Perfiles para la adaptación de los Web Services de @Firma 6 al protocolo OASIS-DSS

Documento nº:	@Firma-Global-XMLSOAP-PROFILE-DSS
Revisión:	061
Fecha:	14-11-2019
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

CONTROL DE COMPROBACIÓN Y APROBACIÓN

Documento nº:	@Firma-Global-XMLSOAP-PROFILE-DSS
Revisión:	061
Fecha:	14-11-2019

CONTROL DE DISTRIBUCIÓN

Documento nº:	@Firma-Global-XMLSOAP-PROFILE-DSS
Revisión:	061
Fecha:	14-11-2019

Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

Fecha de impresión 10 de noviembre de 2021

CONTROL DE MODIFICACIONES

Documento nº:	@Firma-Global-XMLSOAP-PROFILE-DSS
Revisión:	061
Fecha:	14-11-2019

Rev.	001
Fecha	11-10-2007
Descripción	Documento inicial.

Rev.	002
Fecha	26-10-2007
Descripción	Se han añadido el elemento AdditionalDocumentInfo (apartado 6.3.1.12) y observaciones al elemento DSS TransformedData (apartado 6.3.1.1).

Rev.	003
Fecha	21-01-2008
Descripción	Se ha modificado el tipo del elemento “timeStamp” devuelto en la respuesta del proceso de verificación a xs:string .

Rev.	004
Fecha	10-03-2008
Descripción	Se ha reestructurado el documento para diferenciar los elementos nuevos introducidos por los perfiles de los ya definidos por el estándar. Se ha detallado la relación de los perfiles definidos con otros perfiles y las mejoras realizadas sobre los mismos. Se ha añadido nuevos códigos de respuesta e identificadores. Incluido schemas de los perfiles así como de elementos ya definidos para detallar al lector el contenido de las interfaces XML. Se ha suprimido el protocolo de recuperación de firma del perfil Archive de @Firma al no incluir información nueva sobre el definido por OASIS.

Rev.	005
Fecha	04-03-2008
Descripción	Añadido componente XMLSignatureMode.

Rev.	006
Fecha	13-06-2008
Descripción	Se corrige una errata en las URIs de especificación de formatos de firma, donde se especificaba que la versión soportada para generación de firmas CAdES era la 1.6.3, cuando en realidad es la 1.7.3.
Rev.	007
Fecha	27-06-2008
Descripción	Se ha agrupado los elementos comunes del perfil XSS en el apartado 6.5 y se ha contemplado la generación y verificación de firmas PDF y ODF.

Rev.	008
Fecha	30-06-2008
Descripción	Se permite los componentes “dss:SignatureType” y “ades:SignatureForm” en los mensajes de respuesta de firma.

Rev.	009
Fecha	08-01-2009
Descripción	Se recompone el documento dándole una visión gráfica más intuitiva orientada a integradores. Se incluye el perfil VR de OASIS para el protocolo de verificación.

Rev.	010
Fecha	14-01-2009
Descripción	Se modifica el perfil Archive para permitir, mediante petición WS al servicio DSSAfirmaArchiveRetrieval, la obtención de un listado de todas las transacciones de firma finalizadas con éxito para una aplicación dada y cuya referencia externa coincida con la especificada.

Rev.	011
Fecha	15-04-2009
Descripción	Eliminada referencia a procesos de actualización de firma en el servicio de Registrar Firma.

Rev.	012
Fecha	05-05-2009
Descripción	Incluido en los mensaje de respuesta del servicio de Upgrade los componentes “dss:SignatureType” y “ades:SignatureForm” para indicar el formato de la firma generada. Incluido identificadores “Warning” para componente “dss:ResultMajor” y “IncompleteUpgradeOperation” para componente “dss:ResultMinor”.

Rev.	013
Fecha	16-07-2009
Descripción	Se actualizan las referencias al MAP por referencias hacia el MPR.

Rev.	014
Fecha	21-09-2009
Descripción	Modificado los identificadores utilizados por los elementos DSS "vr:FormatOK","vr:SigMathOK" y “vr:PathValiditySummary”.

Rev.	015
Fecha	14-10-2009

Descripción	Se actualiza la documentación con la evolución de los Servicios DSS realizada para la versión 5.4 de la plataforma. Esta actuación se puede resumir en los siguientes puntos:
	• Se incluye nuevos Servicios DSS:
	  ○ Validaciones de Firmas por Lotes.
	  ○ Validaciones de Certificados por Lotes.
	  ○ Validación de Certificado.
	  ○ Consulta de Peticiones Asíncronas.
	• Se añade nueva funcionalidad a los servicios:
	  ○ Firma Delegada (Firma Simple, CoSign y CounterSign).
	  ○ Validación de Firmas.
	  ○ Upgrade de Firma.

Rev.	016
Fecha	14-04-2010
Descripción	Se incluye el descripción del elemento “dss:UpdatedSignature” y la referencia al mismo en los mensajes de respuesta de los Servicios de Firma “CounterSign” y Actualización de Firma.

