# Validation Policy

## Qualified electronic Signatures and Seals (QES) validation service





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

Phone: 902 902 172 (Calls from Spain)

International +34 933 935 946

Website: www.anf.es

**Security Level**

*Public document*

---

**Important notice**



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

Phone: 902 902 172 (Calls from Spain) International (+34) 933 935 946

Website: 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 Regulation (EU) No. 910/2014 of the European Parliament and of the Council, and with section i.6 of the COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of September 8, 2015 (of in accordance with Article 27 (5) and Article 37 (5) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council):

> *"Advanced electronic signatures and advanced electronic seals are similar from the technical point of view. Therefore, the standards for formats of advanced electronic signatures should apply mutatis mutandis to formats for advanced electronic seals.".*

This Validation Policy is subordinate to what is established in the Certification Practice Statement (CPS) of the ANF Autoridad de Certificación.

Regarding the qualified 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 specifications and standards 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 Signature Validation 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 Signature Validation Service Provider (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 in the matter, using operating procedures and information security management procedures that exclude any probability of data manipulation:

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

ANF AC's Validation service has been designed and developed in accordance with:

- **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:** Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation; 2;
- **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 sign tures 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;
- **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 qualified service provider for the validation of qualified electronic signatures and seals. 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 international organization IANA (Internet Assigned Numbers Authority), under the iso.org.dod.internet.private.enterprise branch (1.3.6.1.4.1 -IANA –Registered Private Enterprise-)..

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

- Qualified certificates for electronic signature
- Qualified certificates for electronic seal
- Qualified certificates for website authentication (SSL/TLS - QWAC)
- Qualified time stamping service
- Qualified service for the validation of qualified electronic signatures and seals
- Qualified service for the preservation of qualified electronic signatures and seals

- Qualified registered electronic delivery service (QERDS)

ANF AC, is certified in accordance with international standards:

- ISO 9001 for CAs
- ISO 27001 SGSI
- 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's systems are subject to compliance with the PCI-DSS standard.

### 1.1.2. Supported signature validation service policy(ies)

The QSVS works on the basis of a validation policy of signatures as input, that is, the validation of signatures / seals, is always performed against a validation policy. The validation policies accepted 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 is permanently updated and published at 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. Signature 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 a signature policy (creation), a standard commitment) and this can influence the validation of the signature..
- TSPs related to the signer:
  - The TSP that has issued the signer certificate (CA);
  - 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 TSP:
  - TSA;
  - other SVSPs to whom the SVSP may transmit a request;
  - etc.

- European or foreign trusted list providers; and
- 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 format verification, identification of the signer's certificate, validation context, X.509 validation, cryptographic validation, acceptance of the signature (i.e. the signature validation requirements), etc. According to ETSI TS 119 102-1 specification.

The signature / validation (DA) applications of ANF AC (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:
    - In exclusive configuration **(unqualified report)**
        - It requests a signature validation to the ANF CT component (CryptoAPI of the DA.)
        - he 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.
    - 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:
  - It executes the signature validation service protocol and processes the signature validation in the SVSPl;
  - It runs 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' Trusted Lists, the European Commission's Trusted Lists List, and / or other trusted lists.
    - etc.
  - Creates the qualified signature validation reports related to the application;
  - Creates the signature validation response.

### 1.2.3. Parties involved

- **Qualified Signature Validation Service Provider (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 corresponds to the client who hires the validation service and submits signatures and / or electronic seals to validation.
- **User**. Application or human being that interacts with a signature validation client.
- **Relying 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

- Acceptance of the signature, 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 validation of electronic signatures and seals (SVA)

- Signature validation application, an application that validates a signature against a signature validation policy, and 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, 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.
- Signature PoE, the signature existence proof, 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 seals and / or qualified validation service for qualified electronic signatures. For the purposes of this Policy, the provider is ANF AC.
- 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 signature'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
- Validation service, a system accessible through a communication network, which validates an electronic signature.
- Qualified validation service for qualified electronic seals, as specified in Regulation (EU) No. 910/2014 [i .1], 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 [i .1], Article 33. For the purposes of this Policy, the service is provided by ANF AC.
- Signature validation service server, computer equipment that implements the signature validation protocol and processes the signature / electronic seal validation.
- Subscriber, It 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, 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, verification process and confirmation of the validity of a certificate or an electronic signature.

