POLÍTICA DE CERTIFICACIÓN

Servicio de Validación de Firmas

ÍNDICE

1. INTRODUCCIÓN 2
- 1.1 Alcance 2
- 1.2 Contexto 2

2. NORMATIVA DE REFERENCIA 3
- 2.1 Normas Técnicas 3
- 2.1 Otras Referencias 3

3. SISTEMA DE GESTIÓN 4
- 3.1 DECLARACIÓN DE CUMPLIMIENTO 4
- 3.2 ROLES Y RESPONSABILIDADES 4
- 3.3 GESTIÓN DE INCUMPLIMIENTOS 4

4. ANÁLISIS DE CUMPLIMIENTO 5
- 4.1 Disposiciones generales 5
- 4.2 Elemento de Informe de Validación 7
- 4.3 Elemento de Informe de Validación de Firma 8
  - 4.3.3 Elemento de Identificación de Firma 9
  - 4.3.4 Indicación del Estado de Validación de la Firma 10
  - 4.3.5 Informe de Evaluación de Restricciones de Validación 11
  - 4.3.6 Información sobre el Tiempo de Validación de la Firma 12
  - 4.3.7 Elemento Documento del Firmante 13
  - 4.3.8 Elemento de Atributo de Firma 14
  - 4.3.9 Elemento de Información del Firmante 15
  - 4.3.10 Elemento de Calidad de la Firma 16
  - 4.3.11 Elemento de Información del Proceso de Validación de la Firma 16
  - 4.3.12 Elemento de Datos del Informe de Validación Asociado 17
- 4.4 Objetos de Validación de Firma 18
  - 4.4.5 Objeto de Validación 19
  - 4.4.6 Prueba de Existencia (POE) 20
  - 4.4.7 Provisión de Prueba de Existencia (POE Provisioning) 21
  - 4.4.8 Informe de Validación del Objeto de Validación 21
- 4.5 Información del Validador 22
- 4.6 Firma del Informe de Validación 23

5. ANEXOS 24
- 5.1 Acceso al servicio de validación 24
- 5.2 Documentación API del servicio de validación 24
- 5.3 Ejemplos de informes de validación 24
  - 5.3.1 Informe desde la UI del Servicio 24
  - 5.3.2 Informe XML 25

5.3.2.1 Informe Simple 25
5.3.2.2 Informe Detallado 26
5.3.2.3 Informe Diagnóstico 37

CONTROL DE DOCUMENTO

Título	Política de Certificación del Servicio de Validación de Firmas		
Código	CP-QVAL - Validación de Firmas		
Versión	1.0	**Fecha Versión Actual**	28/01/2025
Fecha Creación	28/01/2025	**Fecha Aprobación**	28/01/2025
Revisado por	Jesús López	**Aprobado por**	Benito Galán
Tipología información	Interna y/o privada		

Control de Cambios y Versiones		
Fecha	**Versión**	**Motivo del Cambio**
28/01/2025	1.0	Primera versión.

1. INTRODUCCIÓN

1.1 Alcance

Esta política define el alcance del servicio ofrecido por Viafirma para la validación de firmas basado en el cumplimiento de la especificación técnica ETSI TS 119 102.

1.2 Contexto

La aplicación de la presente política se da bajo el contexto del marco regulatorio definido para prestadores cualificados de servicios de confianza.

2. NORMATIVA DE REFERENCIA

2.1 Normas Técnicas

Las siguientes normas y especificaciones técnicas son referencias en la aplicación y cumplimiento de la presente política.

- ETSI EN 319 102-1
- ETSI TS 119 102-2
- ETSI EN 319 401

2.1 Otras Referencias

- Reglamento eIDAS 2.
- Resolución Núm. 071-19 del Consejo Directivo del INDOTEL y sus disposiciones sobre Seguridad de la Información y estándares internacionales: ETSI EN 319 401, ETSI TS 119 102-2, ETSI EN 319 102-1.
- Resolución Núm. 055-06 Sobre Protección de datos Personales por los sujetos regulados de la Ley Núm.126-02.
- Resolución Núm.142-06 Sobre Protección de los derechos de los consumidores de la Ley Núm. 126-02.
- Resolución 043- 2021 que actualiza las condiciones del seguro de responsabilidad civil de los sujetos regulados de la Ley Núm.126-02.

3. SISTEMA DE GESTIÓN

3.1 DECLARACIÓN DE CUMPLIMIENTO

Declaración formal de la organización sobre el cumplimiento de la norma.

3.2 ROLES Y RESPONSABILIDADES

El servicio de validación de firmas cuenta con la participación coordinada del departamento de desarrollo, encargado del diseño, análisis e implementación del producto denominado internamente "**Viafirma Audit Trail**".

La distribución, publicación y mantenimiento del servicio basado en este producto se realiza desde el departamento de operaciones y servicios junto al apoyo del equipo de DevOps y arquitectura.

Todas estas actividades son incorporadas en los distintos planes de tratamiento de riesgos a cargo del departamento SGSI.

Los responsables de las áreas y departamentos mencionados anteriormente cuentan con su correspondiente nombramiento, pudiendo ser consultado en el siguiente registro de nombramientos:

📂 SGSI > A.1 Controles de Seguridad > 5.3 - Funciones, responsabilidades y autoridades de la organización > Nombramientos

3.3 GESTIÓN DE INCUMPLIMIENTOS

Los incumplimientos o desviaciones identificadas para esta política serán tratadas acorde al procedimiento de gestión de cambios establecido para el resto de políticas y prácticas de certificación de nuestra organización.

De igual forma, esta política será revisada con carácter semestral, junto al resto de políticas y procedimientos.

4. ANÁLISIS DE CUMPLIMIENTO

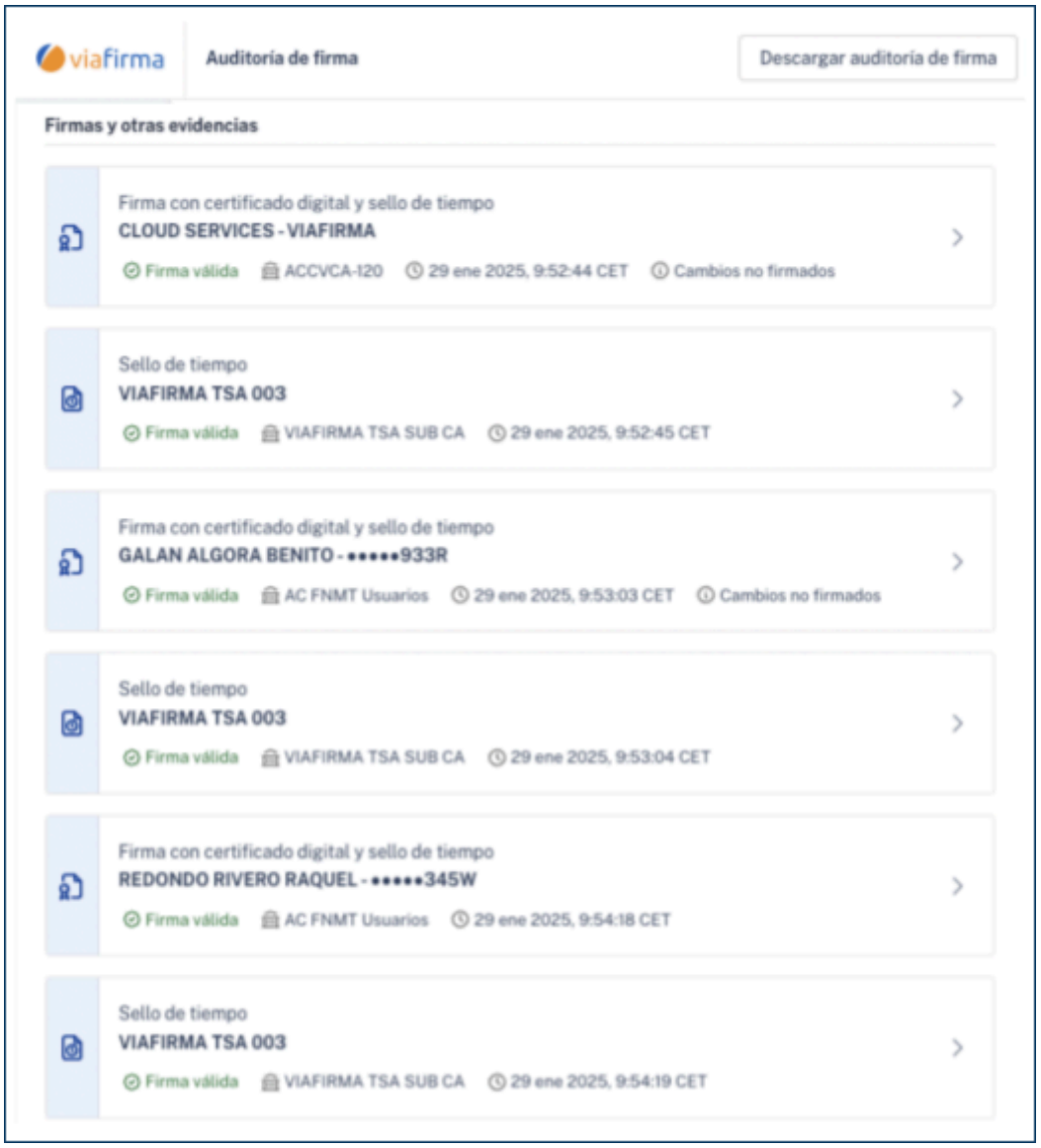
El informe de validación de firma cuenta con una estructura definida en la norma técnica ETSI TS 119 102 Parte 2 (*Electronic Signatures and Infrastructures (ESI);Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report*), estableciendo en su capítulo 4 los elementos necesarios que son analizados e implementados por nuestro servicio de validación de la siguiente forma.

