Política de Validación

Servicio Cualificado de Validación de firmas y sellos electrónicos cualificados (QES)

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

Teléfono: 932 661 614 (Llamadas desde España)

Internacional +34 933 935 946

Web: www.anf.es

Nivel de Seguridad

Documento Público

Aviso Importante

Dirección: Paseo de la Castellana, 79 - 28046 - Madrid (España)

Teléfono: 932 661 614 (llamadas desde España) Internacional (+34) 933 935 946

Web: www.anf.es

ÍNDICE

1. Introducción

1.1. Visión general

Este documento es la Política de Validación de ANF Autoridad de Certificación [ANF AC], en él se establecen las reglas de validación para las firmas electrónicas cualificadas y avanzadas (QES / AES), y para los sellos electrónicos cualificados y avanzados (QEseal / AESeal). Está en conformidad con el Reglamento (UE) n°910/2014 del Parlamento Europeo y del Consejo, y con el apartado i.6 de la DECISIÓN DE EJECUCIÓN (UE) 2015/1506 DE LA COMISIÓN de 8 de septiembre de 2015 (de conformidad con el apartado 5 del artículo 27 y el apartado 5 del artículo 37 del Reglamento (UE) nº 910/2014 del Parlamento Europeo y Del Consejo):

> *"Las firmas electrónicas avanzadas y los sellos electrónicos avanzados son similares desde el punto de vista técnico, por lo que las normas para los formatos de firmas electrónicas avanzadas deben aplicarse mutatis mutandis a los formatos de sellos electrónicos avanzados".*

Esta Política de Validación está subordinada a lo establecido en la Declaración de Prácticas de Certificación de ANF Autoridad de Certificación.

Respecto a la firma electrónica y el sello electrónico, cualificado, de conformidad con el Reglamento eIDAS y con esta Política, el resultado general de la validación no cambia, independientemente de si se trata de una firma / sello electrónico avanzado o cualificado, siempre que haya sido elaborado empleando un certificado cualificado de firma (QES), o un certificado cualificado de sello electrónico (QEseal).

La Infraestructura de Clave Pública (PKI) de ANF AC es administrada en conformidad con el marco legal del Reglamento [UE] 910/2014 del Parlamento Europeo, y con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza de España.

Este documento ha sido elaborado de conformidad con la legislación vigente de España y las especificaciones y normas paneuropeas para la prestación de servicios de confianza. Su estructura sigue la recomendación del Anexo A ETSI TS 119 441.

Esta política de validación de firmas establece el conjunto de restricciones procesadas o para ser procesadas por el servicio de validación (SVA). Este servicio funciona sobre la base de una política de validación de firmas como entrada. La política de validación soportada por el SVA de ANF AC está definida en el apartado 1.1.2 de este documento.

ANF AC es el Prestador Cualificados del Servicio de Validación de Firmas y Sellos Electrónicos (QSVSP) y proporciona este servicio cualificado de validación (QSVS).

Este servicio comprueba que los archivos firmados/sellados sometidos a validación cumplen los requisitos del Reglamento eIDAS y estándares en la materia, utilizando procedimientos operativos y procedimientos de gestión de la seguridad de la información que excluyen cualquier probabilidad de manipulación de datos:

- Comprueba la validez de QES / AES y QEseal / AESeal.
- Verifica certificados cualificados: verificando calificación, integridad, autenticidad y vigencia.
- Verifica certificados TSA/TSU: verificando calificación, integridad, autenticidad y vigencia.
- Verifica sellos cualificados de tiempo electrónico: verificando calificación, integridad, autenticidad.

El servicio de Validación de ANF AC ha sido diseñado y desarrollado en conformidad con las normas:

- **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 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 TS 119 312:** Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- **ETSI TS 119 612**: Electronic Signatures and Infrastructures (ESI); Trusted Lists
- **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. Identificación del TSP

ANF Autoridad de Certificación [ANF AC], es el prestador del servicio cualificado de validación de firmas y sellos electrónicos cualificados. Es una entidad jurídica constituida al amparo de la Ley Orgánica 1/2002 del 22 de marzo e inscrita en el Ministerio del Interior con el número nacional 171.443 y NIF G-63287510.

ANF AC utiliza OIDs según el estándar ITU-T Rec. X.660 y el estándar ISO/IEC 9834-1:2005 y tiene asignado el código privado de empresa (SMI Network Management Private Enterprise Codes) 18332 por la organización internacional IANA (Internet Assigned Numbers Authority), bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 -IANA –Registered Private Enterprise-).

ANF AC es prestador cualificado en los siguientes servicios de confianza eIDAS:

- Certificados cualificados de firma electrónica
- Certificados cualificados de sello electrónico

- Certificados cualificados de autenticación web (SSL/TLS - QWAC)
- Servicio de sellado de tiempo cualificado
- Servicio cualificado de validación de firmas y sellos electrónicos cualificados
- Servicio cualificado de conservación de firmas y sellos electrónicos cualificados
- Servicio cualificado de entrega electrónica certificada

ANF AC, está certificada en conformidad con las normas internacionales:

- ISO 9001 Sistema de Gestión de la Calidad
- ISO 27001 SGSI
- ISO 14001 Medio ambiente

Además, como miembro de Global Compact de la ONU, ANF AC respeta los 10 principios establecidos y asume la norma ISO 26000. Los sistemas de ANF AC son sometidos a cumplimiento de la norma PCI-DSS

1.1.2. Política(s) de servicio de validación admitidas

El QSVS funciona sobre la base de una política de validación de firmas como entrada, es decir, la validación de firmas / sellos, se realiza siempre contra una política de validación. Las políticas de validación admitidas y cuyos requerimientos son utilizados para realizar el proceso son:

Política Validación de ANF AC	OID 1.3.6.1.4.1.18332.56.1.1
Se ajusta a los criterios de validación ETSI TS 119 441	OID 0.4.0.19441.1.1
Se ajusta a los criterios de validación cualificada ETSI TS 119 441	OID 0.4.0.19441.1.2
Se ajusta a los criterios de validación cualificada ETSI TS 119 172-4	OID 0.4.0.191724

Esta Política de Validación de ANF AC permanentemente actualizada y publicada en https://www.anf.es

El informe de validación especifica la clave y nivel de firma / sello electrónico validado. El tercero que confía es el responsable de determinar su aplicabilidad al propósito comercial y, por tanto, su aceptación o rechazo.

1.2. Componentes del servicio de validación

1.2.1. Actores SVS

El servicio de validación contempla la participación de:

- El firmante puede restringir / limitar la firma (por ejemplo, mediante una política de firma (creación), un compromiso tipo) y esto puede influir en la validación de la firma.
- TSP relacionados con el firmante:
  - El TSP ha emitido el certificado de firmante (CA);
  - Cualquier TSP que pueda estar implícito en la generación de firmas:
    - el TSP que maneja el (Q) SCD en nombre del firmante;
    - el TSP que genera la firma;
    - TSA;
    - VA, respuesta OCSP,
    - etc.

- Otros TSP:
  - TSA;
  - otros SVSP a quienes el SVSP puede transmitir una solicitud;-
  - etc.
- Los proveedores de listas de confianza europeos o extranjeros; y
- La Comisión Europea proporciona la lista de listas de confianza.

1.2.2. Arquitectura del servicio

El servidor del servicio de validación de firma (SVSServ) implementa el SVA, es decir, la aplicación realiza verificación del formato, la identificación del certificado del firmante, el contexto de validación, la validación X.509, la validación criptográfica, la aceptación de la firma (es decir, los requerimientos de la firma validación), etc. según la especificación ETSI TS 119102-1.

Las aplicaciones de firma / validación (DA) de ANF AC (Safe Box y critical Access) pueden configurarse para operar exclusivamente del lado del cliente (p.ej. cuando no tienen conexión a internet), o compartida en modalidad cliente y servidor (mediante conexión a Internet con el servidor del servicio de validación de firmas (SVSServ).