- Signature validation, verification process and confirmation 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 verification, verification 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, the process of verifying the cryptographic value of a signature using signature verification data.
- Verifier, entity that wants to validate or verify an electronic signature.

### 1.3.2. Abbreviations

| | |
|---|---|
| **ANF AC:** | ANF Autoridad de Certificación |
| **VA:** | Validation Authorit |
| **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 |
| **QTSP:** | Qualified Trust Services Provider |
| **PoE**: | Proof of Existence |
| **QES**: | Qualified certificate for electronic signature |
| **QEseal**: | Qualified certificate for electronic seal |
| **QSVSP**: | Qualified Signature/Seal Validation Service Provider |
| **QSVS:** | Qualified Signature/Seal Validation Service |
| **SD**: | Signer's Document |
| **SDO**: | Signed Data Object |
| **SVA** : | Signature/Seal Validation Application |
| **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 Services Provider

**VPR**: signature Validation PRocess

## 1.4. Policies and practices

### 1.4.1. Organization administrating the TSP documentation

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

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

### 1.4.2. Contact person

| | |
|---|---|
| **Department** | Legal Department |
| **Email 1** | soporte@anf.es |
| **Email 2** | mcmateo@anf.es |
| **Department** | Technology and regulatory compliance |
| **Email 3** | pablo@anf.es |
| **Address** | Paseo de la Castellana, 79 |
| **Locality** | Madrid |
| **Postal Code** | 28046 |
| **Phone number** | 902 902 172 (Calls from Spain)<br>International (+34) 933 935 946 |

### 1.4.3. TSP (public) documentation applicability

| | | | |
|---|---|---|---|
| **Document name** | Validation Policy Qualified electronic Signatures and Seals (QES) validation service | | |
| **Version** | 2.7. | | |
| **OID** | 1.3.6.1.4.1.18332.56.1.1 | | |
| **Approval date** | 23/03/2022 | **Fecha de publicación** | 23/03/2022 |

| Version | Changes | Approval | Publication |
|---|---|---|---|
| 2.7. | Revisión anual. | 23/03/2022 | 23/03/2022 |
| 2.6. | Revisión anual. | 12/04/2021 | 12/04/2021 |
| 2.5. | ETSI TS 119 441 alignment technical corrections | 18/11/2020 | 18/11/2020 |
| 2.4. | Technical fixes | 15/01/2020 | 15/01/2020 |
| 2.3. | Annual review | 23/02/2019 | 23/02/2019 |
| 2.2. | Annual review | 05/06/2018 | 05/06/2018 |
| 2.1. | Annual review | 12/08/2017 | 12/08/2017 |
| 2.0. | Annual review | 16/03/2016 | 16/03/2016 |

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

- Certification Practices Statement OID 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
- Subscriber Service Contract OID 1.3.6.1.4.1.18332.5.1.4
- Risks evaluation OID 1.3.6.1.4.1.18332.80.6.3
- Risk Asessment Matrix OID 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 ANF AC corporate website in a Spanish and English language version in the different versions that have been approved, in case of discrepancy, the Spanish language version prevails.

# 2. Trust Service management and operation

## 2.1. Internal organization

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

### 2.1.1. Organization reliability

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

### 2.1.2. Segregation of duties

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 document ANF AC.
- 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 subjects of the certificates.

## 2.3. Asset management

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

## 2.4. Access control

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

## 2.5. Cryptographic controls

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

## 2.6. Physical and environmental security

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

## 2.7. Operation security

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

## 2.8. Network security

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

## 2.9. Incident management

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

## 2.10. Collection of evidence

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

## 2.11. Business continuity management

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

## 2.12. TSP termination plan

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

## 2.13. Compliance

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

# 3. Signature validation service design

## 3.1. Signature validation process requirements

When the signature validation service aims to validate qualified electronic signatures or seals 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

