recognition of qualified electronic signatures.	No additional controls are required except those indicated in Annex I of the Regulation.
4. If a certificate qualified for electronic signature is revoked after its initial activation, it loses its validity from the moment of revocation and its status cannot be restored under any circumstances.	In accordance with the Policy and Practice for QES / QESeal Qualified Trust Services.
5. Member States may determine national rules regarding suspension temporary validity of the accredited certificate for the electronic signature complying with the following terms:	In accordance with ETSI TS 110 102-1 if in the certificate validation a result is processed validation / wrong answer is received due to to the suspended QES / QESeal certificate, the Service the validation process will end. The indication of is INDETERMINATE and the additional code TRY_LATER with the time of suspension and, if any, the nextUpdate field of the CRL or OCSP-response is used to determine the next validation.
A) if the certificate qualified for the signature electronics is temporarily suspended, loses its validity for the term of the suspension	
B) The duration of the suspension is indicated clearly in the database of	

certificates and the status of the suspended certificate is visible during the term of the in-service suspension, providing information about the certificate status	
***Art. 26.** Requirements for advanced electronic signatures*	
The advanced electronic signature corresponds to the following requirements: A) is uniquely	
related to the signer of the Guaranteed through supported formats *the signature* with AdES.	
B) can identify the signer of the signature	Guaranteed through AdES compatible formats.
C) has been created through data for the creation of electronic signatures that the signer of the signature Guaranteed through supported formats *electronics can use with high reliability and* with AdES. *solely under your control; Y*	
D) It relates to the data signed with him from a way that It allows meet any consecutive modification on them	Guaranteed through AdES compatible formats.

3.4.9. Signature of the qualified validation report

ANF AC, in its capacity as SVSP, signs the qualified validation reports using a qualified electronic seal using a Hardware Security Module (HSM), certified in accordance with Common Criteria ISO 15408 EAL 4 +. The keys (public - private) have been generated inside this cryptographic device.

In case of making backup copies of the keys, the keys will be protected to guarantee their integrity and confidentiality by the cryptographic module before being stored outside that device.

The signature is PAdES level LT or XAdES level LT, depending on the format of the report PDF or XML respectively. ANF AC as PCSC provides the service of qualified electronic stamps and qualified electronic time stamps.