Los servicios de validación se dividen en los siguientes componentes:

- El cliente de validación de firmas es un componente o una pieza de software que implementa la validación de firmas. En particular:
  - En configuración exclusiva (**informe no cualificado**)
    - Solicita una validación de firma al componente ANF CT (CriptoAPI del DA).
    - El DA permite solicitar validación de una firma o múltiples validaciones de firma.
    - El DA ejecuta el protocolo de validación de firmas exclusivamente del lado del usuario.
    - El DA elabora el informe de validación.
    - Se realiza la presentación del informe de validación.
    - El cliente dispone de:
      - Una interfaz de usuario para ingresar manualmente la solicitud.
      - Una interfaz de usuario para presentar el informe.
  - En configuración compartida (**informe cualificado**)
    - Solicita una validación de firma al SVSServ.
    - El servicio permite solicitar validación de una firma o múltiples validaciones de firma.
    - Ejecuta el protocolo de validación de firmas (SVP) del lado del usuario.
    - En su caso, se ocupa de la presentación del informe de validación y firma.
    - El cliente dispone de:
      - Una interfaz de usuario para ingresar manualmente la solicitud.
      - Una interfaz de máquina para solicitudes automatizadas.

- Una interfaz de usuario para presentar el informe y validar la firma que lo autentica.

- El servidor de servicio de validación de firmas (SVSServ), implementa el protocolo de validación de la firma por parte del SVSP. En particular:
  - Ejecuta el protocolo de servicio de validación de firmas y procesa la validación de firmas en el SVSPl;
  - Ejecuta la aplicación de validación de firma (SVA) como se define en ETSI TS 119 102-1, que implementa el algoritmo de validación definido en ETSI TS 119 102-1. Para ello, el servicio consulta entre otros:
    - La CA que ha emitido el certificado del firmante (para los servicios de información de estado de certificado (s) (solo se realiza consulta a respondedor OCSP, no se realiza consulta de Lista de Revocación CRL).
    - La CA de la (s) TSA (s) que han proporcionado marcas de tiempo dentro de la firma.
    - Otros SVSP para controles complementarios.
    - Lista de Confianza del país en el que opera el PCSC emisor, y / u otras listas de confianza.
    - etc.
  - Crea los informes cualificados de validación de firmas relacionados con la solicitud;
  - Crea la respuesta de validación de firmas.

1.2.3. Partes que intervienen

- **Prestador cualificado de servicios de validación (QSVSP).** En el contexto de este documento ANF AC. ANF AC asume la responsabilidad general del servicio de validación, incluso cuando algunas funciones sean asumidas por terceros contratados.
- **Suscriptor.** Corresponde al cliente que contrata el servicio de validación y somete a validación firmas y/o sellos electrónicos.
- **Usuario.** Aplicación o ser humano que interactúa con un cliente de validación de firmas.
- **Tercero que confía.** Terceros que sin ser el suscriptor o el usuario, están autorizados a acceder a los informes de validación cualificada y confían en ellos.

1.3. Definiciones y abreviaciones

1.3.1. Definiciones

- Aceptación de la firma, verificación técnica a realizar sobre la propia firma o sobre los atributos de la firma.
- Aplicación de firma/validación, suite de utilidades que permiten elaborar firmas electrónicas AdES y validación de firmas y sellos electrónicos (SVA).

- Aplicación de validación de firmas, aplicación que valida una firma contra una política de validación de firmas, y que emite una indicación de estado (es decir, el estado de validación de la firma) y un informe de validación de la firma. La aplicación de validación de ANF AC está en conformidad con la ETSI TS 119 102-1.
- Cliente de validación de firmas, componente de software que implementa el protocolo de validación de firmas al usuario.
- Datos de validación, datos que se utilizan para validar una firma electrónica.
- Estado de validación de la firma, una de las siguientes indicaciones: TOTAL-APROBADO, TOTAL-FALLO o INDETERMINADO.
- Informe de validación de firmas, informe completo de validación elaborado por la aplicación de validación de firmas. Permite inspeccionar los detalles de las valoraciones tomadas durante la validación e investigar las indicaciones de estado detalladas por la aplicación de validación. El informe elaborado por el servicio de validación de ANF AC cumple los requisitos establecidos por la ETSI TS 119102-1 y el informe se elabora conforme a la ETSI TS 119102-2
- PoE de firma, la prueba de existencia de firma, es el objeto de datos de firma el cual es reseñado en el informe de validación.
- Política de validación de firmas, conjunto de restricciones de validación de firmas que son procesadas por la aplicación de validación que determinan el resultado de la validación (APROBADO,FALLO o INDETERMINADO).
- Prestador de servicios de validación cualificado, SVSP que proporciona un servicio de validación cualificado para sellos electrónicos cualificados y/o servicio de validación cualificado para firmas electrónicas cualificadas. A efectos de esta Política el prestador es ANF AC.
- Reglas de aplicabilidad de firmas, conjunto de reglas, aplicables a una o más firmas electrónicas, que define los requisitos para determinar si una firma es adecuada para un negocio o un propósito legal en particular.
    - El propietario de las reglas de aplicabilidad de la firma suele ser la parte que confía y estas reglas pueden ser compartidas por una comunidad. Las reglas de aplicabilidad de firmas pueden manejarse mediante una extensión del servicio proporcionado por el QSVSP que ofrecerá verificación de aplicabilidad.
- Restricción de creación (firma), criterios utilizados al crear una firma digital.
- Restricción de validación de firmas, criterios técnicos con los que se puede validar una firma electrónica. El servicio de validación de ANF AC sigue las especificaciones de la ETSI TS 119102-1.
- Servicio de validación, sistema accesible a través de una red de comunicación, que valida una firma electrónica.
- Servicio de validación cualificado para sellos electrónicos cualificados, según se especifica en el Reglamento (UE) nº 910/2014 [i .1], Artículo 40. A efectos de esta Política el servicio es el proporcionado por ANF AC.
- Servicio de validación cualificado para firmas electrónicas cualificadas, según se especifica en el Reglamento (UE) nº 910/2014 [i .1], Artículo 33. A efectos de esta Política el servicio es el proporcionado por ANF AC.
- Servidor de servicio de validación de firmas, equipamiento informático que implementa el protocolo de validación de firmas y procesa la validación de firma / sello electrónico.
- Suscriptor, corresponde al cliente, persona física o jurídica, que contrata el servicio de validación y somete a validación firmas y/o sellos electrónicos.

- Tipo de compromiso, indicación aceptada por el firmante de la implicación exacta de una firma electrónica.
- Usuario, aplicación o ser humano que interactúa con un cliente de validación de firmas.
- Validación, proceso de verificación y confirmación de la validez de un certificado o una firma electrónica.
- Validación de firma, proceso de verificación y confirmación de que una firma digital es técnicamente válida.
- Validación de la firma electrónica cualificada, según se especifica en el artículo 32 del Reglamento (UE) nº 910/2014.
- Validación de sello electrónico cualificado, según se especifica en el artículo 40 del Reglamento (UE) nº 910/2014.
- Verificación de aplicabilidad, parámetros de verificación para determinar si una firma se ajusta a las reglas de aplicabilidad de la firma se puede proporcionar como complemento del servicio de validación de firmas definido ETSI TS 119 441. Tiene un mayor alcance que la validación especificada en la citada ETSI TS.
- Verificación de firma, proceso de verificación del valor criptográfico de una firma utilizando datos de verificación de firma.
- Verificador, entidad que quiere validar o verificar una firma electrónica.

1.3.2. Abreviaciones

ANF AC: ANF Autoridad de Certificación

AV: Autoridad de Validación

HSM: Módulo de Seguridad Criptográfica en conformidad con una certificación Common Criteria ISO 15408 EAL 4+ o FIPS PUB 140-2 nivel 3

OCSP: protocolo de comprobación del Estado de un certificado en línea

PCSC: Prestador Cualificado de Servicios de Confianza

PoE: prueba de existencia

QES: certificado cualificado de firma electrónica

QEseal: certificado cualificado de sello electrónico

QSVSP: Prestador Cualificado de Servicios de Validación de firmas / sellos

QSVS: Servicio Cualificado de Validación de firmas / sellos

SD: documento del firmante

SDO: objeto de datos firmado

SVA : aplicación de validación de firmas y sellos electrónicos

SVP: protocolo de validación de firmas

SVR: informe de validación de firmas

SVS: servicio de validación de firmas

SVSServ: servidor del servicio de validación de firma

TSA: Autoridad de Sellado de Tiempo

TSU: unidad de sellado de tiempo

TSP: Prestador de Servicios de Confianza

VPR: proceso de validación de firmas

1.4. Políticas y prácticas

1.4.1. Organización que administra la documentación del TSP

La Junta Rectora de la PKI es la responsable de la administración de esta Política y el conjunto de prácticas de certificación de ANF AC.