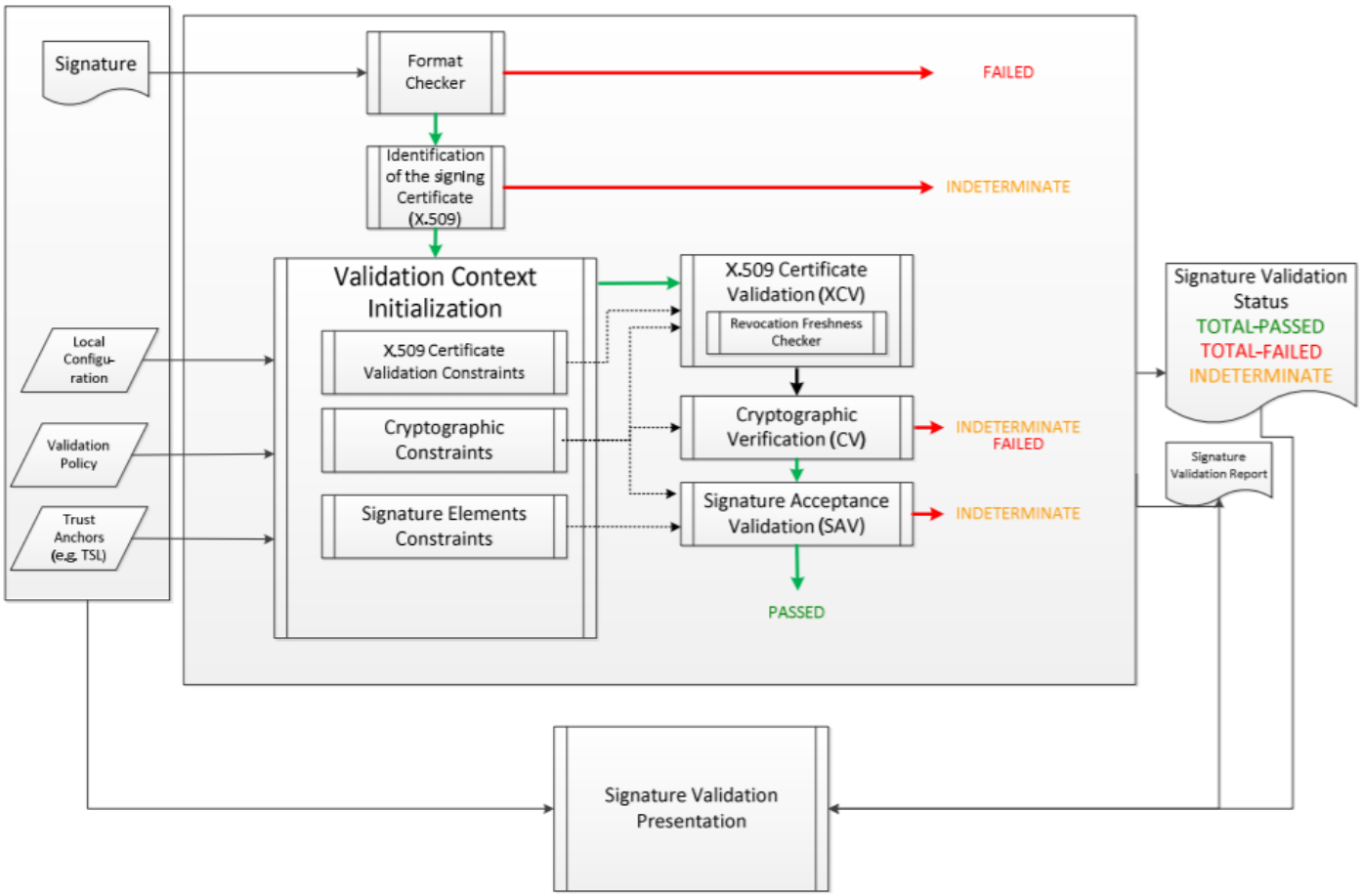


*Ilustración 1 Basic Signature Validation ETSI TS 119 172-1*

**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:<br>1. The signed document (s) (SD) and the signature (s) (SDO (s)) that signs them; or |

| | |
|---|---|
| | 2. the signed document (s) representation (s) (SDR (s)) and the signatures that sign them, to avoid exposing the content of the document to the validation service.<br><br>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 / seal. 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.<br><br>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.<br><br>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 procedure.** |
| | 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.<br>The validation response includes the validation reports. It includes the OID of the Service Policy and the OID of the signature validation policy used.<br>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 her responsibility, decides whether to accept the signature or not. |

## 3.2. Signature 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 seals

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 signing.