Rev.	017
Fecha	03-05-2010
Descripción	Añadido componente *cmism:getContentStream* en las peticiones de los servicios: • Firma Delegada (Simple, CoSign, CounterSign). • Validación y Actualización de Firma. • Validación de Certificado.

Rev.	018
Fecha	05-07-2010
Descripción	Incuido nuevos identificadores: - urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:SignedDataNotProvided (Anexo A.3.5). - urn:afirma:dss:1.0:profile:XSS:detail:SignatureCore:code:SignedDataNotProvided (Anexo A.3.7).

Rev.	019
Fecha	05-08-2010
Descripción	Se corrige el namespace correspondiente al elemento AdditionalReportOption en el ejemplo de Verificación de firmas y se aclaran algunos puntos del manual relacionados con el uso de ciertos elementos en la verificación de firmas.

Rev.	020
Fecha	15-11-2010
Descripción	Añadida en respuesta de ValidarFirma los elementos “dss:SignatureType” y “ades:SignatureForm” para incluir el formato de la firma validada.

Rev.	021
Fecha	23-12-2010
Descripción	Se actualizan las referencias a TI por TGS.

Rev.	022
Fecha	02-03-2011
Descripción	Se cambian los logos del Ministerio y se sustituyen las referencias a MPR por MPTAP. Se modifica la URL del perfil .

Rev.	023
Fecha	10-03-2011
Descripción	Se eliminan referencias a redinteradministrativa.

Rev.	024
Fecha	25-03-2011
Descripción	Se añaden las referencias y constantes necesarias para el perfil PAdES en cuanto a la validación de firmas en formato PAdES Básico y PAdES-BES.

Rev.	025
Fecha	30-03-2011
Descripción	Corregida la URI que identifica al resultado de tipo “Pending” dentro del componente "dss:ResultMajor" a la especificada en el perfil "Asynchronous Processing DSS".

Rev.	026
Fecha	12-05-2011
Descripción	Se añade una nota indicando que los formatos de hash MD2 y MD5 no se podrán utilizar en la generación de firmas de la plataforma. Se indica explícitamente que el resto de formatos de hash se puede combinar con cualquier formato de firma.

Rev.	027
Fecha	18-05-2011
Descripción	Se añade información al respecto de las políticas de Firma Soportadas.

Rev.	028
Fecha	24-05-2011
Descripción	Se modifican las referencias y constantes necesarias para el perfil PAdES Basic y PAdES-BES. Se añaden referencias y constantes necesarias para los perfiles PAdES-EPES y PAdES-LTV.

Rev.	029
Fecha	21-07-2011
Descripción	Se incluye una tabla en el apartado 8.2 donde se detallan las restricciones existentes para la extensión de una firma electrónica.

Rev.	030
Fecha	07-09-2011
Descripción	Se incluye en le apartado A.3.3 una aclaración sobre la generación y actualización de firmas CADES-XL.

Rev.	031
Fecha	21-09-2011
Descripción	Actualización del nombre del documento. Se formatea adecuadamente el documento y se corrigen títulos. Se actualizan las referencias a MPTAP (Ministerio de Política Territorial y Administraciones Públicas) por Gobierno de España. Actualización del logo de Gobierno de España en la cabecera.

Rev.	032
Fecha	13-10-2011
Descripción	Se incluyen nuevos identificadores en los apartados A.3.5 y A.3.7.

Rev.	033
Fecha	22-12-2011
Descripción	Se añade el identificador para el resultado de la validación de la extensión crítica id-kp-timestamping y se actualizan los ResultMinor para la tarea de validación del certificado del sello de tiempo contenido en el diccionario de sello de tiempo más reciente en una firma PAdES-LTV.

Rev.	034
Fecha	09-01-2012
Descripción	Se actualizan y corrigen las tablas relativas al Servicio de Actualización de Firmas de manera que una firma CAdES-A no puede actualizarse a CAdES-A, idem para XAdES-T a XAdES-T, idem para XAdES-C a XAdES-C, idem para XAdES-X a XAdES-X, idem para XAdES-XL a XAdES-XL e idem para XAdES-A a XAdES-A. Se modifica el nombre del documento 'Perfiles para la adaptación de los Web Services de @Firma 5 al protocolo OASIS-DSS' por 'Manual de Programación de WS estándar AVANZADOS DSS', así como todas las referencias al mismo. Se actualizan las tareas de validación. Se actualizan las siglas. Se añade una nueva tabla para las actualizaciones de firmas PDF.

Rev.	035
Fecha	12-06-2012
Descripción	Incluidos nuevos identificadores para contemplar los casos de cadena de certificación no válida en procesos de validación de firma.

Rev.	036
Fecha	03-09-2012
Descripción	Se actualiza el apartado 8.2.1.2.7 para indicar los componentes que se incluyen según la firma sea PDF o PADES.

Rev.	037
Fecha	08-02-2013
Descripción	Actualizado al catálogo de servicios ofrecidos por @firma 6.