4.1 Disposiciones generales

Descripción del Requisito: estado general y adicional para cada una de las firmas realizadas.

Cumplimiento: el servicio de validación itera por cada elemento de firma incorporado al documento mostrando para cada uno de ellos un estado general que facilita al usuario final un fácil entendimiento de la validación sin bajar a un mayor nivel de detalle.

A continuación un ejemplo del resultado general de validación de un documento firmado tras ser analizado por nuestro servicio de validación.

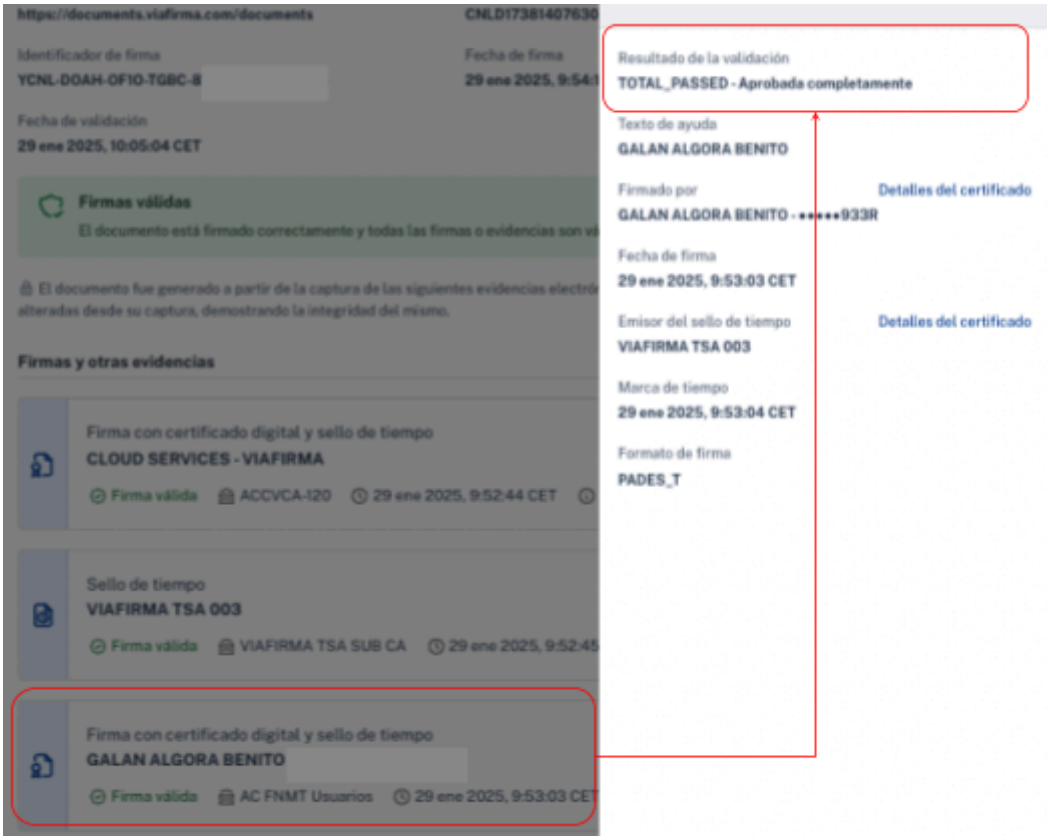

viafirma
Auditoría de firma
Descargar auditoría de firma
Firmas y otras evidencias
Firma con certificado digital y sello de tiempo
CLOUD SERVICES - VIAFIRMA
Firma válida
ACCVCA-120
29 ene 2025, 9:52:44 CET
Cambios no firmados
Sello de tiempo
VIAFIRMA TSA 003
Firma válida
VIAFIRMA TSA SUB CA
29 ene 2025, 9:52:45 CET
Firma con certificado digital y sello de tiempo
GALAN ALGORA BENITO - •••••933R
Firma válida
AC FNMT Usuarios
29 ene 2025, 9:53:03 CET
Cambios no firmados
Sello de tiempo
VIAFIRMA TSA 003
Firma válida
VIAFIRMA TSA SUB CA
29 ene 2025, 9:53:04 CET
Firma con certificado digital y sello de tiempo
REDONDO RIVERO RAQUEL - •••••345W
Firma válida
AC FNMT Usuarios
29 ene 2025, 9:54:18 CET
Sello de tiempo
VIAFIRMA TSA 003
Firma válida
VIAFIRMA TSA SUB CA
29 ene 2025, 9:54:19 CET

4.2 Elemento de Informe de Validación

- **Presencia:** Obligatoria
- **Descripción del Requisito:** Este elemento actúa como contenedor para los informes sobre la validación de una o más firmas. Debiendo contener uno o más elementos *signature-validation-report*, tal como se especifica en la cláusula 4.3.

El servicio de validación agrupa a modo de contenedores los distintos elementos de firmas identificados en el documento, pudiendo de hecho contar con distintos contenedores en aquellos casos en los que se identifiquen elementos de firma electrónica avanzada que deben ser tratados de forma separada.

Para cada firma incluida en el informe de validación se incluye una validación individual de cada una de ellas.



4.3 Elemento de Informe de Validación de Firma

Presencia: Obligatoria

Descripción del Requisito: Este elemento representa la información de validación para una única firma. Debe contener una secuencia de elementos descritos en las cláusulas 4.3.3 a 4.3.12. Este elemento también se utiliza en el informe de validación de un objeto de validación de firma (ver cláusula 4.4.8). Las reglas sobre si un elemento contenido dentro de este elemento es obligatorio u opcional pueden ser diferentes en este caso. Este elemento también puede contener cualquier otra información proporcionada por el proceso de validación.

Todos los elementos de firma son incorporados al informe y para cada uno de ellos se incluye validación individual, incluyendo las firmas asociadas a los sellos de tiempo o sellos electrónicos.

4.3.3 Elemento de Identificación de Firma

Presencia: Condicional

Descripción del Requisito: Este elemento debe estar presente en el informe de validación de una firma, a menos que el elemento de estado de validación de la firma (ver cláusula 4.3.4) indique que no ha sido posible realizar una validación porque la firma no cumplía con uno de los estándares base hasta el punto de que el bloque de construcción de verificación criptográfica no pudo procesarla (indicación principal TOTAL-FAILED, subindicación FORMAT_FAILURE, como se especifica en ETSI EN 319 102-1 [1], cláusula 5.1.3, tabla 6).

Este elemento puede estar presente en un informe de validación de un objeto de validación de firma (ver cláusula 4.4.8).

Contenido: Este elemento debe contener:

1. El DTBSR (ver cláusula 4.2.8 en ETSI EN 319 102-1 [1]) junto con un identificador del algoritmo hash utilizado para calcular el hash.
2. Una indicación de si el DTBSF (ver cláusula 4.2.7 en ETSI EN 319 102-1 [1]) o el DTBSR (ver cláusula 4.2.8 en ETSI EN 319 102-1 [1]) ha sido procesado por el SVA.

   NOTA 1: Esto permite que el formato del informe definido en el presente documento se utilice cuando un SVA haya verificado la firma criptográfica y la validez del (los) certificado(s) sin haber visto los documentos ni otros elementos de una firma AdES.

3. Una indicación de si el Signer's Document (SD) (ver cláusula 4.2.3 en ETSI EN 319 102-1 [1]) o el Signer's Document Representation (SDR) (ver cláusula 4.2.4 en ETSI EN 319 102-1 [1]) ha sido procesado por el SVA.

   NOTA 2: Esto permite que el formato del informe definido en el presente documento se utilice cuando un SVA haya verificado una firma AdES procesando únicamente el hash del documento del firmante.

Este elemento también puede contener:

4. Un identificador único que permita que este elemento sea referenciado dentro del informe de validación.
5. El valor de la firma digital.
6. Un identificador proporcionado por el DA.
7. Uno o más elementos adicionales que ayuden a identificar de manera única una firma y los datos de la firma.

4.3.4 Indicación del Estado de Validación de la Firma

Presencia: Obligatoria

Descripción del requisito:

Cuando está presente en el informe de validación de una firma, este elemento proporciona información sobre el estado de la validación completa de la firma en el contexto de una política de validación de firma específica.

Cuando está presente en un informe de validación de un objeto de validación de firma, este elemento proporciona información sobre el resultado de la validación de ese objeto en el contexto de una política de validación de firma específica seleccionada para la validación de la firma.

Contenido:

Este elemento debe contener un elemento de indicación de estado principal como se define en la cláusula 4.3.4.2.

Este elemento puede contener uno o más elementos de sub-indicación como se define en la cláusula 4.3.4.3.

NOTA: Puede haber más de un elemento de sub-indicación cuando el SVA necesita reportar múltiples problemas.

4.3.5 Informe de Evaluación de Restricciones de Validación

Presencia: Condicional

Descripción del Requisito:

Este elemento debe estar presente en el informe de validación de una firma.
Este elemento puede estar presente en un informe de validación de un objeto de validación de firma (ver cláusula 4.4.8).