- 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 qualified 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.
- It provides the User Party with the correct result of the validation process (status indication and report) and allows them to 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 an 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's proof.
  Indicates that the entity providing that indication has sent the signed data (but not necessarily created 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 evidence.
  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. Indicates that the signature is intended solely to indicate having witnessed the signature of another person on the same document (signed data) which 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.En caso de que este documento indique requisitos y reglas específicos, prevalecerán sobre los pertinentes del 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, those contained in 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 are recorded, as well as the result of the

request (success or failure). 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 in the electronic signature, electronic seal, or issuance of a time stamp. OCSP responses shall 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 | Issuer 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 <certificado_ca>*
*-issuer <certificado_ia> -cert <certificado_a_consultar>*
*-url <url_de_verificación>*
*El campo <url_de_verificación > deberá ser el indicado en el campo "Authority Information Access" del certificado.*

Example to perform GET queries with open SSL:

*Se genera el request:*
*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*
*Se convierte a 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 / seal 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.

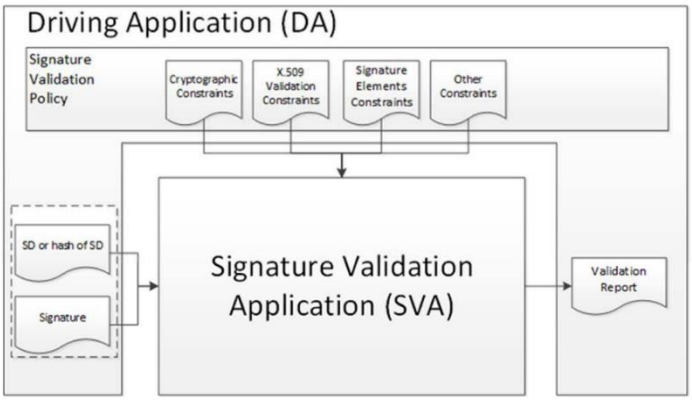


Figura: Modelo de validación de firma ETSI TS 119 102-1

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 seal. Exclusively for Windows OS.

- **Critical Acces**. It is an end-user desktop application. Exclusively for Windows OS,
- **Web Service**. This service is available in two modalities:
    - Web client that allows human user validations through the browser.
    - No interface to perform automatic validations. Available for Linux OS.

In every modality 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 all of them are validated.

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 seal validation processes in different formats:

- Validation process for the basic signature / seal 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 QTSP, 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. It follows the requirements established by ETSI TS 119 102-2 and ETSI TS 119 441. In the event that ANF AC decide to make any variation in them, this variation will be included in this policy.