Departamento	Junta Rectora de la PKI
Correo electrónico	juntapki@anf.es
Dirección	Paseo de la Castellana, 79 Localidad Madrid – 28046 - España
Teléfono contacto nacional	902 902 172 (Llamadas desde España)
Teléfono contacto Internac.	(+34) 933 935 946

1.4.2. Persona de contacto

Departamento	Departamento Legal
Correo electrónico 1	soporte@anf.es
Correo electrónico 2	mcmateo@anf.es
Departamento	Tecnología y cumplimiento normativo
Correo electrónico 3	pablo@anf.es
Dirección	Paseo de la Castellana, 79
Localidad	Madrid
Código Postal	28046
Número de teléfono	902 902 172 (Llamadas desde España) Internacional (+34) 933 935 946

1.4.3. Aplicabilidad de la documentación pública

Nombre del documento	Política de Validación del Servicio Cualificado de Validación de firmas y sellos electrónicos cualificados		
Versión	2.9.		
OID	1.3.6.1.4.1.18332.56.1.1		
Fecha de aprobación	11/03/2024	**Fecha de publicación**	11/03/2024

Versión	Cambios	Aprobación	Publicación
2.9.	Revisión anual, cambios menores de redacción	11/03/2024	11/03/2024
2.8.	Revisión anual. Actualizar la referencia a la ETSI TS 119 172-4 V1.1.1 del 2021-05 (anteriormente en fase borrador).	14/03/2023	14/03/2023
2.7.	Revisión anual	23/03/2022	23/03/2022
2.6.	Revisión anual	12/04/2021	12/04/2021
2.5.	Correcciones técnicas alineación ETSI TS 119 441	18/11/2020	18/11/2020
2.4.	Correcciones técnicas	15/01/2020	15/01/2020
2.3.	Revisión anual	23/02/2019	23/02/2019
2.2.	Revisión anual	05/06/2018	05/06/2018
2.1.	Revisión anual	12/08/2017	12/08/2017
2.0.	Revisión anual	16/03/2016	16/03/2016

El identificador de esta Política de Certificación sólo será cambiado si se producen cambios sustanciales que afectan a su aplicabilidad.

La entrada en vigor de una nueva versión se produce en el momento de su publicación, la política es publicada en la Web corporativa de ANF AC www.anf.es

- Declaración de Prácticas de Certificación OID 1.3.6.1.4.1.18332.1.9.1.1
- Términos y Condiciones OID 1.3.6.1.4.1.18332.5.1.5
- Contrato de Prestación de Servicios OID 1.3.6.1.4.1.18332.5.1.4
- Evaluación de Riesgos OID 1.3.6.1.4.1.18332.80.6.3
- Matriz análisis de Riesgos OID 1.3.6.1.4.1.18332.13.2.1
- Plan de continuidad de negocio y recuperación de desastres OID 1.3.6.1.4.1.18332.13.1.1
- Servicio de Validación Cualificada -Procedimiento – Interpretación - Evidencias– Batería de pruebas OID 1.3.6.1.4.1.18332.56.1.2

El organismo encargado de revisar y aprobar en su caso esta política es la Junta Rectora de la PKI, máxima autoridad en la organización ANF AC. Esta política será revisada al menos una vez al año, y siempre que se produzcan cambios asi lo requiera, verificando que esté en harmonía con la Declaración de Prácticas de Certificación de ANF A y su adenda.

Esta política es publicada en la Web corporativa de ANF AC en versión de idioma español e inglés en las distintas versiones que han sido aprobadas, en caso de discrepancia, prevalece la versión de idioma español.

2. Gestión y operación del servicio de confianza

2.1. Organización interna

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.1.1. Confiabilidad de la organización

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.1.2. Segregación de funciones

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

- Prestador del servicio cualificado de validación, en el contexto de este documento ANF AC.
- Suscriptores, corresponde a los terceros que confían en el servicio de validación y someten a validación firmas y/o sellos electrónicos.
- Usuarios, corresponde a la aplicación o ser humano que interactúa con la aplicación de firma/validación sobre un cliente de validación de firmas.

2.2. Recursos humanos

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.3. Gestión de activos

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.4. Control de accesos

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.5. Controles criptográficos

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.6. Seguridad física y ambiental

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.7. Seguridad operativa

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.8. Seguridad de la red

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.9. Administración de incidentes

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.10. Recolección de evidencias

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.11. Plan de continuidad de negocio y recuperación de desastres

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.12. Plan de cese

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

2.13. Conformidad

Según lo definido en la DPC de ANF AC en cuanto a los sujetos signatarios de los certificados.

3. Diseño del servicio de validación de firmas

3.1. Requisitos del proceso de validación

Cuando el servicio de validación de firmas tiene como objetivo validar firmas o sellos electrónicos cualificados como los definidos en el Artículo 32.1 del Reglamento (UE) No 910/2014, el proceso de validación seguirá los requisitos de ETSI TS 119 172-4 V1.1.1 *(2021-05).*

3.1.1. Proceso de validación de firma al SVSServ sigue el algoritmo de ETSI TS 119 102-1

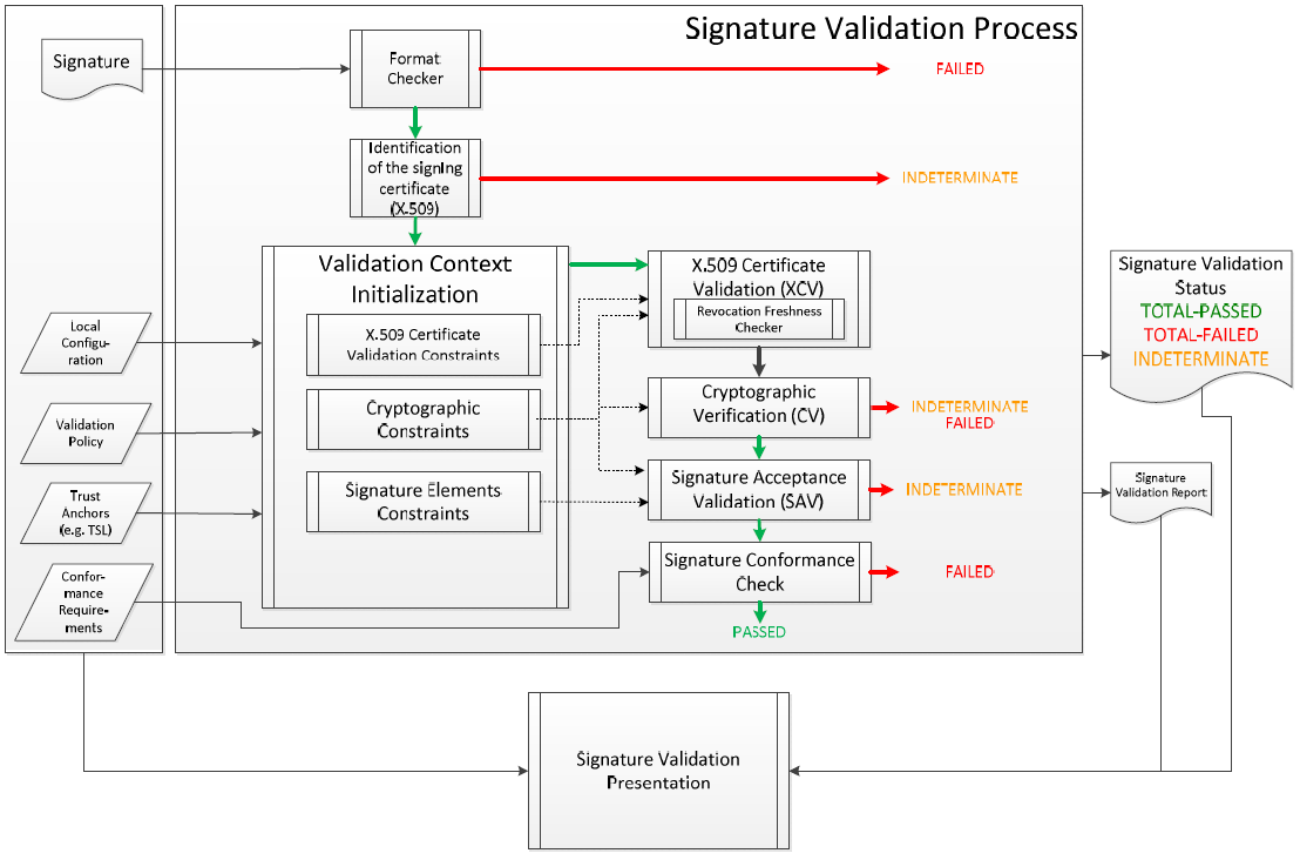

Ilustración 1 Basic Signature Validation ETSI TS 119 172-1

Procedimiento funcional del servicio de validación:

Paso 1	El cliente genera y envía una solicitud de validación de firma a ANF AC. Los protocolos que respaldan la solicitud y la respuesta se corresponden con la especificación ETSI TS 119 442. La solicitud incluye: 1. El documento/s firmado/s (SD) y la firma/s (SDO) que los firma; o

	2. los documentos firmados/s representación/es (SDR) y las firmas que los firman, para evitar exponer el contenido del documento al servicio de validación. El mapeo entre los documentos firmados y sus resúmenes utilizados dentro de las firmas es esencial al verificar una firma. En conformidad con el Reglamento (UE) nº 910/2014, el vínculo entre el documento firmado y la firma es parte de las condiciones para una firma / sello electrónico avanzado. Sin embargo, debido a razones de confidencialidad o rendimiento, hay casos de uso en los que es preferible enviar sólo los resúmenes hash de los documentos firmados. En este caso, la verificación de integridad del documento firmado y su correspondencia con la firma, queda fuera del control y la responsabilidad del SVSServ. En otros casos, es el componente de ANF AC el que calcula el valor hash de los documentos firmados, o cualquier atributo como archivo atributos, En este caso, ANF AC garantiza que la integridad de los documentos no se ha visto comprometida durante el proceso. En cualquiera de los supuestos, los hash esperados son calculados con las mismas funciones hash que las utilizadas en la firma.
Paso 2	**SVSServ realiza el proceso de validación.**
	El proceso de validación se corresponde con la especificación ETSI TS 119 102-1]. La validación la realiza el SVSP de acuerdo con la presente política de validación de firma. La firma del proceso de validación sigue lo establecido en la ETSI TS 119 102-1.
Paso 3	**El SVSServ prepara y envía la respuesta de validación.**
	Los protocolos que respaldan la solicitud y la respuesta son los especificados en ETSI TS 119 442. La respuesta de validación incluye los informes de validación. Incluye el OID de la Política de Servicio y el OID de la política de validación de firmas utilizada. El informe de validación se corresponde con la especificación ETSI TS 119102-2, y está firmado por sello electrónico de ANF AC.
Paso 4	**Presentación del informe de validación**
	El cliente puede ofrecer un módulo de presentación de validación de firma para presentar el informe de validación que especifica el resultado y proporciona informe detallado de cada uno de los atributos firmados. El usuario, bajo su responsabilidad decide si acepta la firma o no.

3.2. Requisitos del protocolo de validación

El protocolo de validación empleado por ANF AC cumple con ETSI TS 119 442 *"Protocol profiles for trust service providers providing AdES digital signature validation services".*

3.2.1. Validación de firmas y sellos electrónicos

Los Servicios de Validación Cualificada de ANF AC permiten confirmar la validez de un QES / QEseal, siempre que:

- El certificado que respalda la firma / sello electrónico en el momento de la firma ha sido cualificado (QC) en conformidad con el anexo I del Reglamento eIDAS.

- El certificado cualificado ha sido emitido por un Prestador Cualificado de Servicios de Confianza y es vigente en el momento de la firma.
- Los datos de validación de la firma corresponden a los datos proporcionados por la Parte Usuaria.
- El conjunto único de datos que representa al Sujeto de la firma electrónica en el certificado ha sido debidamente entregado a la Parte Usuaria.
- Si en el momento de firmar se ha utilizado un seudónimo, y esto ha sido claramente indicado a la Parte Usuaria.
- La firma / sello electrónico ha sido creado por un dispositivo para la firma electrónica cualificada / creación de sello.
- La firma / sello electrónico ha sido creado empleando componentes criptográficos calificados como seguros.
- Si la firma / sello electrónico al crearlo ha sido sometido a una determinada política de firma electrónica autorizada por esta política.
- La integridad de los datos firmados no ha sido comprometida.
- Los requisitos para una firma electrónica avanzada (artículo 26 del Reglamento) se han cumplido en el momento de la firma.
- Proporciona a la Parte Usuaria el resultado correcto del proceso de validación (indicación de estado e informe) y le permite conocer cualquier problema relacionado con la seguridad.
- El servicio da a las Partes Usuarias la oportunidad de recibir el resultado del proceso de validación de una manera automatizada, confiable y eficaz, y que incluye una firma (o sello) cualificado de ANF AC como QTSP.
- El objeto de datos firmado debe contener en sus atributos los certificados necesarios.

Además, de acuerdo con la ETSI TS 119 172-1, se tendrá en cuenta la posible inclusión de compromisos de firma y se hará constar en el informe de validación. Concretamente, los compromisos de firma aceptados (puede incluir uno o varios) son:

- OID 1.2.840.113549.1.9.16.6.1 - la firma está destinada únicamente a fines de autenticación de datos.
  Indica que el firmante reconoce haber creado, aprobado y enviado los datos firmados,
  el URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin .
- OID 1.2.840.113549.1.9.16.6.2 - como acuse de recibo.
  Indica que el firmante reconoce haber recibido el contenido de los datos firmados,
  el URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt .
- OID 1.2.840.113549.1.9.16.6.3 - como prueba de entrega.
  Indica que el TSP que proporciona esa indicación ha entregado un dato firmado en un buzón accesible al destinatario de los datos firmados,
  el URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery .
- OID 1.2.840.113549.1.9.16.6.4 - Prueba del remitente.
  Indica que la entidad que proporciona esa indicación ha enviado los datos firmados (pero no necesariamente lo creó),
  el URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfSender .
- OID 1.2.840.113549.1.9.16.6.5 - Prueba de aprobación.
  Indica que el firmante ha aprobado el contenido de los datos firmados,
  el URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfApproval .
- OID 1.2.840.113549.1.9.16.6.6 - Prueba de creación.

Indica que el firmante ha creado los datos firmados (pero no necesariamente aprobados, ni enviados), el URI de este compromiso es http://uri.etsi.org/01903/v1.2.2#ProofOfCreation .
ANF AC, de acuerdo con lo establecido en el Anexo B de la ETSI 119 172-1, ha creado los siguientes OIDs propietarios:

OID 1.3.6.1.4.1.18332.27.1.9 - Uso de la firma como credencial en un control de acceso.
La firma está destinada únicamente a fines de autenticación de entidades con el fin de dejar evidencia de la solicitud de acceso realizada por el firmante.

OID 1.3.6.1.4.1.18332.27.1.12 - Autorización intermedia
La firma está destinada únicamente como una aprobación intermedia como parte de un proceso de decisión;

OID 1.3.6.1.4.1.18332.27.1.14 - Visto, marca de lectura.
La firma está destinada únicamente para indicar haber revisado un documento;

OID 1.3.6.1.4.1.18332.27.1.15 - Intervención en la compulsa legal de un documento original.
La firma está destinada únicamente a certificar que el firmante garantiza que el documento firmado es una copia auténtica que se corresponde íntegramente con un original.;

OID 1.3.6.1.4.1.18332.27.1.16 - Intervención como testigo.
Indica que la firma está destinada únicamente a indicar haber sido testigo de la firma de otra persona en el mismo documento (datos firmados) la cual ha leído íntegramente el documento, y lo ha firmado como acreditación de su conformidad a los mismos.

OID 1.3.6.1.4.1.18332.27.1.1 - Plenos efectos legales según Política de firma OID 1.3.6.1.4.1.18332.27.1.1.

Indica que la firma está destinada a ser utilizada en un marco legal y contractual, en el cual se desea acreditar con fuerza probatoria y plena validez jurídica, que el firmante está de acuerdo, salvo en aquellas cuestiones en las que haya expresado una mención, o salvedad, o compromiso con los acuerdos y condiciones que implícita o explícitamente se reseñan en los datos firmados. Las firmas electrónicas generadas en el ámbito de esta Política de Firma Electrónica, pueden utilizarse para suscribir todo tipo de documentos electrónicos, de acuerdo con las limitaciones de uso que establece la legislación vigente, y las restricciones derivadas de la Política de Certificación a la que está sometido el certificado electrónico utilizado en su creación.

La validez técnica del QES / QESeal se verifica de acuerdo con el proceso descrito en el documento ETSI EN 319 102-1 y se confirma mediante la emisión de certificados de estado electrónico cualificados.

Las siguientes secciones describen el modelo de concepto del servicio de validación, la selección del proceso de validación y el resultado (estado e informe) del certificado calificado validado para QES / QESeal.