Este elemento especifica el conjunto de restricciones de validación que han guiado el proceso de validación, independientemente de la forma en que las restricciones hayan sido definidas (ver ETSI EN 319 102-1 [1], cláusula 5.1.4.1).

Contenido:

Cuando una política de validación de firma formal, como se define en ETSI TS 119 172-1 [11], ha sido seleccionada explícita o implícitamente por el DA, este elemento debe contener una referencia a esa especificación de política de validación de firma formal en un elemento de política formal (ver cláusula 4.3.5.3).

NOTA: La referencia a la política de validación de firma formal indica que esta política ha guiado la validación. Información detallada sobre la validación de las restricciones individuales que componen esta política puede reportarse adicionalmente en los elementos de restricción de validación.

Este elemento debe contener elementos individuales de informe de restricción de validación (ver cláusula 4.3.5.4) que reporten sobre las restricciones de validación que han sido aplicadas explícita e implícitamente por el SVA.

Este elemento también debe contener elementos individuales de informe de restricción de validación (ver cláusula 4.3.5.4) que reporten sobre las restricciones de validación que, de acuerdo con la conformidad con ETSI EN 319 102-1 [1], deberían haber sido verificadas pero que han sido deshabilitadas o anuladas por la política de validación en uso.

Cuando una política de validación de firma formal proporcionada por el DA no fue aplicada o no fue completamente aplicada por el SVA, el informe de validación debe contener elementos individuales de informe de restricción de validación (ver cláusula 4.3.5.4) que informen sobre cuáles restricciones de validación fueron aplicadas y cuáles han sido ignoradas o anuladas.

4.3.6 Información sobre el Tiempo de Validación de la Firma

Presencia: Condicional

Descripción del Requisito:

Este elemento debe estar presente en el informe de validación de una firma. Este elemento puede estar presente en un informe de validación de un objeto de validación de firma (ver cláusula 4.4.8). Este elemento proporciona información relacionada con el tiempo en la validación.

Contenido:

Este elemento debe contener:

1. La fecha y hora en que se realizó la validación; y
2. La fecha y hora para las cuales se ha identificado una Prueba de Existencia (POE) de la firma y se ha determinado el estado de validación.

Este elemento también puede contener información sobre la fuente de la POE y, cuando la POE haya sido derivada por el Servicio de Validación de Firma (SVA), un identificador que haga referencia al objeto de validación de firma que fue esencial para dicha prueba.

La información de fecha y hora debe proporcionarse en UTC.

NOTA: El segundo valor corresponde al tiempo actual en la validación de Firma Básica. Puede ser el tiempo actual o un punto en el pasado al validar Firmas con Tiempo, Firmas con Material de Validación a Largo Plazo o Firmas que garantizan la Disponibilidad y la Integridad del Material de Validación a Largo Plazo.

4.3.7 Elemento Documento del Firmante

Presencia: Condicional

Descripción del Requisito: Este elemento debe estar presente en el informe de validación de una firma. Este elemento puede estar presente en un informe de validación de un objeto de validación de firma (ver cláusula 4.4.8). Este elemento identifica el documento que ha sido cubierto por la firma.

Contenido:

Este elemento debe contener, ya sea la Representación del Documento del Firmante (SDR) directamente, cuando el SDR es un valor hash, o una referencia a un objeto de validación dentro del Elemento de Objetos de Validación de Firma (ver cláusula 4.4). Cuando esté presente, el objeto de validación debe contener el SDR o un URI que permita recuperarlo.

Este elemento también puede contener una referencia a un objeto de validación de firma dentro del Elemento de Objetos de Validación de Firma (ver cláusula 4.4) cuando el Documento del Firmante (SD) haya sido proporcionado por la Autoridad de Validación (DA) al Servicio de Validación de Firma (SVA). Cuando esté presente, el objeto de validación debe contener el SD o un URI que permita recuperarlo.

NOTA: El documento del firmante está especificado en ETSI EN 319 102-1 [1]. Puede ser la entrada específica de formato en la función hash, cuyo resultado se usa como una de las entradas para calcular el valor de la firma. Esto incluye cualquier procesamiento, transformación o procedimientos de canonización requeridos por el formato de la firma.

El formato de un SDR almacenado como objeto de validación está fuera del alcance del presente documento.

4.3.8 Elemento de Atributo de Firma

Presencia: Condicional

Descripción del Requisito: Este elemento debe estar presente siempre que la firma contenga atributos de firma. Este elemento proporciona los atributos de firma que estaban presentes en la firma validada.

Contenido:

Este elemento debe consistir en una secuencia con una instancia por cada atributo contenido en la firma.

Cada elemento de esa secuencia debe contener:

1. El tipo del atributo.
2. Indicación de si el atributo era un atributo firmado o no firmado.

También puede contener:

3. Información dependiente del atributo extraída del atributo. El **Anexo A** especifica dicha información para los atributos definidos en **CAdES [i.1]**, **PAdES [i.3]** y **XAdES [4]**.
4. Una o más referencias a objetos de validación de firma dentro del **Elemento de Objetos de Validación de Firma** (ver cláusula 4.4).

4.3.9 Elemento de Información del Firmante

Presencia: Condicional

Descripción del Requisito: Cuando se haya identificado un certificado de firma, este elemento debe estar presente en el informe de validación de una firma. En caso contrario, este elemento puede estar presente. Este elemento proporciona información sobre el firmante.

Contenido:

Este elemento debe contener una referencia a un objeto dentro del Elemento de Objetos de Validación de Firma (ver cláusula 4.4).

El objeto referenciado debe ser el certificado identificado como el certificado del firmante y contener el conjunto único de datos que representan al firmante.

Este elemento también puede contener una representación en un formato legible por humanos del firmante.

EJEMPLO: Nombres distinguidos o nombres alternativos del sujeto contenidos en el certificado del firmante.

Cuando se haya utilizado un seudónimo en el momento de la firma, este elemento debe contener una indicación de que se ha utilizado un seudónimo.

4.3.10 Elemento de Calidad de la Firma

Presencia: Condicional

Descripción del Requisito:

Este elemento contiene información que respalda la calidad de la firma.

EJEMPLO: Firma electrónica cualificada, firma electrónica avanzada respaldada por un certificado cualificado.

Contenido:

Este elemento debe contener uno o más URN que indiquen la calidad de la firma.

NOTA: La definición de los URN para la calidad de la firma está fuera del alcance del presente documento.

4.3.11 Elemento de Información del Proceso de Validación de la Firma

Presencia: Opcional

Descripción del Requisito: Este elemento proporciona información sobre el proceso de validación de firma realizado.

Contenido:
Este elemento debe contener uno o más de los siguientes elementos:

1. Un **URI** que indique el proceso de validación utilizado (ver **ETSI EN 319 102-1 [1]**, cláusulas **5.3, 5.5 y 5.6.3**). Este **URI** debe tener uno de los siguientes valores:
    - urn:etsi:019102:validationprocess:Basic cuando el SVA haya realizado el Proceso de Validación de Firmas Básicas, según lo especificado en ETSI EN 319 102-1 [1], cláusula 5.3.

- urn:etsi:019102:validationprocess:LTVM cuando el SVA haya realizado el Proceso de Validación para Firmas con Tiempo y Firmas con Material de Validación a Largo Plazo, según ETSI EN 319 102-1 [1], cláusula 5.5.
- urn:etsi:019102:validationprocess:LTA cuando el SVA haya realizado el Proceso de Validación para Firmas que garantizan la Disponibilidad a Largo Plazo y la Integridad del Material de Validación, según ETSI EN 319 102-1 [1], cláusula 5.6.

2. También se puede incluir cualquier otro **URI** que indique el proceso de validación en caso de que ninguno de los procesos mencionados haya sido aplicado.
3. Un **URI** que identifique la política del servicio de validación, cuando sea aplicable.
4. Un **URI** que identifique la declaración de prácticas del servicio de validación, cuando sea aplicable.
5. Otra información proporcionada por el proceso de validación.

4.3.12 Elemento de Datos del Informe de Validación Asociado

Presencia: Opcional

Descripción del Requisito:

Este elemento contiene información adicional sobre la validación de la firma o una restricción de validación de firma.

Contenido:

Este elemento debe contener uno o más de los elementos descritos en las cláusulas 4.3.12.3 a 4.3.12.8.

4.4 Objetos de Validación de Firma

Presencia: Opcional

Descripción del Requisito:

Este elemento actúa como un contenedor para los objetos de validación utilizados durante el proceso de validación.

NOTA: Esto evita la duplicación de objetos de validación, por ejemplo, CRLs, cuando el informe de validación contiene la validación de más de una firma u objeto de validación.

Contenido:

Cuando esté presente, este elemento debe contener una secuencia de elementos de objetos de validación de firma, que representan el conjunto de objetos de validación utilizados en el proceso de validación, junto con su informe de validación cuando corresponda.

EJEMPLO: Documentos del firmante, listas de confianza, información de revocación (CRLs, respuestas OCSP) o registros de evidencia.

Cada elemento de objeto de validación de firma en esta lista debe tener las siguientes propiedades, descritas en las cláusulas siguientes:

- Un identificador que haga referencia de manera única a este objeto de validación dentro del informe de validación.
- El tipo de objeto.
- El objeto en sí mismo o una referencia al objeto.

Además, pueden estar presentes los siguientes datos sobre el objeto de validación de firma:

- Información sobre una prueba del momento más temprano de existencia del objeto.
- Información sobre los objetos para los cuales este objeto de validación proporciona pruebas de existencia.
- Un informe de validación sobre la validación del objeto.