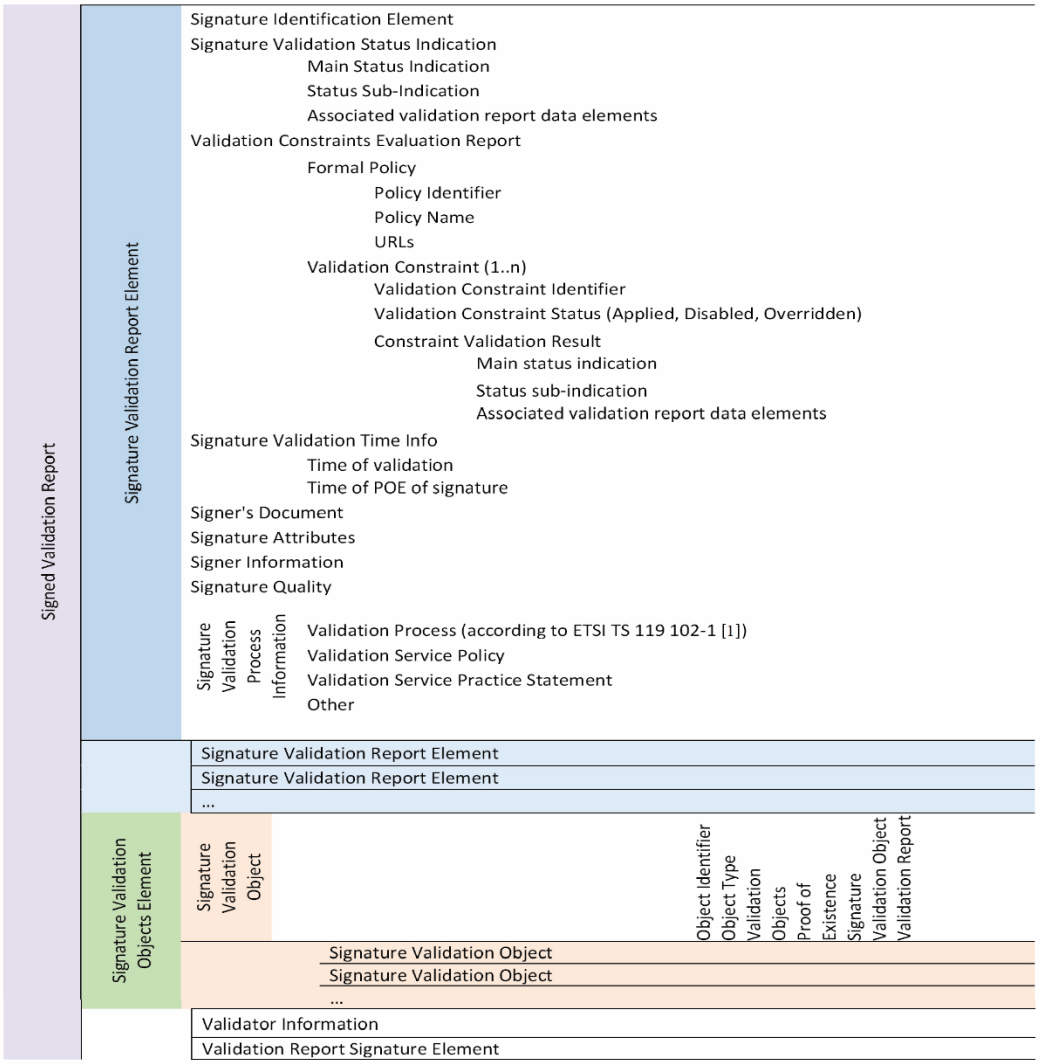


*Ilustración 2 Structure and elements of the validation report according to ETSI TS 119 102-2 v 1.2.1*

### 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) format, which details the validation of the signature / seal performed, which allows the DA to check in detail the decisions made during the validation and 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- PASSED** | The QES / QESeal validation process has a TOTAL-PASSED:<br>• QES / QESeal cryptographic checks have been successful (including verification of hashes of the different data objects, indirectly signed);<br>• positively validated the certification of the identity of the signer (ie the signature certificate is valid); and<br>• 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 TOTAL-FAILURE result because the cryptographic checks of the QES / QESeal<br>They are unsuccessful (including the 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 QC suspension time. | 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. |
| **UNDETERMINED** | The available information is not enough to carry out the validation process and determine the QES / QESeal status indication: TOTAL-PASS or TOTAL-FAILURE | The validation process provides information to explain the cause that results in “indeterminate”, and to help determine what data is missing to complete the validation process. |

The validation report includes the status indication for **TOTAL-FAILURE** and **UNDETERMINED**. 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**

| Status indication | Auxiliary cod | Semantics | Validation Report Data |
|---|---|---|---|
| **TOTAL-FAILURE** | HASH-FALLO | The QES / QESeal validation process leads to TOTAL-FAILURE, because at least one hash of an object that participates in the signature does not correspond to the hash registered in QES / QESeal. | The validation process provides an identifier that explicitly identifies a signature / seal object causing the error in the QES / QESeal. |
| | FORMATO-FALLO | QES / QESeal is not compatible with the supported standards indicated in this document at a level that does not allow the block to be processed cryptographically. | The validation process provides information on the failed process of the QES / QESeal |
| | SIG-CRYPTO-FALLO | The QES / QESeal validation process leads to FULL-FAILURE, because the value of the signature cannot be verified with the help of the public key of the QES / QESeal certificate. | The validation process is negative due to inconsistency of the QES / QESeal certificate. |
| | POLICY-FALLO | 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. |
| | REVOCADO | The QES / QESeal validation process leads to TOTAL-FAILURE because: the QES / QESeal certificate has been revoked, and<br>there is a test based on a Timetamping that determines that the Signature / seal is drawn up after the revocation of the certificate. | The validation process provides:<br>· The validation of the certification chain.<br>The date of revocation / suspension of the QES / QESeal certificate.<br>· CRL where applicable.<br>· Electronic QES / QESeal time stamp. |
| **UNDETERMINED** | SIG_CONSTR AINT_FAILURE | The QES / QESeal validation process leads to UNDETERMINED, because one or more attributes of QES / QESeal no correspond to the validation items. | The validation process provides:<br>• The certification chain used in the validation process.<br>• Additional information about the cause |