Rev.	038
Fecha	07/03/2013
Descripción	Se añaden las referencias correspondientes en el servicio de validación de certificados al uso de la validación ligera de certificados mediante TSL, así como la información del certificado devuelta en caso de haberla solicitado.

Rev.	039
Fecha	06/05/2013
Descripción	Se indica en los servicios de firma servidor Co y Counter, aquellos formatos de firma en los que no está permitido su uso. Se indica en el servicio de firma servidor, que no se permite la generación de firmas con formato PAdES.

Rev.	040
Fecha	13/05/2013
Descripción	Se corrige una errata en la respuesta de validación de firmas para el perfil DSS. Corrección: Si dos firmantes firman un mismo contenido se repetirá el contenido de los elementos *afxp:DataInfo***.** Antes de la corrección se indicaba que solo aparecería un *afxp:DataInfo* compartido en el caso de que dos firmantes firmaran lo mismo (cofirmas). Se corrige un errata en los valores posibles de las peticiones de actualización de firmas. Corrección: El servicio de actualización de firmas solo permite actualizar el formato y no la versión de la firma original. Antes de la corrección se indicaba que se podia especificar la versión de la firma actualizada.

Rev.	041
Fecha	22/05/2013
Descripción	Se añade un nuevo elemento en el apartado “Identificadores de resultado del proceso” para indicar que uno de los sellos de tiempo está emitido por la misma TSA que otro de los sellos de tiempo de la misma firma: urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:Repeated Se añade un nuevo elemento en el apartado “Identificadores de tareas de validación” para indicar que existe un sello de tiempo emitido por la misma TSA que otro de los sellos de tiempo de la misma firma: SignatureTimeStamp:code:RepeatedTSA

Rev.	042
Fecha	29/05/2013
Descripción	Se elimina la descripción de la lista de servicios disponibles la correspondiete a ArchiveSubmit, la cual por error se seguía manteniendo a pesar de no encontrarse disponible el servicio.

Rev.	043
Fecha	31/05/2013
Descripción	Se añade una aclaración en el apartado 0

Rev.	044
Fecha	03/06/2013
Descripción	Se modifica el apartado 8.2 corrigiendo en la tabla de actualización de firmas origen a XAdES-T las actualizaciones desde firmas XMLDSIG. Se modifican los apartados 8.2.1.1.2 y 8.2.1.1.6 para indicar que las firmas enveloping tambien se pueden validar en base64. Se modifica el apartado 8.1.1.2.5 de manera que ahora no se mencionan los modos 'enveloped o detached' ya que el elemento se puede aplicar a todas las firmas XML/XAdES

Rev.	045
Fecha	14/10/2014
Descripción	Se incluye aclaraciones sobre el comportamiento del servicio de actualización de firma en base a la inclusión o no del firmante objetivo (apartado 8.2.2.1.6)

Rev.	046
Fecha	15/12/2014
Descripción	Se añade el identificador para el resultado de la validación del nivel de certificación de todos los diccionarios de firma contenidos en un documento PDF, así como la información asociada a su ResultMinor y DetailType.

Rev.	047
Fecha	05/05/2015
Descripción	Se elimina cualquier referencia a personas y empresas. Se añade la información de los nuevos elementos que pueden incluirse como información adicional en la respuesta del servicio de validación de firmas DSS, esto es, SignerRole, SigningTime y CommitmentTypeIndication.

Rev.	048
Fecha	15/12/2015
Descripción	Se modifican los puntos 8.1.1.1 Se añade la posibilidad de enviar el hash del documento a firmar en lugar del documento. 8.1.2.1 Se añade la posibilidad de enviar la firma a co-firmar en la petición. 8.1.3.1 Se añade la posibilidad de enviar la firma a contra-firmar en la petición. Se añaden nuevos ejemplos que ilustran las modificaciones.

Rev.	049
Fecha	12/01/2016
Descripción	Se añade toda la información asociada a la capacidad de la plataforma para generar, validar y actualizar los formatos de firma CAdES Baseline, PAdES Baseline y XAdES Baseline en sus formas B-Level, T-Level, LT-Level y LTA-Level. Igualmente, se añade toda la información asociada a la capacidad de la plataforma para validar y actualizar firmas ASiC-S. Se elimina el formato de firma ODF-T pues no está soportado. Se elimina la información relativa a la tarea de validación de la cadena de certificación para firmas PAdES, ya que dicha tarea ha pasado a englobarse en la tarea de validación del certificado firmante.

Rev.	050
Fecha	01/08/2016
Descripción	Se modifica la orientación de las páginas asociadas al punto A.3.7. Se añade una explicación en el punto 8.2 indicando que la actualización de firmas XAdES con versiones inferiores a v1.3.2 sólo permite como formato máximo XAdES-T.

Rev.	051
Fecha	03/08/2016
Descripción	Adaptación a plantillas de documentos.