4.4.5 Objeto de Validación

Presencia: Obligatorio

Descripción del Requisito:

Este elemento contiene o hace referencia al objeto de validación.

Contenido:

Este elemento debe contener uno o más de los siguientes elementos:

1. El objeto en sí mismo.
2. Una versión codificada en Base64 del objeto.
3. Un hash criptográfico del objeto.
4. Un URI donde se pueda recuperar el objeto.

NOTA:

Siempre que el informe incluya un hash criptográfico del objeto, este corresponde al hash calculado por el proceso de validación durante la validación. Este hash puede utilizarse para verificar la integridad del objeto de validación cuando no está incluido en el informe, pero puede recuperarse a través del URI proporcionado.

4.4.6 Prueba de Existencia (POE)

Presencia: Opcional

Descripción del Requisito:

Este elemento contiene información sobre una prueba del momento más temprano de la existencia del objeto.

Contenido:

Este elemento debe contener la información de la POE que proporciona el momento más temprano de la existencia del objeto.

Esta propiedad debe incluir:

1. El valor de tiempo para esa prueba en **UTC**.
2. Una indicación de si la **POE** ha sido:
    - Derivada durante la validación.
    - Proporcionada al **SVA** como entrada.
    - Derivada según la política.

EJEMPLO 1: Una política puede requerir el uso del tiempo de firma reclamado como POE para la firma.

Este elemento también puede contener:

3. Un identificador que haga referencia al **objeto de validación de firma** que fue esencial para esa prueba.

EJEMPLO 2: Los registros de evidencia o los sellos de tiempo pueden ser objetos de validación de firma esenciales para esa prueba.

4.4.7 Provisión de Prueba de Existencia (POE Provisioning)

Presencia: Condicional

Descripción del Requisito:

Cuando un objeto de validación proporciona pruebas de existencia para otros objetos, esta propiedad proporciona información sobre esos objetos.

Contenido:

Este elemento debe contener:

1. El valor de tiempo para esa prueba en **UTC**.
2. Una lista de referencias a la firma o a objetos de validación de firma dentro del informe de validación de firma que están cubiertos por esa prueba.

NOTA: Este elemento puede utilizarse para presentar la relación entre los sellos de tiempo y los datos sellados con dichos sellos.

EJEMPLO: Los sellos de tiempo y los registros de evidencia pueden proporcionar pruebas de existencia.

4.4.8 Informe de Validación del Objeto de Validación

Presencia: Opcional

Descripción del Requisito:

Este elemento puede estar presente siempre que el objeto de validación de firma sea un objeto firmado y su firma haya sido validada durante el proceso de validación general.

Descripción:

Este elemento contiene un informe de validación para el objeto de validación de firma.

Contenido:

Este elemento debe contener un informe de validación sobre la validación del objeto de validación de firma.

El informe debe cumplir con lo establecido en el presente documento.
Cualquier objeto de validación que haya sido utilizado en la validación de este objeto debe incluirse en el Elemento de Objetos de Validación de Firma dentro del informe de validación principal.

NOTA: La firma en el informe de validación principal protege el informe de validación de un objeto de validación.

4.5 Información del Validador

Presencia: Opcional

Descripción del Requisito:

Este elemento identifica la entidad que valida la firma y genera el informe de validación.

Contenido:

Este elemento debe contener la identidad digital del servicio de validación, según lo especificado en la cláusula 5.5.3 de ETSI TS 119 612 [6].

Este elemento también puede contener otra información sobre el Proveedor de Servicios de Confianza (TSP), según lo especificado en la cláusula 5.4 de ETSI TS 119 612 [6], así como cualquier información adicional que pueda utilizarse para identificar al validador.

4.6 Firma del Informe de Validación

Presencia: Opcional

Descripción del Requisito: Este elemento contiene la firma del informe de validación.

Contenido:

Cuando esté presente, este elemento debe contener la firma sobre el informe de validación de firma, la cual debe ser generada por el servicio de validación que realizó la validación y creó el informe de validación.

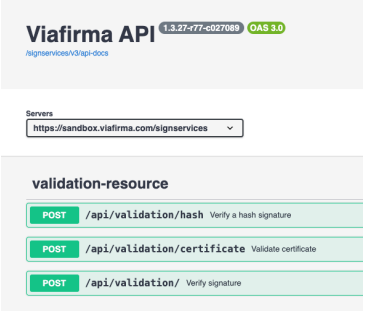
5. ANEXOS

5.1 Acceso al servicio de validación

El servicio de validación de firmas se encuentra publicado en la siguiente dirección: https://valida.viafirma.com

5.2 Documentación API del servicio de validación

La documentación del API del servicio de validación de firma está basada en openApi 3.0, contando además con una herramienta visual de ayuda a integradores basada en Swagger, publicada para entorno sandbox en la siguiente dirección: https://sandbox.viafirma.com/signservices/swagger-ui/index.html



El uso del API requiere credenciales de autenticación que deben ser solicitadas y suministradas por Viafirma a las partes interesadas.

5.3 Ejemplos de informes de validación

5.3.1 Informe desde la UI del Servicio

El siguiente enlace apunta a un informe de ejemplo de validación un documento firmado por dos firmantes y que incorpora además sello electrónico, sellos de tiempo y estamper de firma.

ℹ️ YCNL-DOAH-OF10-TGBC-8173-8140-8581-76

5.3.2 Informe XML

Acorde la norma técnica de validación el servicio genera los formatos XML necesarios con los detalles y resultados.