| | | | |
|---|---|---|---|
| | CHAIN_CONSTRAINTS_FAILURE | The QES / QESeal validation process leads to UNDETERMINED, because the certification chain used in the validation process does not correspond to the elements related to the validation certificate | The validation process provides:<br>• The certification chain used in the validation process.<br>• Additional information about the cause |
| | CERTIFICATE_CHAIN_GENERAL_FAILURE | The QES / QESeal validation process leads to UNDETERMINED, because the certification chain check shows an error due to an unstated reason. | The validation process provides:<br>Additional information on why. |
| | CRYPTO_CONSTRAINTS | The QES / QESeal validation process leads to UNDETERMINED, because at least one of the algorithms used or the size of the keys used with these algorithms is below the required level of cryptographic security and also:<br>The QES / QESeal certificates were generated after a time until these algorithms / keys were considered secure; and what's more:<br>QES / QESeal is not protected by a sufficiently reliable time stamp seal before the time until which the algorithms / keys are considered secure. | The validation process provides: An identification / designation of actual QES / QES or of a certificate generated with an algorithm or a key size below the required level of cryptographic security. |
| | EXPIRED | The QES / QESeal validation process 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 validity range of the certificate | |
| | CRYPTO_CONSTRAINT_FAILURE_NO_POE | At least one of the algorithms used in the QES / QESeal or in the corresponding certificates that participate in its validation or the size of the key is below the required level of cryptographic security and there is also no proof that the signatures / seals or these certificates have been generated before the time until which this algorithm / key has been considered secure. | The validation process provides:<br>Identification of QES / QESeal or the corresponding certificate Generated with Unacceptable Key Length or with an algorithm no meets cryptographic security requirements. |
| | 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 will be available at a later stage. | |
| | SIGNED_DATA_NOT_FOUND | Data for signature / seal cannot be received | The validation process provides:<br>The identifier (for example URI) of the data for the signature / seal that caused the error |
| | GENERIC | other reasons. | The validation process provides: Additional information showing why |

| | | | |
|---|---|---|---|
| | | | the validation status is UNDETERMINED |

### 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 QES / QESeal validation (SVA or DA) |
|---|---|
| (M) 1. X509 Restricción de validación de certificados: Este conjunto de restricciones se refiere a los requisitos en el proceso de validación de la cadena de certificación de conformidad con IETF RFC 5280. Las restricciones pueden ser diferentes para los diferentes tipos de certificados (por ejemplo, certificados de firma. Para respuestas OCSP, para listas CRL, sellos electrónicos de tiempo / TST). La semántica de un posible conjunto de valores requeridos que se utiliza para presentar estos requisitos se determina de la siguiente manera: | |
| (M) 1.1 SetOfTrustAnchors: Esta restricción indica un conjunto de Autoridades Certificadoras (TA) de confianza aceptables con el fin de limitar el proceso de validación. | EU (TSL) ECUADOR (TSL) PERU (TSL) REPUBLICA DOMINICANA (TSL) MEXICO (TSL) ARGENTINA (TSL) |
| (M) 1.2 CertificationPath: Esta restricción muestra la ruta de certificación utilizada por la SVA para la validación QES / QESeal. La ruta de certificación<br>Tiene "n" longitud desde el principio / la Autoridad Confianza (VA) hacia los certificados QES / QESeal utilizados al validar la firma. La restricción puede incluir el camino o indicar la necesidad de incluir el camino proporcionado a través del QES / QESeal, si lo hay. | |
| (m) 1.3. *user-initial-policy-set:* Pursuant to IETF RFC 5280 clausula 6.1.1 (c)<br>(m) 1.4. *initial-policy-mapping-inhibit*: Pursuant to IETF RFC 5280 clausula 6.1.1 (e)<br>(m) 1.5. *initial-explicit-policy*: Pursuant to IETF RFC 5280 clausula 6.1.1 (f)<br>(m) 1.6. *initial-any-policy-inhibit*: Pursuant to IETF RFC 5280 clausula 6.1.1 (g)<br>(m) 1.7. *initial-permitted-subtrees*: Pursuant to<br>IETF RFC 5280 clausula 6.1.1 (h)<br>(m) 1.8. *initial-excluded-subtrees*: Pursuant to<br>IETF RFC 5280 clausula 6.1.1 (i) | 100 Mb. |