Rev.	052
Fecha	04/08/2016
Descripción	Se añade un comentario el punto A.3.3 (Formatos soportados por el Sistema) indicando que el formato PKCS#7 se encuentra obsoleto para procesos de generación de firma. Se añade un comentario en el punto 8.3 (Servicio de Validación de Certificados) indicando que el servicio de validación de certificados valida también los certificados de CA's intermedias como raíces.

Rev.	053
Fecha	07/10/2016
Descripción	Se incluye el nuevo tipo de ResultMinor urn:afirma:dss:1.0:profile:XSS:resultminor:UnnecessaryUpgradeOperation para los casos de ResultMajor de tipo urn:oasis:names:tc:dss:1.0:resultmajor:Warning. Se añade un anexo para aclarar las posibles respuestas de la plataforma en procesos de actualización/generación de firma.

Rev.	054
Fecha	20/01/2017
Descripción	Se incluye una aclaración en el punto 8.2 acerca de que es posible actualizar firmas XAdES v1.2.2 hasta formato -A.

Rev.	055
Fecha	27/04/2017
Descripción	Se incluye una aclaración en el punto 8.1.2 indicando que no se permite la co-firma de firmas CAdES LTA-Level.

Rev.	056
Fecha	02/01/2018
Descripción	Se incluye el anexo A.6 en el que se informa de la necesidad de revisar la Guía 807 del Esquema Nacional de Seguridad.

Rev.	057
Fecha	25/01/2018
Descripción	Se añade el comentario “Este servicio solo está disponible en el modelo federado” en el servicio DSSAfirmaArchiveRetrieval.

Rev.	058
Fecha	26/03/2018
Descripción	Se corrige la nota que indica en el servicio de validación de certificados los mapeos mínimos que se devuelven al reconocer un certificado frente a una TSL en vez de contra la política de validación de la plataforma.

Rev.	059
Fecha	09/05/2018
Descripción	Se modifican los apartados 8.2.1.1.6, 8.2.1.1.7 y 8.2.1.1.20 , para indicar el comportamiento en caso de firmas PAdES.

Rev.	060
Fecha	22/08/2018
Descripción	Se modifica el apartado 8.1.1.2.5 para dejar claro que el atributo WichDocument del elemento SignaturePtr es obligatorio.

Rev.	061
Fecha	14/11/2019
Descripción	Se añaden los apartados 8.2.1.1.21, 8.2.1.1.22, 8.2.1.2.6 y 8.2.2.1.9. Además, se actualizan los apartados 8.2.1.1, 8.2.1.2 y 8.2.2.1.

Índice

1 Objeto

El objeto de este documento es definir los perfiles que se utilizarán para adaptar los servicios de la plataforma @firma 6 a las especificaciones definidas por la organización OASIS para los servicios de firma electrónica DSS.

2 Alcance

La información contenida en el presente documento abarca los siguientes puntos:

- Definición del perfiles XSS y Archive de @Firma, tanto la definición de los nuevos componentes definidos como su relación con las implementaciones DSS definidas por OASIS
- Descripción de la implementación de los anteriores perfiles en los Servicios de la Plataforma.

3 Siglas

OASIS	Organization for the Advancement of Structured Information Standards
XML	eXtensible Markup Language
SOAP	Simple Object Access Protocol
DSS	Digital Signature Services
CMS	Cryptographic Message Syntax
CAdES	CMS Advanced Electronic Signatures
CAdES-BES	CAdES - Basic Electronic Signature
CAdES-EPES	CAdES - Explicit Policy-based Electronic Signatures
CAdES-T	CAdES with Timestamp

CAdES-C	CAdES with complete validation data references
CAdES-X	CAdES - eXtended signature with time indication
CAdES-XL	CAdES - extended long signature with time indication
CAdES-A	CAdES - Archival electronic signature
XMLDSignature	XML Digital Signature
XAdES	XML Advanced Electronic Signatures
XAdES-BES	XAdES - Basic Electronical Signature
XAdES-EPES	XAdES - Explicit Policy Electronical Signature
XAdES-T	XAdES with Timestamp
XAdES-C	XAdES with complete validation data references
XAdES-X	XAdES - eXtended signature with time indication
XAdES-XL	XAdES - extended long signature with time indication
XAdES-A	XAdES - Archival electronic signature
PDF	Portable Document Format
PAdES	PDF Advanced Electronic Signatures
PAdES-BES	PAdES - Basic Electronical Signature
PAdES-EPES	PAdES - Explicit Policy Electronical Signature
PAdES-LTV	PAdES - Long Term Validation
ODF	Open Document Format
XSS	eXtended Signature Services

TSA	Time Stamping Authority
TST	Time-Stamp Token
CATCert	Agencia Catalana de Certificación
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
RFC	Request For Comments
URN	Uniform Resource Name
OID	Object Identifier
CA	Certificate Authority
MD	Message-Digest
SHA	Secure Hash Algorithm
ASN.1	Abstract Syntax Notation One
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
OOXML	Office Open XML
ASiC	Associated Signature Containers
ASiC-S	Associated Signature Containers Simple
CAdES B-Level	CMS Advanced Electronic Signatures Basic Level
CAdES T-Level	CMS Advanced Electronic Signatures Trusted Time for Signature Existence
CAdES LT-Level	CMS Advanced Electronic Signatures Long Term Level