5.3.2.1 Informe Simple

Ref. simpleReport.xml

Python

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SimpleReport xmlns="http://dss.esig.europa.eu/validation/simple-report">
    <Policy>
        <PolicyName>QES AdESQC TL based</PolicyName>
        <PolicyDescription>Validate electronic signatures and indicates whether they are Advanced electronic
Signatures (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a
                Qualified electronic Signature (QES). All certificates and their related chains supporting the
signatures are validated against the EU Member State Trusted Lists (this includes
                signer's certificate and certificates used to validate certificate validity status services -
CRLs, OCSP, and time-stamps).
      </PolicyDescription>
    </Policy>
    <ValidationTime>2025-01-29T11:33:09</ValidationTime>
    <DocumentName></DocumentName>
    <ValidSignaturesCount>0</ValidSignaturesCount>
    <SignaturesCount>1</SignaturesCount>
    <Signature Id="id-9a8d1dfe229f2ebe6995980a1bd72452fcaa5c825efda70002504276ac8eeb90"
SignatureFormat="PAdES-BASELINE-B">
        <SigningTime>2023-03-27T20:03:13</SigningTime>
        <SignedBy>JOSE RAUL MADERA OROPEZA</SignedBy>
        <SignatureLevel description="Not applicable">N/A</SignatureLevel>
        <Indication>INDETERMINATE</Indication>
        <SubIndication>NO_POE</SubIndication>
        <Errors>The certificate path is not trusted!</Errors>
        <Errors>The past signature validation is not conclusive!</Errors>
        <Warnings>The signature/seal is an INDETERMINATE AdES!</Warnings>
        <SignatureScope name="Full PDF" scope="FullSignatureScope">Full document</SignatureScope>
    </Signature>
</SimpleReport>
```

5.3.2.2 Informe Detallado

Ref. detailedReport.xml

Python

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DetailedReport xmlns="http://dss.esig.europa.eu/validation/detailed-report">
    <Signatures Id="id-9a8d1dfe229f2ebe6995980a1bd72452fcaa5c825efda70002504276ac8eeb90">
        <ValidationProcessBasicSignatures>
            <Constraint Id="id-9a8d1dfe229f2ebe6995980a1bd72452fcaa5c825efda70002504276ac8eeb90">
                <Name NameId="ADEST_ROBVPIIC">Is the result of the Basic Validation Process conclusive?</Name>
                <Status>NOT OK</Status>
                <Error NameId="ADEST_ROBVPIIC_ANS">The result of the Basic validation process is not
conclusive!</Error>
            </Constraint>
            <Conclusion>
                <Indication>INDETERMINATE</Indication>
                <SubIndication>REVOKED_NO_POE</SubIndication>
                <Errors NameId="BBB_XCV_ISCR_ANS">The certificate is revoked!</Errors>
            </Conclusion>
        </ValidationProcessBasicSignatures>
        <ValidationProcessLongTermData>
            <Constraint>
                <Name NameId="LTV_ABSV">Is the result of the Basic Validation Process acceptable?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint
Id="ac83c9118b61d0c886bf3423b136ec9542a2e062adf6177491509bee027f19faa4c375d19852d579df0dd4b2325548862a608e2a12ea
956b32e992bbefb37bba">
                <Name NameId="ADEST_RORPIIC">Is the result of the revocation data validation process
acceptable?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint
Id="942a1c24f08db9666c72b1cefb9bbfdfa346b844a1a323be89fd799402b4edd3d2abfbec06bd9834973c64d2f80635db150a92e376e6
30f558deae7cc0bcf8b5">
                <Name NameId="ADEST_RORPIIC">Is the result of the revocation data validation process
acceptable?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="ADEST_IRTPTBST">Is revocation time posterior to best-signature-time?</Name>
                <Status>NOT OK</Status>
                <Error NameId="ADEST_IRTPTBST_ANS">The revocation time is not posterior to
best-signature-time!</Error>
                <AdditionalInfo>Best signature time : 2025-01-29 12:33</AdditionalInfo>
            </Constraint>
            <Conclusion>
                <Indication>INDETERMINATE</Indication>
                <SubIndication>REVOKED_NO_POE</SubIndication>
                <Errors NameId="ADEST_IRTPTBST_ANS">The revocation time is not posterior to
best-signature-time!</Errors>
            </Conclusion>
        </ValidationProcessLongTermData>
```

```
        <ValidationProcessArchivalData>
            <Constraint>
                <Name NameId="ARCH_LTVV">Is the result of the LTV validation process acceptable?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="PSV_IPSVC">Is past signature validation conclusive?</Name>
                <Status>NOT OK</Status>
                <Error NameId="PSV_IPSVC_ANS">The past signature validation is not conclusive!</Error>
            </Constraint>
            <Conclusion>
                <Indication>INDETERMINATE</Indication>
                <SubIndication>NO_POE</SubIndication>
                <Errors NameId="PSV_IPSVC_ANS">The past signature validation is not conclusive!</Errors>
            </Conclusion>
        </ValidationProcessArchivalData>
    </Signatures>
    <BasicBuildingBlocks
Id="ac83c9118b61d0c886bf3423b136ec9542a2e062adf6177491509bee027f19faa4c375d19852d579df0dd4b2325548862a608e2a12ea
956b32e992bbefb37bba" Type="REVOCATION">
        <ISC>
            <Constraint>
                <Name NameId="BBB_ICS_ISCI">Is there an identified candidate for the signing certificate?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </ISC>
        <CV>
            <Constraint>
                <Name NameId="BBB_CV_IRDOF">Is the reference data object(s) found?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_CV_IRDOI">Is the reference data object(s) intact?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_CV_ISI">Is the signature intact?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </CV>
        <SAV>
            <Constraint>
                <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                <Status>OK</Status>
                <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </SAV>
        <XCV>
            <Constraint>
```

```
                <Name NameId="BBB_XCV_CCCBB">Can the certificate chain be built till the trust anchor?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
                <Name NameId="BBB_XCV_SUB">Is the certificate validation concluant ?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
            <SubXCV Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3" TrustAnchor="true">
                <Conclusion>
                    <Indication>PASSED</Indication>
                </Conclusion>
            </SubXCV>
        </XCV>
        <Conclusion>
            <Indication>PASSED</Indication>
        </Conclusion>
    </BasicBuildingBlocks>
    <BasicBuildingBlocks
Id="942a1c24f08db9666c72b1cefb9bbfdfa346b844a1a323be89fd799402b4edd3d2abfbec06bd9834973c64d2f80635db150a92e376e6
30f558deae7cc0bcf8b5" Type="REVOCATION">
        <ISC>
            <Constraint>
                <Name NameId="BBB_ICS_ISCI">Is there an identified candidate for the signing certificate?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </ISC>
        <CV>
            <Constraint>
                <Name NameId="BBB_CV_IRDOF">Is the reference data object(s) found?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_CV_IRDOI">Is the reference data object(s) intact?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_CV_ISI">Is the signature intact?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </CV>
        <SAV>
            <Constraint>
                <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                <Status>OK</Status>
                <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
```

```
        </SAV>
        <XCV>
            <Constraint>
                <Name NameId="BBB_XCV_CCCBB">Can the certificate chain be built till the trust anchor?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint Id="1131C097A9DCB12D151815D6114D379194F0CF87344131D56B0703A6C38F11F0">
                <Name NameId="BBB_XCV_SUB">Is the certificate validation concluant ?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA">
                <Name NameId="BBB_XCV_SUB">Is the certificate validation concluant ?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
                <Name NameId="BBB_XCV_SUB">Is the certificate validation concluant ?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
            <SubXCV Id="1131C097A9DCB12D151815D6114D379194F0CF87344131D56B0703A6C38F11F0" TrustAnchor="false">
                <Constraint>
                    <Name NameId="BBB_XCV_ICSI">Is the certificate's signature intact?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                    <Status>OK</Status>
                    <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ISCR">Is the certificate not revoked?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ISCOH">Is the certificate on hold?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ICTIVRSC">Is the current time in the validity range of the signer's
certificate?</Name>
                    <Status>OK</Status>
                    <AdditionalInfo>Certificate validity : 2021-10-26 22:59 to 2031-10-26 21:59</AdditionalInfo>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_OCSP_NO_CHECK">The certificate has the id-pkix-ocsp-nocheck extension
(RFC is skipped)</Name>
                    <Status>OK</Status>
                </Constraint>
                <Conclusion>
                    <Indication>PASSED</Indication>
                </Conclusion>
            </SubXCV>
            <SubXCV Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA" TrustAnchor="false">
                <Constraint>
                    <Name NameId="BBB_XCV_ICSI">Is the certificate's signature intact?</Name>
                    <Status>OK</Status>
```

```
                </Constraint>
                <Constraint>
                    <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                    <Status>OK</Status>
                    <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ISCR">Is the certificate not revoked?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ISCOH">Is the certificate on hold?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ICTIVRSC">Is the current time in the validity range of the signer's
certificate?</Name>
                    <Status>OK</Status>
                    <AdditionalInfo>Certificate validity : 2021-09-23 09:51 to 2041-09-23 09:51</AdditionalInfo>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_RFC">Is the revocation freshness check concluant ?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Conclusion>
                    <Indication>PASSED</Indication>
                </Conclusion>
                <RFC>
                    <Constraint>
                        <Name NameId="BBB_XCV_IRDPFC">Is the revocation data present for the certificate?</Name>
                        <Status>OK</Status>
                    </Constraint>
                    <Constraint>
                        <Name NameId="BBB_RFC_NUP">Is there a Next Update defined for the revocation
data?</Name>
                        <Status>OK</Status>
                    </Constraint>
                    <Constraint>
                        <Name NameId="BBB_RFC_IRIF">Is the revocation information fresh for the
certificate?</Name>
                        <Status>OK</Status>
                        <AdditionalInfo>Next update : 2025-05-03 12:04</AdditionalInfo>
                    </Constraint>
                    <Constraint>
                        <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                        <Status>OK</Status>
                        <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
                    </Constraint>
                    <Conclusion>
                        <Indication>PASSED</Indication>
                    </Conclusion>
                </RFC>
            </SubXCV>
            <SubXCV Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3" TrustAnchor="true">
                <Conclusion>
                    <Indication>PASSED</Indication>
                </Conclusion>
            </SubXCV>
```

```
        </XCV>
        <Conclusion>
            <Indication>PASSED</Indication>
        </Conclusion>
    </BasicBuildingBlocks>
    <BasicBuildingBlocks Id="id-9a8d1dfe229f2ebe6995980a1bd72452fcaa5c825efda70002504276ac8eeb90"
Type="SIGNATURE">
        <FC>
            <Constraint>
                <Name NameId="BBB_FC_IEFF">Is the expected format found?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </FC>
        <ISC>
            <Constraint>
                <Name NameId="BBB_ICS_ISCI">Is there an identified candidate for the signing certificate?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_ICS_ISCS">Is the signing certificate signed?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_ICS_ISASCP">Is the signed attribute: 'signing-certificate' present?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_ICS_ISACDP">Is the signed attribute: 'cert-digest' of the certificate
present?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_ICS_ICDVV">Is the certificate's digest value valid?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_ICS_AIDNASNE">Are the issuer distinguished name and the serial number
equal?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </ISC>
        <VCI>
            <Constraint>
                <Name NameId="BBB_VCI_ISPK">Is the signature policy known?</Name>
                <Status>OK</Status>
            </Constraint>
            <Conclusion>
                <Indication>PASSED</Indication>
            </Conclusion>
        </VCI>
        <CV>
            <Constraint>
```

```
            <Name NameId="BBB_CV_IRDOF">Is the reference data object(s) found?</Name>
            <Status>OK</Status>
        </Constraint>
        <Constraint>
            <Name NameId="BBB_CV_IRDOI">Is the reference data object(s) intact?</Name>
            <Status>OK</Status>
        </Constraint>
        <Constraint>
            <Name NameId="BBB_CV_ISI">Is the signature intact?</Name>
            <Status>OK</Status>
        </Constraint>
        <Conclusion>
            <Indication>PASSED</Indication>
        </Conclusion>
    </CV>
    <SAV>
        <Constraint>
            <Name NameId="BBB_SAV_ISQPSTP">Is signed qualifying property: 'signing-time' present?</Name>
            <Status>OK</Status>
        </Constraint>
        <Constraint>
            <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
            <Status>OK</Status>
            <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
        </Constraint>
        <Conclusion>
            <Indication>PASSED</Indication>
        </Conclusion>
    </SAV>
    <XCV>
        <Constraint>
            <Name NameId="BBB_XCV_CCCBB">Can the certificate chain be built till the trust anchor?</Name>
            <Status>OK</Status>
        </Constraint>
        <Constraint Id="942A1C24F08DB9666C72B1CEFB9BBFDFA346B844A1A323BE89FD799402B4EDD3">
            <Name NameId="BBB_XCV_SUB">Is the certificate validation concluant ?</Name>
            <Status>NOT OK</Status>
            <Error NameId="BBB_XCV_SUB_ANS">The certificate validation is not concluant!</Error>
        </Constraint>
        <Conclusion>
            <Indication>INDETERMINATE</Indication>
            <SubIndication>REVOKED_NO_POE</SubIndication>
            <Errors NameId="BBB_XCV_ISCR_ANS">The certificate is revoked!</Errors>
        </Conclusion>
        <SubXCV Id="942A1C24F08DB9666C72B1CEFB9BBFDFA346B844A1A323BE89FD799402B4EDD3" TrustAnchor="false">
            <Constraint>
                <Name NameId="QUAL_UNIQUE_CERT">Is the certificate unique ?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_XCV_ICSI">Is the certificate's signature intact?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                <Status>OK</Status>
                <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
            </Constraint>
```

```
                <Constraint>
                    <Name NameId="BBB_XCV_ISCGKU">Has the signer's certificate given key-usage?</Name>
                    <Status>OK</Status>
                    <AdditionalInfo>Key usage : keyEncipherment, digitalSignature,
nonRepudiation</AdditionalInfo>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_AIA_PRES">Is authority info access present?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_REVOC_PRES">Is revocation info access present?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ISCR">Is the certificate not revoked?</Name>
                    <Status>NOT OK</Status>
                    <Error NameId="BBB_XCV_ISCR_ANS">The certificate is revoked!</Error>
                    <AdditionalInfo>Revocation reason : superseded (date : 2023-10-24 18:37)</AdditionalInfo>
                </Constraint>
                <Conclusion>
                    <Indication>INDETERMINATE</Indication>
                    <SubIndication>REVOKED_NO_POE</SubIndication>
                    <Errors NameId="BBB_XCV_ISCR_ANS">The certificate is revoked!</Errors>
                </Conclusion>
                <RFC>
                    <Constraint>
                        <Name NameId="BBB_XCV_IRDPFC">Is the revocation data present for the certificate?</Name>
                        <Status>OK</Status>
                    </Constraint>
                    <Constraint>
                        <Name NameId="BBB_RFC_NUP">Is there a Next Update defined for the revocation
data?</Name>
                        <Status>WARNING</Status>
                        <Warning NameId="BBB_RFC_NUP_ANS">There is no Next Update defined for the revocation
data!</Warning>
                    </Constraint>
                    <Constraint>
                        <Name NameId="BBB_RFC_IRIF">Is the revocation information fresh for the
certificate?</Name>
                        <Status>OK</Status>
                        <AdditionalInfo>Next update : not defined</AdditionalInfo>
                    </Constraint>
                    <Constraint>
                        <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                        <Status>OK</Status>
                        <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
                    </Constraint>
                    <Conclusion>
                        <Indication>PASSED</Indication>
                    </Conclusion>
                </RFC>
            </SubXCV>
            <SubXCV Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA" TrustAnchor="false">
                <Constraint>
                    <Name NameId="BBB_XCV_ICSI">Is the certificate's signature intact?</Name>
                    <Status>OK</Status>
                </Constraint>
```

```
                <Constraint>
                    <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                    <Status>OK</Status>
                    <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ISCR">Is the certificate not revoked?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ISCOH">Is the certificate on hold?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_ICTIVRSC">Is the current time in the validity range of the signer's
certificate?</Name>
                    <Status>OK</Status>
                    <AdditionalInfo>Certificate validity : 2021-09-23 09:51 to 2041-09-23 09:51</AdditionalInfo>
                </Constraint>
                <Constraint>
                    <Name NameId="BBB_XCV_RFC">Is the revocation freshness check concluant ?</Name>
                    <Status>OK</Status>
                </Constraint>
                <Conclusion>
                    <Indication>PASSED</Indication>
                </Conclusion>
                <RFC>
                    <Constraint>
                        <Name NameId="BBB_XCV_IRDPFC">Is the revocation data present for the certificate?</Name>
                        <Status>OK</Status>
                    </Constraint>
                    <Constraint>
                        <Name NameId="BBB_RFC_NUP">Is there a Next Update defined for the revocation
data?</Name>
                        <Status>OK</Status>
                    </Constraint>
                    <Constraint>
                        <Name NameId="BBB_RFC_IRIF">Is the revocation information fresh for the
certificate?</Name>
                        <Status>OK</Status>
                        <AdditionalInfo>Next update : 2025-05-03 12:04</AdditionalInfo>
                    </Constraint>
                    <Constraint>
                        <Name NameId="ASCCM">Are signature cryptographic constraints met?</Name>
                        <Status>OK</Status>
                        <AdditionalInfo>Validation time : 2025-01-29 12:33</AdditionalInfo>
                    </Constraint>
                    <Conclusion>
                        <Indication>PASSED</Indication>
                    </Conclusion>
                </RFC>
            </SubXCV>
            <SubXCV Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3" TrustAnchor="true">
                <Conclusion>
                    <Indication>PASSED</Indication>
                </Conclusion>
            </SubXCV>
        </XCV>
```

```
        <PSV>
            <Constraint>
                <Name NameId="PSV_IPCVA">Is past certificate validation acceptable?</Name>
                <Status>NOT OK</Status>
                <Error NameId="PSV_IPCVA_ANS">The past certificate validation is not acceptable!</Error>
            </Constraint>
            <Conclusion>
                <Indication>INDETERMINATE</Indication>
                <SubIndication>NO_POE</SubIndication>
                <Errors NameId="PSV_IPCVA_ANS">The past certificate validation is not acceptable!</Errors>
            </Conclusion>
        </PSV>
        <PCV>
            <Constraint>
                <Name NameId="BBB_XCV_CCCBB">Can the certificate chain be built till the trust anchor?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_XCV_ICSI">Is the certificate's signature intact?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="BBB_XCV_ICSI">Is the certificate's signature intact?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="PCV_IVTSC">Is validation time sliding conclusive?</Name>
                <Status>NOT OK</Status>
                <Error NameId="PCV_IVTSC_ANS">The indications returned by validation time sliding
sub-process.</Error>
            </Constraint>
            <Conclusion>
                <Indication>INDETERMINATE</Indication>
                <SubIndication>NO_POE</SubIndication>
                <Errors NameId="PCV_IVTSC_ANS">The indications returned by validation time sliding
sub-process.</Errors>
            </Conclusion>
            <ControlTime>2025-01-29T11:33:09</ControlTime>
        </PCV>
        <VTS>
            <Constraint>
                <Name NameId="BBB_VTS_IRDPFC">Is there a satisfying revocation status information ?</Name>
                <Status>OK</Status>
            </Constraint>
            <Constraint>
                <Name NameId="PSV_ITPOCOBCT">Is there a POE of the certificate at (or before)
control-time?</Name>
                <Status>NOT OK</Status>
                <Error NameId="PSV_ITPOOBCT_ANS">No Proof Of Existence found at (or before)
control-time!</Error>
                <AdditionalInfo>Control time : 2025-01-29 12:33</AdditionalInfo>
            </Constraint>
            <Conclusion>
                <Indication>INDETERMINATE</Indication>
                <SubIndication>NO_POE</SubIndication>
                <Errors NameId="PSV_ITPOOBCT_ANS">No Proof Of Existence found at (or before)
control-time!</Errors>
            </Conclusion>
```

```
            <ControlTime>2025-01-29T11:33:09</ControlTime>
        </VTS>
        <Conclusion>
            <Indication>INDETERMINATE</Indication>
            <SubIndication>REVOKED_NO_POE</SubIndication>
            <Errors NameId="BBB_XCV_ISCR_ANS">The certificate is revoked!</Errors>
        </Conclusion>
    </BasicBuildingBlocks>
    <QMatrixBlock>
        <SignatureAnalysis Id="id-9a8d1dfe229f2ebe6995980a1bd72452fcaa5c825efda70002504276ac8eeb90"
SignatureQualification="N/A">
            <Constraint>
                <Name NameId="QUAL_IS_ADES">Is the signature/seal an acceptable AdES (ETSI EN 319 102-1)
?</Name>
                <Status>WARNING</Status>
                <Warning NameId="QUAL_IS_ADES_IND">The signature/seal is an INDETERMINATE AdES!</Warning>
            </Constraint>
            <Constraint>
                <Name NameId="QUAL_TRUSTED_CERT_PATH">Is the certificate path trusted?</Name>
                <Status>NOT OK</Status>
                <Error NameId="QUAL_TRUSTED_CERT_PATH_ANS">The certificate path is not trusted!</Error>
            </Constraint>
            <Conclusion>
                <Indication>FAILED</Indication>
                <Errors NameId="QUAL_TRUSTED_CERT_PATH_ANS">The certificate path is not trusted!</Errors>
                <Errors NameId="QUAL_TRUSTED_CERT_PATH_ANS">The certificate path is not trusted!</Errors>
                <Warnings NameId="QUAL_IS_ADES_IND">The signature/seal is an INDETERMINATE AdES!</Warnings>
            </Conclusion>
        </SignatureAnalysis>
    </QMatrixBlock>
</DetailedReport>
```