En caso de que no exista un requisito específico indicado sobre el Servicio en este documento, se aplicarán los requisitos del punto i.5 del ETSI EN 319 102.

En caso de que este documento indique requisitos y reglas específicas, prevalecerán sobre los pertinentes del ETSI EN 319 102-1.

En caso de que exista una discrepancia entre los requisitos y las reglas de este documento y los del ETSI EN 319 102, prevalecerán los contenidos en este documento.

El SVSServ gestiona registros de eventos (LOGs) que permiten acreditar servicios prestados y la hora en que se han producido. Además, se registran los tipos de servicios de validación que han sido solicitados, el resultado de la solicitud (éxito o fracaso) y la identidad del suscriptor que los ha solicitado con el fin de administrar consumos. El acceso a esta información está restringido a personal expresamente autorizado.

3.2.2. Validación de los TSP

SVSServ gestiona un repositorio con las Listas de Confianza (TSL) publicadas por cada uno de los países miembros de la Unión y mantiene un control de versionado almacenando el histórico.

Diariamente se realiza una comprobación de publicación de nuevas TSL. Cuando se descarga una nueva versión antes de depositar confianza en ella, se realiza una verificación de firma e integridad utilizando la clave pública de la última versión de LOTL.

La interpretación de la TSL es realizada por SVSServ en conformidad con lo establecido en la ETSI TS 119 612.

3.2.3. Servicio OCSP

El SVSServ procede a la verificación del estado de vigencia de los certificados empleados en la elaboración de la firma /sello electrónico mediante consulta OCSP, no se realiza comprobación de estado contra listas de revocación CRL. Se requiere que la respuesta OCSP esté en conformidad con la norma IETF RFC 6960, X.509, Internet Public Key Infrastructure Online Certificate Status Protocol –OCSP, y utilice algoritmos de firma en conformidad con la ETSI TS 119 312.

Los Respondedores OCSP deben de atender consultas en tiempo real, directamente sobre los repositorios de la entidad emisora de los certificados empleados, ya sea en la elaboración de la firma, sello, o emisión de un sello de tiempo. Las respuestas OCSP deben estar firmadas electrónicamente por el QTSP. El proceso de validación comprende el certificado sometido a consulta y toda la cadena de la Jerarquía de Certificación hasta primer nivel (excluido CA Raíz).

Los campos contenidos en la respuesta OCSP según la especificación RFC 6960:

Campo	Definición
CertID.hashAlgorithm	Identificador del algoritmo hash
CertID. issuerNameHash	Hash del DN del emisor (OCTET STRING)
CertID.serialNumber	Número de serie del certificado que se desea validar
CertID. issuerKeyHash	Hash de la clave pública del emisor (OCTET STRING)
nonce	Opcional
certReq	Todas las respuestas contienen la cadena de certificación de ANF AC hasta la raíz. Su presencia y valor es ignorada.

Se detalla a continuación un ejemplo de consulta con OpenSSL:

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.

Ejemplo para realizar consultas tipo GET con OpenSSL:

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

Aclaración: Se ha detectado que OpenSSL puede emitir las siguientes respuestas de error:

1/ Si la CA raíz ha firmado directamente el certificado de entidad final, OpenSSL devuelve:
Response Verify Failure
Verify error: self signed certificate in certificate chain

2/ Si la respuesta del OCSP responder es de un tipo CRL, OpenSSL devuelve:
Response Verify
Failure signer certificate not found

3/ Los servidores OCSP Responder de ANF AC soportan consultas GET y POST.

3.3. Interfaces

De acuerdo con el modelo conceptual del proceso de validación de firma / sello electrónico en ETSI EN 319 102-1, el software con funciones de validación para QES / QESeal incluye dos componentes:

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

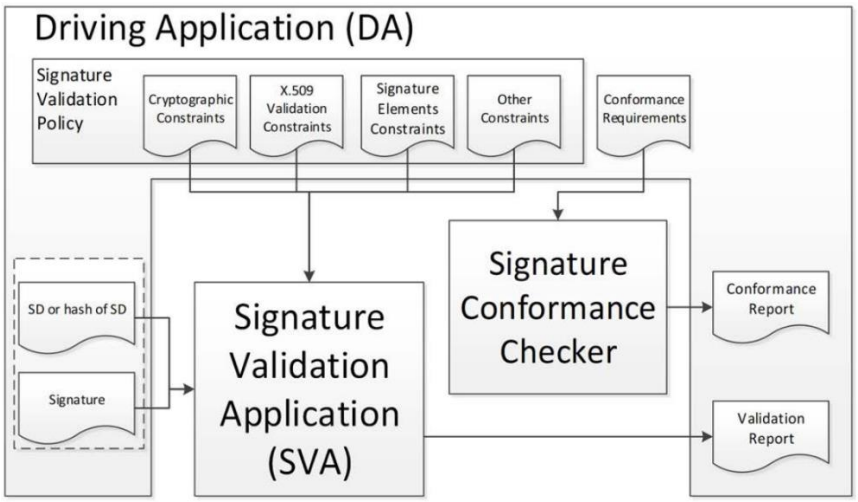

Figura: Modelo de validación de firma ETSI TS 119 102-1

ANF AC, pone a disposición de sus suscriptores tres modalidades:

- **Safe Box.** Se trata de una aplicación de usuario final que una vez instalada activa en el menú contextual del Shell (botón derecho del puntero), posibilitando hacer llamadas por línea de comando a la aplicación SafeBox. Esta aplicación permite realizar firmas electrónicas y proceso de validación cualificado de firmas y sellos electrónicos. Exclusivamente para SO Windows.
- **Critical Acces**. Se trata de una aplicación de escritorio de usuario final. Exclusivamente para SO Windows.
- **Web Service.** Este servicio está disponible en dos modalidades:
    - Cliente Web que permite realizar validaciones de usuario humano mediante navegador.
    - Sin interfaz de usuario para realizar validaciones automáticas. Disponible para cualquier SO.

En todas las modalidades el usuario puede seleccionar el objeto de datos firmado caso que no esté incluido en el SDO. Pero no se permite al usuario proporcionar más entradas para el proceso de validación (p.ej. elementos para parametrizarla política de validación, clase de firma, etc)

En todas las modalidades es posible realizar validación de múltiples firmas, y se realiza validación de todas ellas.

SVA activa la librería ANF CryptoToken, componente “Driving Application” (DA) que recibe el resultado del proceso de validación en forma de certificado cualificado de validación (estado e informe) del SVSServ.

El servicio soporta procesos de validación de firmas y sellos electrónicos en diferentes formatos:

- Proceso de validación para el formato básico de firma / sello
- Proceso de validación para Firmas con Sello de Tiempo Electrónico
- Proceso de validación para Firmas con Sello de Tiempo Electrónico y verificación de estado de vigencia en origen OCSP.

DA, utiliza bibliotecas estandarizadas y componentes que han sido probados. Se mantienen las últimas versiones clasificadas para explotación.

SVA, mantiene la integridad y confidencialidad de toda la información proporcionada por el usuario y de cualquier dato que fluya entre la aplicación y el usuario, incluso en el caso de un entorno público.

Salvo que el suscriptor haya contratado el servicio cualificado de conservación de firmas y sellos electrónicos de ANF AC, el SVSServ no almacenará el SD.

3.3.1. Canal de comunicación

El canal de comunicación entre el cliente y el SVSServ transporta la solicitud de validación de firma (1.) y la respuesta (3.). Puede ser sincrónico o asincrónico. Cubre la autenticación del SVSP (protocolo de comunicaciones SSL), para evitar falsos informes y puede admitir la autenticación de clientes.

Cuando el SVSP solicita la intervención de TSA (ANF AC TSA para sellado de tiempo) o, petición de estado OCSP (ANF AC VA para respuestas OCSP) o, petición TSL, etc. , se emplea protocolo de comunicaciones SSL.

Los suscriptores del servicio de validación se autentican ante el SvSServ empleando credenciales suministradas por ANF AC.

3.3.2. SVSP – otro TSP

ANF AC, para realizar la prestación del servicio puede tener que consultar a otro PCSC, por ejemplo consulta de estado OCSP. En ese caso, el canal de comunicación entre ANFA C y otros prestadores, requiere que el PSC llamado esté cualificado, la información recibida esté firmada y sea posible validarla.

El servicio de validación puede verse afectado por las prácticas, políticas y SLA de otros TSP que no están bajo el control de ANF AC.