CAdES LTA-Level	CMS Advanced Electronic Signatures Long Term with Archive Time-stamps
XAdES B-Level	XML Advanced Electronic Signatures Basic Level
XAdES T-Level	XML Advanced Electronic Signatures Trusted Time for Signature Existence
XAdES LT-Level	XML Advanced Electronic Signatures Long Term Level
XAdES LTA-Level	XML Advanced Electronic Signatures Long Term with Archive Time-stamps
PAdES B-Level	PDF Advanced Electronic Signatures Basic Level
PAdES T-Level	PDF Advanced Electronic Signatures Trusted Time for Signature Existence
PAdES LT-Level	PDF Advanced Electronic Signatures Long Term Level
PAdES LTA-Level	PDF Advanced Electronic Signatures Long Term with Archive Time-stamps

4 Documentos de Referencia

[DDS Core] oasis-dss-core-spec-v1.0-os - Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0. 11 April 2007.

[DSS XSS] oasis-dss-1.0-core-profiles-XSS-spec-wd07 – eXtended Signature Services (XSS) Profile of the OASIS Digital Signature Service (DSS). Working Draf 07, 24 Marzo 2006.

[XMLDSIG] XML-Signature Syntax and Processing. W3C Recommendation, February 2002. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[DSS Archive] oasis-dss-1.0-profiles-archive-spec-wd01 - Signature Archive Profile of the OASIS Digital Signature Service. Working Draft 01, 27 December 2005

[DSS AdES] oasis-dss-1.0-profiles-AdES-spec-v1.0-os – Advance Electronic Signature Profile of the OASIS Digital Signature Service. Version 1.0 , 11 April 2007

[DSS APAP] oasis-dss-profiles-asynchronous_processing-spec-v1.0-os Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services Version 1.0 11 April 2007

[DSS SIGPOL] oasis-dssx-1.0-profiles-sigpolicy. Signature Policy Profile of the OASIS Digital Signature Services Version 1.0, Committee Draft 01, 18 May 2009

[SAMLCore1.1] oasis-sstc-saml-core-1.1 - E. Maler et al. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V 1.1. OASIS, November 2002.

[DSS VR] oasis-dss-profile-for-comprehensive-signature-verification-report -v1.0-os - Profile for comprehensive mulTGS-signature verification reports for OASIS Digital Signature Services Version 1.0. OASIS Working Draft, 5 Mayo 2008

[RFC3161] http://www.ietf.org/rfc/rfc3161.txt. - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF RFC 3161, Agosto 2001.

[CAdES] ETSI TS 101 733 V1.7.3 - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). Enero 2007

[XAdES]	ETSI TS 101 903 V1.3.2 - XML Advanced Electronic Signatures (XAdES). Marzo 2006
[OASIS CMIS]	Content Management Interoperability Services (CMIS) Version 1.0 Committee Draft 04 23 September 2009
[PAdES-1]	ETSI TS 102 778-1 V1.1.1 (2009-07) - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES
[PAdES-2]	ETSI TS 102 778-2 V1.2.1 (2009-07) - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1
[PAdES-3]	ETSI TS 102 778-3 V1.1.2 (2009-12) - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles
[PAdES-4]	ETSI TS 102 778-4 V1.1.2 (2009-12) - Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile
[CAdES-2.2.1]	ETSI TS 101 733 V2.2.1 (2013-04) / Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
[PAdES_Baseline]	ETSI TS 103 172 V2.1.1 (2012-03) / Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
[ASiC_Baseline]	ETSI TS 103 174 V2.1.1 (2012-03) / Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile
[CAdES_Baseline]	ETSI TS 103 173 V2.2.1 (2013-04) / Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile
[ASiC]	ETSI TS 102 918 V1.3.1 (2013-06) / Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
[XAdES_Baseline]	103 171 V2.1.1 (2012-03) / Electronic Signatures and Infrastructures (ESI);

XAdES Baseline Profile

5 Introducción

El estándar Digital Signature Service de OASIS define protocolos de firma, verificación y custodia basados en interfaces XML. Las especificaciones DSS se encuentran en continuo desarrollo y definen multitud de casos de uso, agrupados por perfiles, para distintos contextos. Utilizando estas interfaces un cliente puede interactuar con cualquier servidor que cumpla con los perfiles definidos.

No obstante, aunque los perfiles DSS se encuentran en un estado de madurez óptimo, no existe uno que se adapte al cien por cien a los servicios que ofrece actualmente la plataforma @firma 5. Por este motivo, se hace necesaria la definición de nuevos perfiles basados en algunos ya definidos por OASIS a los que se le añaden elementos nuevos para recoger aquellos aspectos no contemplados en el estándar.