5.3.2.3 Informe Diagnóstico

Ref. diagnosticReport.xml

Python

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DiagnosticData xmlns="http://dss.esig.europa.eu/validation/diagnostic">
    <DocumentName></DocumentName>
    <ValidationDate>2025-01-29T11:33:09</ValidationDate>
    <Signatures>
        <Signature Id="id-9a8d1dfe229f2ebe6995980a1bd72452fcaa5c825efda70002504276ac8eeb90">
            <SignatureFilename></SignatureFilename>
            <DateTime>2023-03-27T20:03:13</DateTime>
            <SignatureFormat>PAdES-BASELINE-B</SignatureFormat>
            <StructuralValidation>
                <Valid>true</Valid>
            </StructuralValidation>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            <SigningCertificate Id="942A1C24F08DB9666C72B1CEFB9BBFDFA346B844A1A323BE89FD799402B4EDD3">
                <AttributePresent>true</AttributePresent>
                <DigestValuePresent>true</DigestValuePresent>
                <DigestValueMatch>true</DigestValueMatch>
                <IssuerSerialMatch>true</IssuerSerialMatch>
            </SigningCertificate>
            <CertificateChain>
                <ChainItem Id="942A1C24F08DB9666C72B1CEFB9BBFDFA346B844A1A323BE89FD799402B4EDD3">
                    <Source>SIGNATURE</Source>
                </ChainItem>
                <ChainItem Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA">
                    <Source>SIGNATURE</Source>
                </ChainItem>
                <ChainItem Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
                    <Source>TRUSTED_STORE</Source>
                </ChainItem>
            </CertificateChain>
            <ContentType>application/pdf</ContentType>
            <CommitmentTypeIndication/>
            <ClaimedRoles/>
            <Timestamps/>
            <SignatureScopes>
                <SignatureScope name="Full PDF" scope="FullSignatureScope">Full document</SignatureScope>
            </SignatureScopes>
        </Signature>
    </Signatures>
    <UsedCertificates>
        <Certificate Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
```