3.4. Requisitos del informe de validación de firmas

El informe de validación incluye información de ANF AC conforme a ETSI TS 119 612 Apdo. 5.5.2, y de la aplicación empleada. Se siguen los requisitos establecidos por ETSI TS 119 102-2 y ETSI TS 119 441. En caso de que ANF AC decida realizar cualquier variación en ellos, esta variación quedará recogida en esta política.

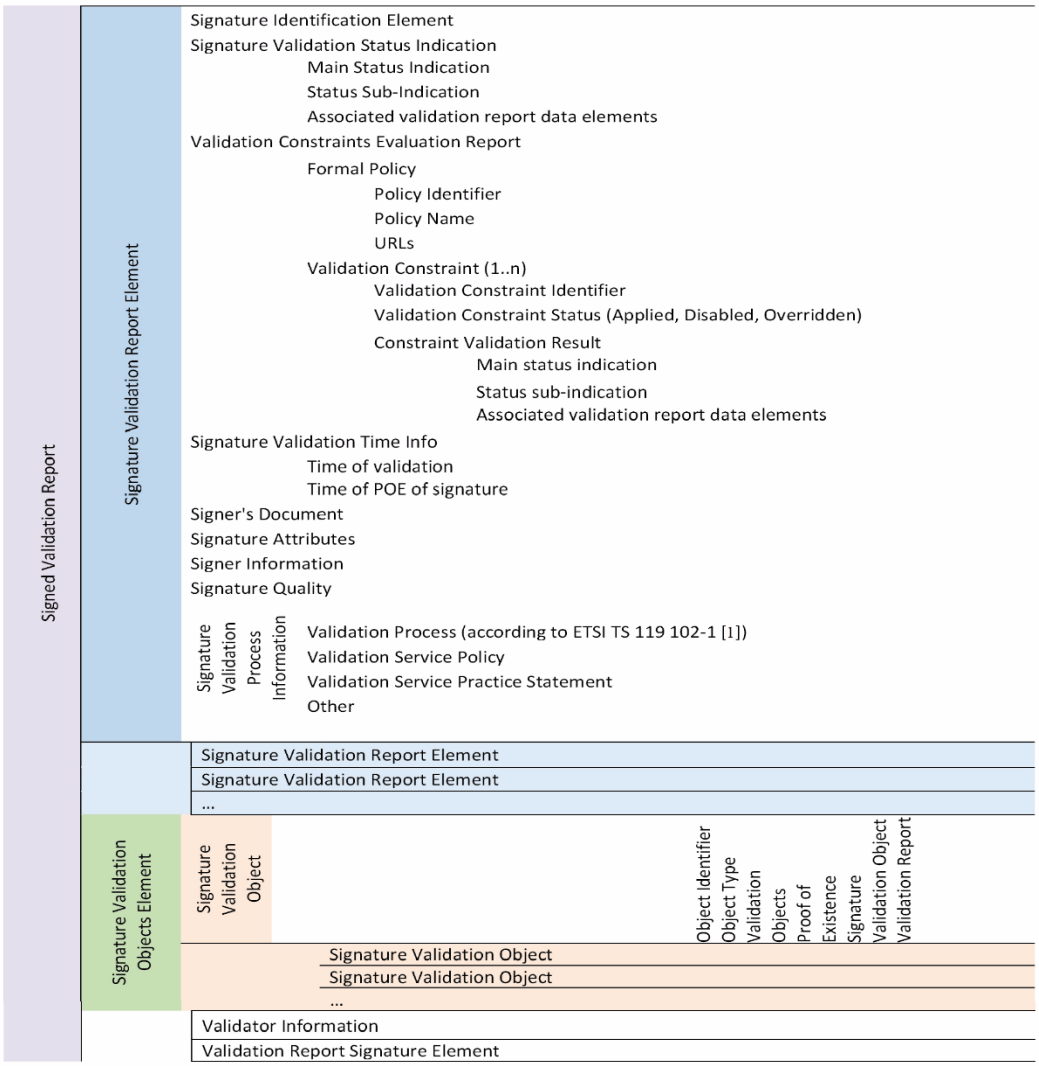

Ilustración 2 Estructura y elementos del informe de validación conforme ETSI TS 119 102-2 v 1.2.1

3.4.1. Indicación de estado del proceso de validación y del informe de validación

El servicio proporciona un informe de validación en formato PDF (firmado PAdES LT) o XML (firmado XAdES – A), que detalla la validación de la firma / sello realizada, lo que permite al DA comprobar en detalle las decisiones tomadas durante la validación y establecer / examinar en detalle las causas de la indicación de estado proporcionada.

El resultado del proceso de validación incluye:

- Una indicación de estado de los resultados del proceso de validación QES / QESeal.
- Una indicación de la política/s de validación cuyos requerimientos han sido aplicados.
- Fecha y hora del estado de validación, incluyendo los datos utilizados para la validación.
- Datos de informes adicionales para la validación de acuerdo con las tablas siguientes:

3.4.2. Indicación de estado para el proceso de validación QES/QESeal

Indicación estado	Semántica	Datos del informe de validación
TOTAL-CONFIRMADO	El proceso de validación QES / QESeal tiene un TOTAL-CONFIRMADO : • comprobaciones criptográficas de QES/QESeal han sido correctas (incluyendo verificación de hashes de los diferentes objetos de datos, firmados indirectamente); • validada positivamente la certificación de la identidad del firmante (es decir, el certificado de firma es válido); y • validado con éxito QES / QESeal	El proceso de validación confirma que la cadena de certificación es validada, incluyendo el certificado para QES/QESeal, utilizado en el proceso de validación junto con un atributo firmado / sellado específico (si existe), que se considera como una prueba de validación.
TOTAL-FALLO	El proceso de validación QES / QESeal tiene un resultado TOTAL-FALLO porque las comprobaciones criptográficas del QES / QESeal Son infructuosos (incluidos los controles de Hashes de los diferentes objetos de datos, Firmado / sellado indirectamente) o ha sido demostrado que la generación de la Firma / sello ha ocurrido después de Revocación / en tiempo de suspensión del QC.	El proceso de validación explica la causa del emitir informe de TOTAL-FALLO para cada uno de los elementos que se tienen en cuenta y que han dado resultado negativo.
INDETERMINADO	La información disponible no es suficiente para realizar el proceso de validación y determinar indicación de estado de QES / QESeal: TOTAL-CONFIRMADO o TOTAL FALLO	El proceso de validación facilita información con el fin de explicar la causa que da como resultado “indeterminado”, y ayudar a determinar los datos que faltan para completar el proceso de validación.

El informe de validación incluye la indicación de estado correspondiente a **TOTAL-FALLO** e **INDETERMINADO**. En la validación QES tiene una estructura que se presenta en la tabla siguiente, y que consta de códigos principales y auxiliares que proporciona el proceso de validación.

Estructura y semántica del informe Validación

Indicación de estado	Código auxiliar	Semántica	Datos del informe de validación
TOTAL-FALLO	HASH-FALLO	El proceso de validación QES / QESeal conduce a TOTALFAILED, Porque al menos un hash de un objeto que participa en la firma, no corresponde al hash registrado en QES / QESeal.	El proceso de validación proporciona un identificador que identifica explícitamente un el objeto de firma / sello que causa el error en el QES / QESeal.
	FORMATO-FALLO	QES / QESeal no es compatible con el estándares soportados indicados en este documento a un nivel que no permite que se procese el bloque criptográficamente.	El proceso de validación proporciona información sobre el proceso fallido de la QES / QESeal
	SIG-CRYPTO-FALLO	El proceso de validación QES / QESeal conduce a TOTAL-FALLO, porque el valor de la firma no se puede comprobar mediante la clave pública del certificado QES / QESeal.	El proceso de validación es negativo por inconsistencia del certificado QES / QESeal.
	POLICY-FALLO	El proceso de validación determina que el QES / QESeal está sometido a una Política de Firma no autorizada por esta Política de Validación.	El proceso de validación es negativo porque la Política de Firma no es autorizada.
	REVOCADO	El proceso de validación QES / QESeal lleva a TOTAL-FALLO porque: el certificado QES / QESeal ha sido revocado, y hay una prueba basada en un Timetamping que determina que la Firma / sello es elaboró después de la revocación del certificado.	El proceso de validación proporciona: · La validación de la cadena de certificación. · El fecha de revocación / suspensión de la certificado QES / QESeal. · CRL en su caso. · Sello de tiempo electrónico del QES / QESeal.
INDETERMINADO	SIG_CONSTR AINT_FAILURE	El proceso de validación QES / QESeal conduce a INDETERMINADO, porque uno o más atributos de QES / QESeal no corresponden a los elementos de validación.	El proceso de validación proporciona: • La cadena de certificación utilizada en el proceso de validación. • Información adicional sobre la causa