| | |
|---|---|
| (m) 1.9. *path-length-constraints*: Esta limitación se refiere al número de certificados de la Autoridad Certificadora (CA) dentro de la cadena de certificación.<br>(m) 1.10. *policy-constraints*: Esta restricción se refiere a la (s) política (s) en el certificado QES / QESeal. | |
| (M) 2. RevocationConstraints: Este conjunto de restricciones se refiere a la verificación de estado de certificados QES / QESeal durante el proceso de validación.<br>Estas restricciones pueden ser diferentes para los diferentes tipos de certificados QES / QESeal. | |
| (M) 2. Restricciones de la revocación: Este conjunto de restricciones se refiere al QES / QESeal (m) 2.1. RevocationCheckingConstraints: Esta restricción se refiere a los requisitos para verificar el certificado QES / QESeal para la revocación / suspensión. Dichas restricciones especifican si el chequeo de la revocación / suspensión es necesario o no y si deben ser utilizadas OCSPresponses o CRL emitidas. La semántica para un posible conjunto de valores requeridos utilizados para presentar estos requisitos se define de la siguiente manera:<br>- ClrCheck: Las verificaciones se realizan en función de la CRL actual;<br>- OcspCheck: El estado de revocación / suspensión se comprueba a través de OCSP IETF RFC 6960;<br>- BothCheck: Ambos controles se realizan a través de OCSP y CRL;<br>- EitherCheck: Los checks se realizan a través de OCSP o mediante CRL;<br>- NoCheck: No checks | eitherCheck |
| (M) 2.2. RevocationFreshnessConstraints: Esta restricción indica los requisitos de tiempo de la información de revocación / suspensión. Las restricciones pueden indicar la diferencia máxima aceptable entre la fecha de emisión de la información sobre el estado de revocación / suspensión del certificado QES / QESeal y el tiempo de validación o exigir que SVA acepte solamente la información para revocación / suspensión emitida en un tiempo especificado después La creación / generación de QES / QESeal. | NO |
| (M) 2.3. RevocationInfoOnExpiredCerts: Esta restricción impone que el certificado QES utilizado en su validación sea emitido por una Autoridad Certificadora (CA), que admita las actualizaciones de los certificados revocados / suspendidos incluso después de haber caducado durante un período más largo que un límite inferior determinado. | NO |
| (M) 3. LoAOnTSPPractices: Esta restricción indica el nivel de acuerdo (LoA) con respecto a las prácticas de TSP (s), que emiten el certificado QES / QESeal para ser confirmados durante el proceso de validación en el camino de los certificados. | NO |
| EUQualifiedCertificateRequired | SI |

| | |
|---|---|
| EUQualifiedCertificateSigRequired | SI |
| EUQualifiedCertificateSealRequired 1 | SI |

### 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 QES / QESeal validation |
|---|---|
| (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 / seals 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 signature elements

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 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 person. | NO |
| (B) 2. ContentRelatedConstraintsAsPartOfSignatureElements: Este conjunto de restricciones muestra los elementos de información necesarios relacionados con el contenido, en la forma de los requisitos cualificados firmados o no firmados presentes en QES / QESeal. El conjunto incluye:<br>(B) 2.1 MandatedSignedQProperties-DataObjectFormat requiere un formato específico del contenido que debe firmar / sellar la persona firmante.<br>(B) 2.2 MandatedSignedQProperties-content-hints requiere información específica que describe el contenido interno firmado / sellado de multicapa<br>Mensajes en los que un contenido se encuentra encapsulado en otro para poder ser firmado por el firmante.<br>(B) 2.3 MandatedSignedQProperties-content-reference requiere la inclusión de información sobre la forma de conectar una solicitud y una | NO |

| | |
|---|---|
| respuesta del mensaje dentro de un intercambio entre ambas partes o la forma en que se debe realizar la conexión, etc.<br>(B) 2.4 MandatedSignedQProperties-content-identifier requiere presencia y eventualmente un valor específico de un identificador que se utilizará más adelante en el atributo firmado que califica "content-reference". | |
| (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:<br>• Whole: all data must be signed;<br>• 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. | NO |