```
            <SubjectDistinguishedName Format="CANONICAL">c=do,o=oficina gubernamental de las tecnologias de la
informacion y comunicacion - ogtic,cn=ogtic root ca</SubjectDistinguishedName>
            <SubjectDistinguishedName Format="RFC2253">C=DO,O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA
INFORMACION Y COMUNICACION - OGTIC,CN=OGTIC ROOT CA</SubjectDistinguishedName>
            <IssuerDistinguishedName Format="CANONICAL">c=do,o=oficina gubernamental de las tecnologias de la
informacion y comunicacion - ogtic,cn=ogtic root ca</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253">C=DO,O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA
INFORMACION Y COMUNICACION - OGTIC,CN=OGTIC ROOT CA</IssuerDistinguishedName>
            <SerialNumber>322847868955659408696920901854753721203015371 02</SerialNumber>
            <CommonName>OGTIC ROOT CA</CommonName>
            <CountryName>DO</CountryName>
            <OrganizationName>OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACION -
OGTIC</OrganizationName>
            <AuthorityInformationAccessUrls/>
            <CRLDistributionPoints/>
            <OCSPAccessUrls/>
            <DigestAlgoAndValues>
                <DigestAlgoAndValue>
                    <DigestMethod>SHA1</DigestMethod>
                    <DigestValue>Ver4j3tIqEWXF9duSW2fa2qqDWY=</DigestValue>
                </DigestAlgoAndValue>
            </DigestAlgoAndValues>
            <NotAfter>2046-09-16T05:56:23</NotAfter>
            <NotBefore>2021-09-16T05:56:23</NotBefore>
            <PublicKeySize>4096</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
                <KeyUsage>crlSign</KeyUsage>
                <KeyUsage>keyCertSign</KeyUsage>
                <KeyUsage>digitalSignature</KeyUsage>
            </KeyUsageBits>
            <IdKpOCSPSigning>false</IdKpOCSPSigning>
            <IdPkixOcspNoCheck>false</IdPkixOcspNoCheck>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>4096</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            <CertificateChain/>
            <Trusted>true</Trusted>
            <SelfSigned>true</SelfSigned>
            <CertificatePolicyIds>
                <oid>2.5.29.32.0</oid>
            </CertificatePolicyIds>
            <QCStatementIds/>
            <QCTypes/>
            <TrustedServiceProviders/>
            <Revocations/>
            <Info/>
        </Certificate>
        <Certificate Id="942A1C24F08DB9666C72B1CEFB9BBFDFA346B844A1A323BE89FD799402B4EDD3">
            <SubjectDistinguishedName Format="CANONICAL">c=do,o=indotel,ou=firma
digital,2.5.4.12=#0c09454e4341524741444f,2.5.4.4=#0c0e4d4144455241204f524f50455a41,2.5.4.42=#0c094a4f53452052415
54c,2.5.4.5=#1311494443444f2d303331303434353033323 9,cn=jose raul madera
```

```
oropeza,2.5.4.46=#13264345525449464943414441f20444520454d504c4541444f205055424c49434f20285153434429</SubjectDisti
nguishedName>
            <SubjectDistinguishedName Format="RFC2253">C=DO,O=INDOTEL,OU=FIRMA
DIGITAL,2.5.4.12=#0c09454e4341524741444f,2.5.4.4=#0c0e4d4144455241204f524f50455a41,2.5.4.42=#0c094a4f53452052415
54c,2.5.4.5=#1311494443444f2d3033313034343530333239,CN=JOSE RAUL MADERA
OROPEZA,2.5.4.46=#13264345525449464943414441f20444520454d504c4541444f205055424c49434f20285153434429</SubjectDisti
nguishedName>
            <IssuerDistinguishedName Format="CANONICAL">c=do,o=oficina gubernamental de las tecnologias de la
informacion y comunicacion - ogtic,cn=ogtic qualified certificates</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253">C=DO,O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA
INFORMACION Y COMUNICACION - OGTIC,CN=OGTIC QUALIFIED CERTIFICATES</IssuerDistinguishedName>
            <SerialNumber>648090805026696387155805408357346982596627038886</SerialNumber>
            <CommonName>JOSE RAUL MADERA OROPEZA</CommonName>
            <CountryName>DO</CountryName>
            <OrganizationName>INDOTEL</OrganizationName>
            <GivenName>JOSE RAUL</GivenName>
            <OrganizationalUnit>FIRMA DIGITAL</OrganizationalUnit>
            <Surname>MADERA OROPEZA</Surname>
            <AuthorityInformationAccessUrls>
                <Url>http://ca.ogtic.gob.do/cer/ogticqualifiedcertificates.crt</Url>
            </AuthorityInformationAccessUrls>
            <CRLDistributionPoints>
                <Url>http://crl.ogtic.gob.do/ogticqualifiedcertificates.crl</Url>
                <Url>http://crl2.ogtic.gob.do/ogticqualifiedcertificates.crl</Url>
            </CRLDistributionPoints>
            <OCSPAccessUrls>
                <Url>http://ca.ogtic.gob.do/ocsp</Url>
            </OCSPAccessUrls>
            <DigestAlgoAndValues>
                <DigestAlgoAndValue>
                    <DigestMethod>SHA1</DigestMethod>
                    <DigestValue>2RGmpLVxcpqhwgEp3NQRrgXYlNw=</DigestValue>
                </DigestAlgoAndValue>
            </DigestAlgoAndValues>
            <NotAfter>2023-11-19T13:35:42</NotAfter>
            <NotBefore>2021-11-19T13:35:42</NotBefore>
            <PublicKeySize>2048</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
                <KeyUsage>keyEncipherment</KeyUsage>
                <KeyUsage>digitalSignature</KeyUsage>
                <KeyUsage>nonRepudiation</KeyUsage>
            </KeyUsageBits>
            <IdKpOCSPSigning>false</IdKpOCSPSigning>
            <IdPkixOcspNoCheck>false</IdPkixOcspNoCheck>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>4096</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            <SigningCertificate Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA"/>
            <CertificateChain>
                <ChainItem Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA">
                    <Source>SIGNATURE</Source>
```

```
                </ChainItem>
                <ChainItem Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
                    <Source>TRUSTED_STORE</Source>
                </ChainItem>
            </CertificateChain>
            <Trusted>false</Trusted>
            <SelfSigned>false</SelfSigned>
            <CertificatePolicyIds>
                <oid Description="qcp-natural-qscd">0.4.0.194112.1.2</oid>
                <oid>1.3.6.1.4.1.49353.6.3.2</oid>
            </CertificatePolicyIds>
            <QCStatementIds>
                <oid Description="qc-compliant">0.4.0.1862.1.1</oid>
                <oid Description="qc-sscd">0.4.0.1862.1.4</oid>
            </QCStatementIds>
            <QCTypes/>
            <TrustedServiceProviders/>
            <Revocations>
                <Revocation
Id="942a1c24f08db9666c72b1cefb9bbfdfa346b844a1a323be89fd799402b4edd3d2abfbec06bd9834973c64d2f80635db150a92e376e6
30f558deae7cc0bcf8b5">
                    <Origin>EXTERNAL</Origin>
                    <Source>OCSPToken</Source>
                    <SourceAddress>http://ca.ogtic.gob.do/ocsp</SourceAddress>
                    <Available>true</Available>
                    <Status>false</Status>
                    <Reason>superseded</Reason>
                    <ProductionDate>2025-01-29T11:33:07</ProductionDate>
                    <ThisUpdate>2025-01-29T11:33:07</ThisUpdate>
                    <RevocationDate>2023-10-24T16:37:28</RevocationDate>
                    <DigestAlgoAndValues>
                        <DigestAlgoAndValue>
                            <DigestMethod>SHA1</DigestMethod>
                            <DigestValue>n75EWIvgBAFOHxMWPwveKnOiZaw=</DigestValue>
                        </DigestAlgoAndValue>
                    </DigestAlgoAndValues>
                    <BasicSignature>
                        <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                        <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
                        <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                        <ReferenceDataFound>true</ReferenceDataFound>
                        <ReferenceDataIntact>true</ReferenceDataIntact>
                        <SignatureIntact>true</SignatureIntact>
                        <SignatureValid>true</SignatureValid>
                    </BasicSignature>
                    <SigningCertificate Id="1131C097A9DCB12D151815D6114D379194F0CF87344131D56B0703A6C38F11F0"/>
                    <CertificateChain>
                        <ChainItem Id="1131C097A9DCB12D151815D6114D379194F0CF87344131D56B0703A6C38F11F0">
                            <Source>OCSP_RESPONSE</Source>
                        </ChainItem>
                        <ChainItem Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA">
                            <Source>SIGNATURE</Source>
                        </ChainItem>
                        <ChainItem Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
                            <Source>TRUSTED_STORE</Source>
                        </ChainItem>
                    </CertificateChain>
                    <Info/>
```