	CHAIN_CONSTRAINTS_FAILURE	El proceso de validación QES / QESeal conduce a INDETERMINADO, porque la cadena de certificación utilizada en el proceso de validación no corresponde a los elementos relacionados con el certificado de validación	El proceso de validación proporciona: • La cadena de certificación utilizada en el proceso de validación. • Información adicional sobre la causa
	CERTIFICATE_CHAIN_GENERAL_FAILURE	El proceso de validación QES / QESeal conduce a INDETERMINADO, porque la verificación de la cadena de certificación muestra un error debido a una razón no establecida.	El proceso de validación proporciona: Información adicional sobre el por qué.
	CRYPTO_CONSTRAINTS	El proceso de validación QES / QESeal conduce a INDETERMINATE, porque al menos uno de los algoritmos utilizados o el tamaño de las claves empleadas con estos algoritmos está bajo el nivel requerido de seguridad criptográfica y además: Los certificados QES / QESeal se generaron después de un momento hasta el cual estos algoritmos / claves se consideraban seguros; y además: QES / QESeal no está protegido por un sellado de sello de tiempo suficientemente fiable antes del tiempo hasta el cual los algoritmos / claves se consideran seguros.	El proceso de validación proporciona: Una identificación / designación de QES / QES real o de un certificado generado con un algoritmo o un tamaño de clave bajo el nivel requerido de seguridad criptográfica.
	EXPIRED	El proceso de validación QES / QESeal conduce a INDETERMINADO, porque el sello de tiempo de la firma es después de la fecha de caducidad (notAfter) del certificado	El proceso de validación proporciona:la cadena de certificación validada
	NO_SIGNING_CERTIFICATE_FOUND	El certificado QES / QESeal no puede ser identificado	

	NO_CERTIFICATE_CHAIN_FOUND	Un elemento de la cadena de certificación para identificar el certificado QES / QESeal no ha sido encontrado.	
	REVOKED_NO_POE	El certificado correspondiente ha sido revocado / suspendido durante la validación. El SVA no puede establecer si el certificado se empleó antes o después del momento de revocación / suspensión	
	OUT_OF_BOUNDS_NO_POE	El certificado ha expirado o aún no es válido en la fecha / hora de validación y SVA no puede determinar si está dentro del intervalo de validez del certificado	
	CRYPTO_CONSTRAINT_FAILURE_NO_POE	Al menos uno de los algoritmos utilizados en el QES / QESeal o en los certificados correspondientes que participan en su validación o el tamaño de la clave está bajo el nivel requerido de seguridad criptográfica y tampoco hay ninguna prueba de que las firmas / sellos o estos certificados hayan sido generados antes del tiempo hasta el cual este algoritmo / clave ha sido considerado como seguro	El proceso de validación proporciona: Identificación de QES / QESeal o del certificado correspondiente Generado con Longitud de clave inaceptable o con un algoritmo no cumple con los requisitos de seguridad criptográfica.
	NO_POE	Falta una evidencia que demuestre que la firma / sello se ha generado antes del reconocimiento de un evento comprometedor (es decir, algoritmo roto).	
	TRY_LATER	No es posible realizar todas las comprobaciones con la información disponible. A pesar de ello, el proceso es posible si la validación utiliza información adicional sobre la Revocación / suspensión que	

		estará disponible en una etapa posterior.	
	SIGNED_DATA_NOT_FOUND	Los datos para la firma / sello no pueden ser recibidos	El proceso de validación proporciona: El identificador (por ejemplo URI) de los datos para la firma / sello que ha causado el error
	GENERIC	otras razones.	El proceso de validación proporciona: Información adicional que muestra por qué el estado de validación es INDETERMINADO

3.4.3. Limitaciones de validación de certificados

Restricciones para la validación de certificados X.509 en el proceso de comprobación de la cadena de certificación de acuerdo con ETSI TS 119 172-1, cláusula A.4.2.1., Tabla A.2. Fila (m).

Restricción	**Valor de restricción en la validación de QES / QESeal (SVA o DA)**
(M) 1. X509CertificateValidationConstraints: 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 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:* De conformidad con IETF RFC 5280 clausula 6.1.1 (c) (m) 1.4. *initial-policy-mapping-inhibit*: De conformidad con IETF RFC 5280 clausula 6.1.1 (e) (m) 1.5. *initial-explicit-policy*: De conformidad con IETF RFC 5280 clausula 6.1.1 (f) (m) 1.6. *initial-any-policy-inhibit*: De conformidad con IETF RFC 5280 clausula 6.1.1 (g) (m) 1.7. *initial-permitted-subtrees*: De conformidad con IETF RFC 5280 cláusula 6.1.1 (h) (m) 1.8. *initial-excluded-subtrees*: De conformidad con IETF RFC 5280 cláusula 6.1.1 (i) (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. (m) 1.10. *policy-constraints*: Esta restricción se refiere a la (s) política (s) en el certificado QES / QESeal.	100 Mb.
(M) 2. RevocationConstraints: Este conjunto de restricciones se refiere a la verificación de estado de certificados QES / QESeal durante el proceso de validación. Estas restricciones pueden ser diferentes para los diferentes tipos de certificados 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: - ClrCheck: Las verificaciones se realizan en función de la CRL actual; - OcspCheck: El estado de revocación / suspensión se comprueba a través de OCSP IETF RFC 6960; - BothCheck: Ambos controles se realizan a través de OCSP y CRL; - EitherCheck: Los checks se realizan a través de OCSP o mediante CRL; - 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	NO

emitida en un tiempo especificado después la creación / generación de QES / QESeal.	
(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. Limitaciones criptográficas

Restricciones criptográficas sobre los algoritmos y parámetros utilizados en la creación de QES / QESeal, como se indica en ETSI TS 119 172-1, cláusula A.4.2.1, Tabla A2, fila (p).

Limitación	Valor de restricción en la validación de QES / QESeal
(P) 1. CryptographicSuitesConstraints: Esta restricción indica requisitos para los algoritmos y parámetros utilizados en la creación de QES / QESeal, o utilizados en la validación de firmas / sellos de objetos incluidos en el proceso de validación (por ejemplo QES / QESeal, certificados, CRLs, OCSP- Sello sellos / TSTs).	En conformidad con ETSI TS 119 312

3.4.5. Limitaciones de los elementos de la firma

Restricciones con respecto a los elementos de QES / QESeal que indican los requisitos de DTBS (Data To Be Signed), de acuerdo con ETSI TS 119 172-1, cláusula A.4.2.1., Tabla A. 2, fila (b).

Limitación	Valor de restricción en la validación de QES / QESeal (SVA o DA)
B) 1. ConstraintOnDTBS: Esta restricción indica los requisitos sobre el tipo de datos que debe firmar / sellar el firmante / persona de sellado.	NO
(B) 2. ContentRelatedConstraintsAsPartOfSignatureElements: Este conjunto de restricciones muestra los elementos de información necesarios relacionados con el contenido, en la forma de los requisitos	NO

cualificados firmados o no firmados presentes en QES / QESeal. El conjunto incluye: (B) 2.1 MandatedSignedQProperties-DataObjectFormat requiere un formato específico del contenido que debe firmar / sellar la persona firmante. (B) 2.2 MandatedSignedQProperties-content-hints requiere información específica que describe el contenido interno firmado / sellado de mensajes multicapa en los que un contenido se encuentra encapsulado en otro para poder ser firmado por el firmante. (B) 2.3 MandatedSignedQProperties-content-reference requiere la inclusión de información sobre la forma de conectar una solicitud y una respuesta del mensaje dentro de un intercambio entre ambas partes o la forma en que se debe realizar la conexión, etc. (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: Esta restricción muestra si se deben firmar los datos o solo una parte específica de ellos. La semántica de un posible conjunto de valores requeridos utilizados para indicar estos requisitos se define de la siguiente manera: • Todo: todos los datos deben estar firmados; • Partes: sólo se debe firmar determinada/s parte/s de los datos. En este caso, se utiliza información adicional para indicar qué partes deben firmarse/sellarse.	NO