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

The qualified service of validation of advanced/qualified electronic signatures/seal (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 y LTA
- CAdES – B – T - LT y LTA
- PAdES – B – T - LT y LTA

### 3.4.7. Supported QES/QESeal restrictions

| Signature / seal position and signed data object | Value |
|---|---|
| Covering QES/QESeal – la firma / sello cubre el objeto de datos | YES |
| Covered (type “letter”) QES/QESeal – El objeto de datos firmado cubre la firma / sello | YES |
| Separate QES/QESeal – La firma / sello y el objeto de datos están separados (independientes) | YES |
| Simultáneamente se compararon repetidamente posiciones | YES |
| Un documento tiene más de un 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 | Execution of the Service |
|---|---|
| **Art. 32. *Requirements for the validation of qualified electronic signatures*** | |
| *1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:* | |
| *A) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with 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 was issued by a qualified trust service provider and was 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 corresponds to the data provided to the relying party;* | It is guaranteed through the QES / QESeal formats. |
| *D) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;* | The signing certificate for QES / QESeal is included in the response by the validations for each supported protocol according to this document. |
| *E) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing.* | Since the pseudonym indication in the Subject field is used only at the express request of the client and after a preliminary agreement between them and the QTSP, the requirements of ETSI EN 319 412-2 in accordance with this document will apply. |
| *F) the electronic signature was created by a qualified electronic signature creation device;* | The certificate validation process complies with the requirements described in EU 2015/1505 for the QTSP that issues qualified certificates. A check is made for the type of SSCD (QSCD) required. |
| *G) the integrity of the signed data has not been compromised;* | It is guaranteed through the supported validation model indicated in this document. |
| *H) the requirements provided for in Article 26 were met at the time of signing.* | It is guaranteed through the supported validation model indicated in this document. |
| *2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.* | The QES / QESeal validation process and the status indication after the check are described in this document. |
| **Art. 33. *Qualified validation service for qualified electronic signatures*** | |
| *1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:* | |
| *A) provides validation in compliance with Article 32 (1); and* | See table above for Article 32 (1). |
| *B) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or* | Users receive, in an automated manner, a qualified validation report esealed by ANF Certification Authority, using the qualified certificate for electronic seal that identifies the QTS ("Digital identity") in the European TSL. |

| | |
|---|---|
| *advanced electronic seal of the provider of the qualified validation service.* | |
| ***Art. 28. Qualified certificates for electronic signatures*** | |
| *1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I..* | It corresponds to the requirements of ETSI 119 412-5, Annex A.1. |
| *2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.* | The certificate validation process complies with the requirements described in EU 2015/1505 for trusted lists.<br>No additional controls are required except those indicated in Annex I of the Regulation. |
| *3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.* | No additional controls are required except those indicated in Annex I of the Regulation. |
| *4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.* | In accordance with the Policy and Practice for QES / QESeal Qualified Trust Services. |
| *5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:* | In accordance with ETSI TS 110 102-1, if a validation result / erroneous response is received in the certificate validation due to the suspended QES / QESeal certificate, the Service will end the validation process. The status indication 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 a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension* | |
| *B) ) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate* | |
| ***Art. 26. Requirements for advanced electronic signatures*** | |
| *An advanced electronic signature shall meet the following requirements:* | |
| *A) it is uniquely linked to the signatory* | It is guaranteed through the AdES formats. |
| *B) it is capable of identifying the signatory* | It is guaranteed through the AdES formats. |
| *C) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and* | It is guaranteed through the AdES formats. |
| *D) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable* | It is guaranteed through the AdES 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 QTSP provides the service of qualified electronic seals and qualified electronic time stamps.