Los perfiles DSS en los que se basa este documento se refieren a "Extended Signature Services (XSS)" según las especificaciones [DSS XSS] para los servicios de firma, verificación de firma , y "Signature Archive Profile" con las características recogidas en [DSS Archive] para los servicios de custodia. Estos perfiles han sido definidos e implementados por CATCERT y están disponibles en:

- En el entorno de Desarrollo en la url:

  https://des-afirma.redsara.es/afirmaws/xsd/dss/oasis-dss-1.0-profiles-XSS-schema-wd02.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/dss/oasis-dss-1.0-profiles-XSS-schema-wd02.xsd

Además de los perfiles anteriormente expuestos, las especificaciones XSS de @firma se basa en el perfil "Comprehensive MulTGS-Signature Verification Reports" recogido en [DSS VR] y disponible en la Web (http://www.oasis-open.org/committees/download.php/28182/2008_05_05_oasis-dss-profile-for-comprehensive-signature-verification-report.doc) para solventar las limitaciones del protocolo de verificación en los procesos de verificación de multifirmas.

En los siguientes apartados definiremos aquellos elementos que incluiremos a los perfiles anteriores. El conjunto de estos elementos formaran los nuevos perfiles de aplicación para la plataforma @firma.

6 Namespaces

El esquema que siguen los elementos definidos en esta implementación DSS tiene asociado los siguientes namespaces:

- Profile XSS @Firma -> urn:afirma:dss:1.0:profile:XSS:schema
- Profile Archive @Firma -> urn:afirma:dss:1.0:profile:archive:schema

Los prefijos utilizados en están implementación están asociados a los siguientes namespace:

- dss: namespace del “Core DSS” [DDS Core]
- ds: namespace del W3C XML-Signature [XMLDSIG]
- xss: namespace del perfil XSS de OASIS [DSS XSS]
- ades: namespace del perfil AdES de OASIS [DSS AdES]
- saml: namespace de las especificaciones SAML de OASIS [SAMLCore1.1]
- vr: namespace de las especificaciones VR de OASIS [DSS VR]
- afxp: namespace del perfil XSS de @Firma
- afap: namespace del perfil Archive de @Firma
- sigpol: namespace del perfil Signature Policy de OASIS [DSS SIGPOL]
- async: namespace del perfil Asynchronous Processing de OASIS [DSS APAP]
- cmism: namespace del CMIS (Content Management Interoperability Services tal como se define en [OASIS CMIS]) Messaging
- asic: namespace del estándar para firmas de tipo Associated Signature Containers [ASiC]

7 Identificadores del perfil

Un perfil DSS se identifica mediante un identificador único, el cual se recomienda sea incluido en el mensaje de petición y es obligatorio incluirlos en los de respuesta. Este identificador permitirá que tanto cliente como servidor tengan identificado la implementación DSS con la que estan interactuando. Para los perfiles de @Firma se definen las siguientes URI's

- Identificador del perfil XSS de @Firma es **urn:afirma:dss:1.0:profile:XSS**
- Identificador del perfil Archive de @Firma es **urn:afirma:dss:1.0:profile:archive**

8 Servicios DSS de @Firma

En este apartado se detallan los Servicios Web que publica la plataforma @Firma siguiendo las recomendaciones Digital Signature Service de OASIS, estos servicios son:

- ***DSSAfirmaSign*.** Servicio de Firma Delegada que permite la realización de operaciones de firma y multifirma de servidor en los formatos soportados por la plataforma.

- ***DSSAfirmaVerify*.** Servicio de Verificación y Actualización de Firma. Permite la verificación de una firma electrónica y la obtención de información adicional sobre dicha firma. El servicio de verificación permitirá además, de forma opcional, la realización de operaciones de upgrade sobre una firma electrónica, pudiendo completar dicha firma a un formato más avanzado.

- ***DSSAfirmaArchiveRetrieval.*** Servicio de Obtención de Firmas Registradas. Este servicio permite la recuperación de una firma registrada en la plataforma a partir de un identificador único de registro siguiendo las recomendaciones del perfil Archive de OASIS. **Este servicio solo está disponible en el modelo federado**.

- ***DSSAfirmaVerifyCertificate.*** Servicio de Verificación de Certificado. Mediante esta interfaz Web Service se puede solicitar la verificación de certificados X509 así como extraer la información del certificado mediante la aplicación del mapeo definido para su tipo.

- ***DSSBatchVerifyCertificate.*** Servicio de Validación Masiva de Certificados. Mediante este servicio se puede solicitar la verificación asíncrona de un conjunto de certificados.

- ***DSSBatchVerifySignature.*** Servicio de Validación Masiva de Firmas. Mediante este servicio se puede solicitar la verificación asíncrona de un conjunto de firmas.

- ***DSSAsyncRequestStatus.*** Servicio de Consulta de Peticiones Asíncrona. Este servicio permite la consulta y obtención de respuesta de peticiones asíncronas.

En los siguientes apartados se describirán los componentes que forman las interfaces XML de petición y respuesta para cada uno de los anteriores servicios.