3.4.6. Limitaciones de formatos y niveles compatibles con QES/QESeal

El servicio cualificado de Validación de firmas / sellos electrónicos avanzados / cualificados (QSVS) de ANF AC, soporta los siguientes formatos de QES / QESeal,

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

y niveles

- XAdES - B – T - LT y LTA
- CAdES – B – T - LT y LTA
- PAdES – B – T - LT y LTA

3.4.7. Restricciones de los QES/QESeal soportados

Posición de la firma/sello y el objeto de datos firmado	Valor
Covering QES/QESeal – la firma / sello cubre el objeto de datos	SI
Covered (type "letter") QES/QESeal – El objeto de datos firmado cubre la firma / sello	SI
Separate QES/QESeal – La firma / sello y el objeto de datos están separados (independientes)	SI
Simultáneamente se compararon repetidamente posiciones	SI
Un documento tiene más de un QES / QESeal	SI

3.4.8. Validación de firmas electrónicas cualificadas de acuerdo con eIDAS: Art. 32 y 33

Art. 32 y 33 del Reglamento (UE) No. 910/2014	Ejecución del Servicio
Art. 32. *Requisitos para la validación de firmas electrónicas cualificadas*	
1. En el proceso de validación de una firma electrónica cualificada se confirma la validez de la firma electrónica cualificada, disponer que:	
A) El certificado justificativo de la firma en el momento de la firma era un certificado cualificado para una firma electrónica, que corresponde al anexo I.	El proceso de validación de los certificados cumple con los requisitos descritos en EU 2015/1505 y ETSI 319 412-5 Anexo A.1 para el QTSP que emite certificados calificados para la firma electrónica.
B) El certificado cualificado ha sido emitido por un proveedor de servicios fiduciarios calificado y ha sido válido en el momento de la firma.	El proceso de validación de los certificados cumple con los requisitos descritos en EU 2015/1505 y ETSI 319 412-5 Anexo A.1 para el QTSP que emite certificados calificados para la firma electrónica.
C) Los datos de validación de la firma corresponden a los datos proporcionados por la parte que confía.	Se garantiza a través de los formatos QES / QESeal.
D) el conjunto único de datos, que representan al firmante de la firma electrónica en el certificado, se entregará a la parte que confía.	El certificado de firma para QES / QESeal se incluye en la respuesta por las validaciones para cada protocolo soportado conforme a este documento.
E) Si en el momento de la firma se ha utilizado un seudónimo, esto se ha indicado claramente a la parte que confía.	Dado que la indicación de pseudónimo en el campo Asunto se utiliza únicamente a petición expresa del cliente y tras un acuerdo preliminar entre ellos y el QTSP, se aplicarán los requisitos de ETSI EN 319 412-2 de conformidad con este documento.
F) La firma electrónica ha sido creada por un dispositivo para la creación de firma electrónica cualificada.	El proceso de validación de los certificados cumple con los requisitos descritos en la UE 2015/1505 para el QTSP que emite certificados calificados. Se realiza una comprobación para el tipo de SSCD (QSCD) requerido.
G) La integridad de los datos firmados no está comprometida.	Se garantiza a través del modelo de validación soportado indicado en este documento.
H) Los requisitos citados en el art. 26 se han cumplido en el momento de la firma.	Se garantiza a través del modelo de validación soportado indicado en este documento.
2. El sistema utilizado para la validación de firma electrónica cualificada proporciona al participante el resultado correcto del proceso de validación y le	El proceso de validación de QES / QESeal y el statusindication después del cheque se describen en este documento.

permite encontrar eventuales problemas relacionados con la seguridad.	
Art. 33. *Servicio de validación cualificado de firmas electrónicas cualificadas*	
1. Sólo podrá prestar un servicio de validación cualificado de firmas electrónicas cualificadas el prestador cualificado de servicios de confianza que:	
A) realice la validación de conformidad con el artículo 32, apartado 1, y	Ver tabla anterior sobre el Artículo 32 (1).
B) permita que las partes usuarias reciban el resultado del proceso de validación de una manera automatizada que sea fiable, eficiente e incluya la firma electrónica avanzada o el sello electrónico avanzado del prestador cualificado de servicio de validación.	Los usuarios reciben, de manera automatizada, un informe de validación cualificada sellado por ANF Autoridad de Certificación, empleando el certificado cualificado de sello electrónico que identifica el servicio ("Digital identity") en la TSL europea.
Art. 28. *Certificados cualificados para firmas electrónicas*	
1. Los certificados cualificados para firmas electrónicas corresponden a los requisitos establecidos en el anexo I.	Corresponde a los requisitos del ETSI 119 412-5, Anexo A.1.
2. Los certificados cualificados para firmas electrónicas no están sujetos a ningún requisito obligatorio que exceda los requisitos establecidos en el anexo I.	El proceso de validación de certificados cumple con los requisitos descritos en EU 2015/1505 para listas de confianza. No se precisan controles adicionales excepto los indicados en el anexo I del Reglamento.
3. Los certificados cualificados para firmas electrónicas pueden incluir datos adicionales no obligatorios. Estos datos no afectan la compatibilidad operativa y el reconocimiento de las firmas electrónicas cualificadas.	No se precisan controles adicionales excepto los indicados en el anexo I del Reglamento.
4. Si un certificado cualificado para la firma electrónica es revocado después de su activación inicial pierde su validez desde el momento de la revocación y su estado no puede ser restaurado en ninguna circunstancia.	De acuerdo con la Política y Práctica para servicios de confianza calificados para QES / QESeal.
5. Los Estados miembros podrán determinar las normas nacionales relativas a la suspensión temporal de la validez del certificado acreditado para la firma electrónica cumpliendo las siguientes condiciones:	De acuerdo con el ETSI TS 110 102-1 si en la validación del certificado se procesa un resultado de validación / respuesta errónea se recibe debido al certificado QES / QESeal suspendido, el Servicio finalizará el proceso de validación. La indicación de estado es INDETERMINATE y el código adicional TRY_LATER con la hora de la suspensión y, si la hay, el campo nextUpdate de CRL u OCSP-response se utiliza para determinar la validación siguiente.
A) si el certificado cualificado para la firma electrónica es suspendido temporalmente, pierde su validez por el término de la suspensión	
B) La duración de la suspensión se indica claramente en la base de datos de los certificados y el estado del certificado suspendido es visible durante el término de la suspensión dentro del servicio,	

proporcionando información sobre el estado del certificado	
***Art. 26**. Requisitos para las firmas electrónicas avanzadas*	
La firma electrónica avanzada corresponde a los siguientes requisitos:	
A) se relaciona de manera única con el firmante de la firma	Se garantiza a través de los formatos compatibles con AdES.
B) puede identificar al firmante de la firma	Se garantiza a través de los formatos compatibles con AdES.
C) se ha creado a través de datos para la creación de firmas electrónicas que el firmante de la firma electrónica puede utilizar con alta fiabilidad y únicamente bajo su control; y	Se garantiza a través de los formatos compatibles con AdES.
D) Se relaciona con los datos firmados con él de una manera que permite encontrar cualquier modificación consecutiva en ellos	Se garantiza a través de los formatos compatibles con AdES.

3.4.9. Firma del informe de validación cualificada

ANF AC, en su calidad de SVSP firma los informes de validación cualificada empleando un sello electrónico cualificado empleando un Módulo de Seguridad Hardware (HSM), certificado en conformidad Common Criteria ISO 15408 EAL 4 +. Las claves (pública – privada) han sido generadas en el interior de este dispositivo criptográfico.

ANF AC Servicio de validación			
Subject	CN = ANF AC Servicio de validación	**Serial number**	995616158423738526593418293
	OI = VATES-G63287510	**Clave Pública**	RSA (2048 Bits)
	OU = Certificado Cualificado de Sello Electronico		
	O = ANF Autoridad de Certificación	**Algorítmo defirma**	Sha256RSA
	C = ES L=Barcelona, ST=Cataluña		
Periodo de vigencia	Válido desde 2023-02-01 17:06:59 hasta 2025-01-31 17:06:59		
x509SKI	UtafUoOU5ofKm7lGQuP7aR+jgBs=		

En caso de realizar copias de seguridad de las claves, las claves estarán protegidas para garantizar su integridad y confidencialidad por el módulo criptográfico antes de ser almacenadas fuera de ese dispositivo.

La firma es PAdES nivel LT o XAdES nivel LT, según corresponda por formato del informe PDF o XML respectivamente. ANF AC en calidad de PCSC presta el servicio de sellos cualificados electrónicos y sellos cualificados de tiempo electrónico.