```
                </Revocation>
            </Revocations>
            <Info>
                <Message Id="0">No CRL info found !</Message>
            </Info>
        </Certificate>
        <Certificate Id="1131C097A9DCB12D151815D6114D379194F0CF87344131D56B0703A6C38F11F0">
            <SubjectDistinguishedName Format="CANONICAL">c=do,o=oficina gubernamental de las tecnologias de la
informacion y comunicacion - ogtic,cn=ogtic ocsp subca</SubjectDistinguishedName>
            <SubjectDistinguishedName Format="RFC2253">C=DO,O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA
INFORMACION Y COMUNICACION - OGTIC,CN=OGTIC OCSP SUBCA</SubjectDistinguishedName>
            <IssuerDistinguishedName Format="CANONICAL">c=do,o=oficina gubernamental de las tecnologias de la
informacion y comunicacion - ogtic,cn=ogtic qualified certificates</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253">C=DO,O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA
INFORMACION Y COMUNICACION - OGTIC,CN=OGTIC QUALIFIED CERTIFICATES</IssuerDistinguishedName>
            <SerialNumber>81274588256281319931688782635592782146006329158</SerialNumber>
            <CommonName>OGTIC OCSP SUBCA</CommonName>
            <CountryName>DO</CountryName>
            <OrganizationName>OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACION -
OGTIC</OrganizationName>
            <AuthorityInformationAccessUrls/>
            <CRLDistributionPoints/>
            <OCSPAccessUrls/>
            <DigestAlgoAndValues>
                <DigestAlgoAndValue>
                    <DigestMethod>SHA1</DigestMethod>
                    <DigestValue>pX1BJhNm8jShaRUSYVICeKA82P0=</DigestValue>
                </DigestAlgoAndValue>
            </DigestAlgoAndValues>
            <NotAfter>2031-10-26T20:59:56</NotAfter>
            <NotBefore>2021-10-26T20:59:56</NotBefore>
            <PublicKeySize>2048</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
                <KeyUsage>digitalSignature</KeyUsage>
            </KeyUsageBits>
            <IdKpOCSPSigning>true</IdKpOCSPSigning>
            <IdPkixOcspNoCheck>true</IdPkixOcspNoCheck>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>4096</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            <SigningCertificate Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA"/>
            <CertificateChain>
                <ChainItem Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA">
                    <Source>SIGNATURE</Source>
                </ChainItem>
                <ChainItem Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
                    <Source>TRUSTED_STORE</Source>
                </ChainItem>
            </CertificateChain>
            <Trusted>false</Trusted>
            <SelfSigned>false</SelfSigned>
```

```
            <CertificatePolicyIds/>
            <QCStatementIds/>
            <QCTypes/>
            <TrustedServiceProviders/>
            <Revocations/>
            <Info>
                <Message Id="0">OCSP check not needed: id-pkix-ocsp-nocheck extension present.</Message>
                <Message Id="1">OCSP check not needed: id-pkix-ocsp-nocheck extension present.</Message>
                <Message Id="2">OCSP check not needed: id-pkix-ocsp-nocheck extension present.</Message>
            </Info>
        </Certificate>
        <Certificate Id="AC83C9118B61D0C886BF3423B136EC9542A2E062ADF6177491509BEE027F19FA">
            <SubjectDistinguishedName Format="CANONICAL">c=do,o=oficina gubernamental de las tecnologias de la
informacion y comunicacion - ogtic,cn=ogtic qualified certificates</SubjectDistinguishedName>
            <SubjectDistinguishedName Format="RFC2253">C=DO,O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA
INFORMACION Y COMUNICACION - OGTIC,CN=OGTIC QUALIFIED CERTIFICATES</SubjectDistinguishedName>
            <IssuerDistinguishedName Format="CANONICAL">c=do,o=oficina gubernamental de las tecnologias de la
informacion y comunicacion - ogtic,cn=ogtic root ca</IssuerDistinguishedName>
            <IssuerDistinguishedName Format="RFC2253">C=DO,O=OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA
INFORMACION Y COMUNICACION - OGTIC,CN=OGTIC ROOT CA</IssuerDistinguishedName>
            <SerialNumber>371334630554270973313381395041929416973712549225</SerialNumber>
            <CommonName>OGTIC QUALIFIED CERTIFICATES</CommonName>
            <CountryName>DO</CountryName>
            <OrganizationName>OFICINA GUBERNAMENTAL DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACION -
OGTIC</OrganizationName>
            <AuthorityInformationAccessUrls>
                <Url>http://ca.ogtic.gob.do/cer/ogticroot.crt</Url>
            </AuthorityInformationAccessUrls>
            <CRLDistributionPoints>
                <Url>http://crl.ogtic.gob.do/ogticroot.crl</Url>
            </CRLDistributionPoints>
            <OCSPAccessUrls>
                <Url>http://ca.ogtic.gob.do/ocsp</Url>
            </OCSPAccessUrls>
            <DigestAlgoAndValues>
                <DigestAlgoAndValue>
                    <DigestMethod>SHA1</DigestMethod>
                    <DigestValue>Cb7e9DjnrkUAV/nB0inrYWjo7tI=</DigestValue>
                </DigestAlgoAndValue>
            </DigestAlgoAndValues>
            <NotAfter>2041-09-23T07:51:46</NotAfter>
            <NotBefore>2021-09-23T07:51:46</NotBefore>
            <PublicKeySize>4096</PublicKeySize>
            <PublicKeyEncryptionAlgo>RSA</PublicKeyEncryptionAlgo>
            <KeyUsageBits>
                <KeyUsage>crlSign</KeyUsage>
                <KeyUsage>keyCertSign</KeyUsage>
                <KeyUsage>digitalSignature</KeyUsage>
            </KeyUsageBits>
            <IdKpOCSPSigning>false</IdKpOCSPSigning>
            <IdPkixOcspNoCheck>false</IdPkixOcspNoCheck>
            <BasicSignature>
                <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                <KeyLengthUsedToSignThisToken>4096</KeyLengthUsedToSignThisToken>
                <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                <ReferenceDataFound>true</ReferenceDataFound>
                <ReferenceDataIntact>true</ReferenceDataIntact>
                <SignatureIntact>true</SignatureIntact>
```

```
                <SignatureValid>true</SignatureValid>
            </BasicSignature>
            <SigningCertificate Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3"/>
            <CertificateChain>
                <ChainItem Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
                    <Source>TRUSTED_STORE</Source>
                </ChainItem>
            </CertificateChain>
            <Trusted>false</Trusted>
            <SelfSigned>false</SelfSigned>
            <CertificatePolicyIds>
                <oid>1.3.6.1.4.1.49353.6</oid>
            </CertificatePolicyIds>
            <QCStatementIds/>
            <QCTypes/>
            <TrustedServiceProviders/>
            <Revocations>
                <Revocation
Id="ac83c9118b61d0c886bf3423b136ec9542a2e062adf6177491509bee027f19faa4c375d19852d579df0dd4b2325548862a608e2a12ea
956b32e992bbefb37bba">
                    <Origin>EXTERNAL</Origin>
                    <Source>CRLToken</Source>
                    <SourceAddress>http://crl.ogtic.gob.do/ogticroot.crl</SourceAddress>
                    <Available>true</Available>
                    <Status>true</Status>
                    <ProductionDate>2024-11-04T10:04:42</ProductionDate>
                    <ThisUpdate>2024-11-04T10:04:42</ThisUpdate>
                    <NextUpdate>2025-05-03T10:04:42</NextUpdate>
                    <DigestAlgoAndValues>
                        <DigestAlgoAndValue>
                            <DigestMethod>SHA1</DigestMethod>
                            <DigestValue>dOBr7hBS+KPpk3DY1bzZHm7AJaw=</DigestValue>
                        </DigestAlgoAndValue>
                    </DigestAlgoAndValues>
                    <BasicSignature>
                        <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
                        <KeyLengthUsedToSignThisToken>4096</KeyLengthUsedToSignThisToken>
                        <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
                        <ReferenceDataFound>true</ReferenceDataFound>
                        <ReferenceDataIntact>true</ReferenceDataIntact>
                        <SignatureIntact>true</SignatureIntact>
                        <SignatureValid>true</SignatureValid>
                    </BasicSignature>
                    <SigningCertificate Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3"/>
                    <CertificateChain>
                        <ChainItem Id="73DC22D876CCE886E5181D0DCB158282D7279A6A655EF51C3155BBD9B65891F3">
                            <Source>TRUSTED_STORE</Source>
                        </ChainItem>
                    </CertificateChain>
                    <Info/>
                </Revocation>
            </Revocations>
            <Info>
                <Message Id="0">No CRL info found !</Message>
                <Message Id="1">No CRL info found !</Message>
                <Message Id="2">No CRL info found !</Message>
            </Info>
        </Certificate>
```

```
    </UsedCertificates>
    <TrustedLists/>
</DiagnosticData>
```