8.1 Servicio de Firma Delegada

El Servicio de Firma Delegada (DSSAfirmaSign) permite la generación de firmas y multifirmas de servidor mediante un certificado alojado en la plataforma, en este caso el cliente delega el proceso de firma a la plataforma. La implementación de este servicio se ha realizado a partir del perfil XSS de @Firma.

OASIS en sus especificaciones para servicio de firma digital (DSS) define diferentes elementos para soportar las peticiones de generación de firmas y las respuestas del proceso. Estos elementos son:

- ***dss:SignRequest***: Elemento XML de petición de firma.
- ***dss:SignResponse***: Elemento XML de respuesta de firma.

La definición de estos elementos se encuentra en el core DSS [DDS Core], así como en los diferentes perfiles soportados, tal y como se detalla en el apartado 0.

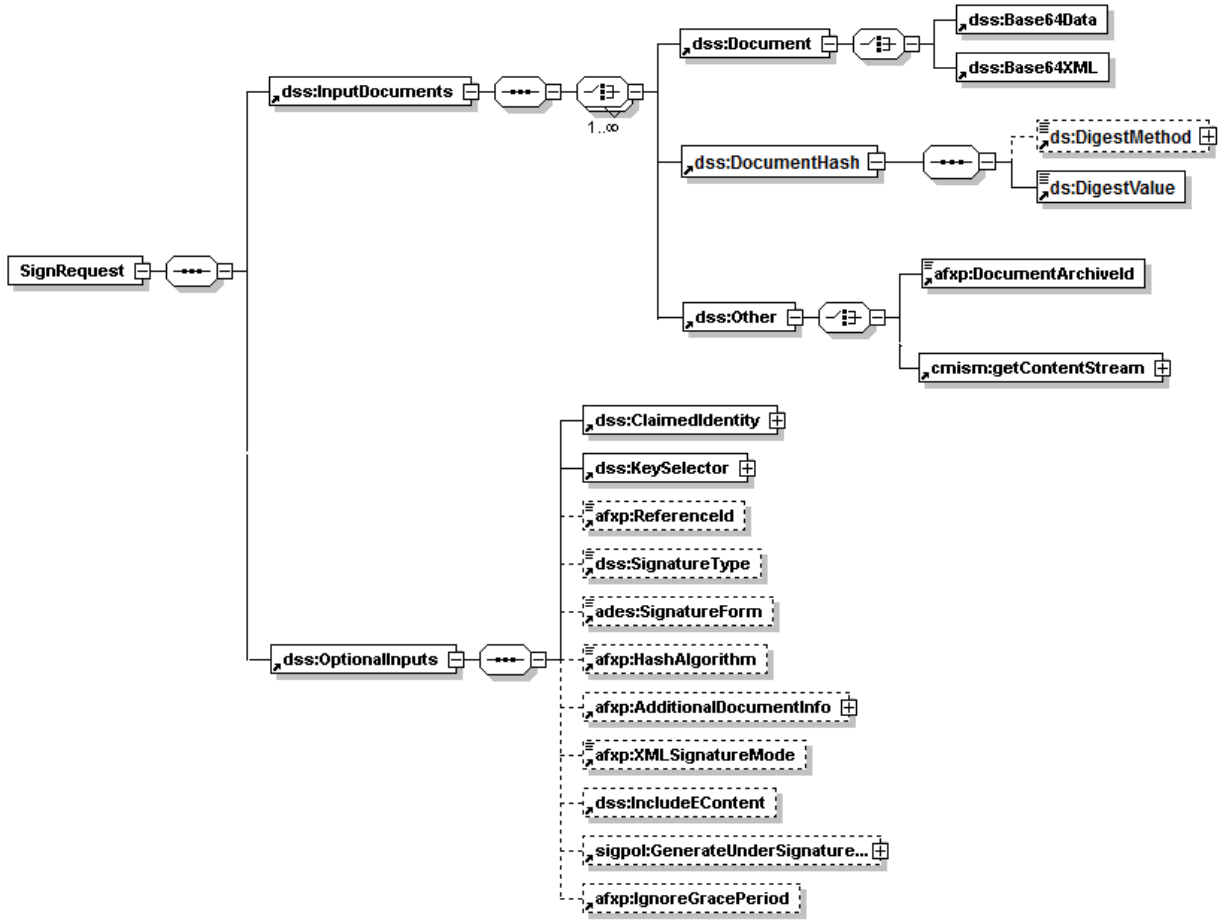
A continuación se detalla la definición de dichos elementos.

8.1.1 Firma Servidor Simple

El proceso de firma servidor consiste en la realización de una firma con un certificado dado de alta en la plataforma sobre unos datos que previamente fueron registrados o se incluyen en la petición.

8.1.1.1 Mensaje XML de Petición.

En la siguiente figura podemos observar los distintos componentes que pueden formar una petición de Firma de Servidor.



Como se observa en la anterior figura la petición de firma *dss:SignRequest* esta compuesta por dos elementos diferenciados:

- *dss:InputDocument.* Elemento que recoger el documento a ser firmado, una referencia al mismo, o su hash calculado. La información de los datos a ser firmados puede incluirse de las siguientes formas:
    - Incluyendo el documento en un elemento *dss:Base64XML* (documento XML) o *dss:Base64Data* (otro tipo de documento)
    - Mediante el identificador de documento de @firma incluido en el componente *afxp:DocumentArchiveId*

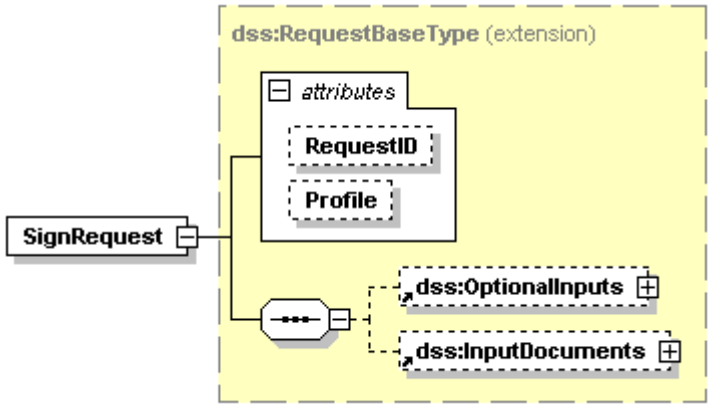
- Incluyendo, en un componente *cmism:getContentStream*, la localización del documento en un gestor documental o repositorio externo

- Incluyendo un hash calculado del documento a firmar en un componente *dss:DocumentHash* insertando el método con el cual se calcula el hash en *ds:DigestMethod* y el hash calculado en *ds:DigestValue*.

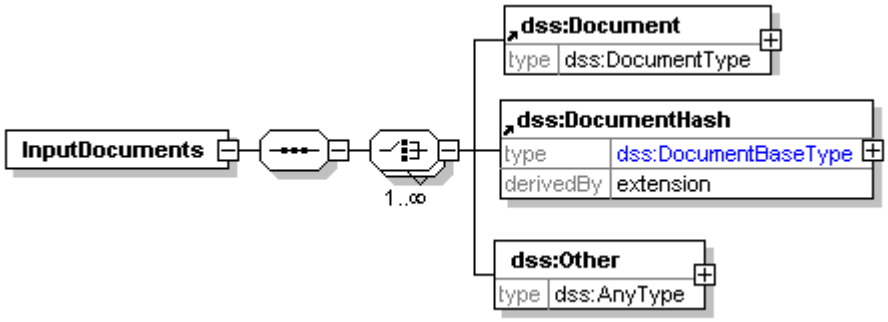
- *dss:OptionalInput.* Elemento que incluye la información necesaria para que el servidor pueda realizar la firma de los datos pasados en el anterior componente, para esta implementación del perfil los paramétros obligatorio son el identificador de aplicación (contenido en el componente *dss:ClaimedIdentity*) y alias del certificado de servidor (incluido en el elemento *dss:KeySelector*). Adicionalmente este componente permite incluir parámetros adicionales como puede ser el algoritmo de hash, el formato de firma, etc.

Los elementos que conformaran una petición de firma de servidor vendrán determinados por diversos factores (naturaleza de los datos a ser firmados, el formato de la firma…), a continuación se detalla cada elemento.

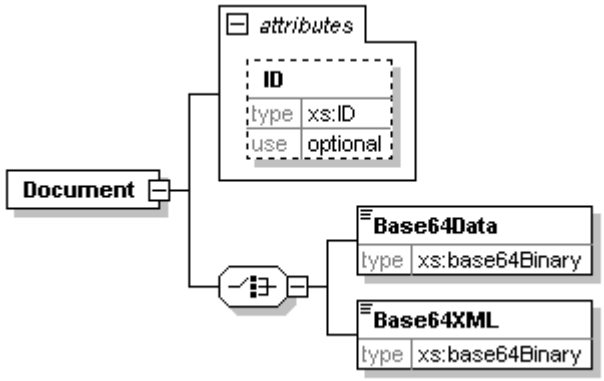
8.1.1.1.1 <dss:SignRequest>

SignRequest		
Diagrama		
Descripción	Componente introducido en las especificaciones [DDS Core] y que constituye el elemento raíz de una petición de generación de firma.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *OptionalInputs.* Este componente se describe en el apartado 8.1.1.1.7 • *InputDocuments.* Este componente se describe en el apartado 8.1.1.1.2	
Atributos	Nombre	Descripción
	Profile	Identificador del perfil soportado por el servicio. Para peticiones de firma delegada (firma de servidor) a la plataforma, el valor de este atributo será: **urn:afirma:dss:1.0:profile:XSS**, esta URI identifica al perfil *XSS* de @Firma.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma. Si la aplicación cliente incluye este atributo, la respuesta generada por el servidor incluirá de igual manera un atributo con el mismo valor en el elemento *SignResponse*.

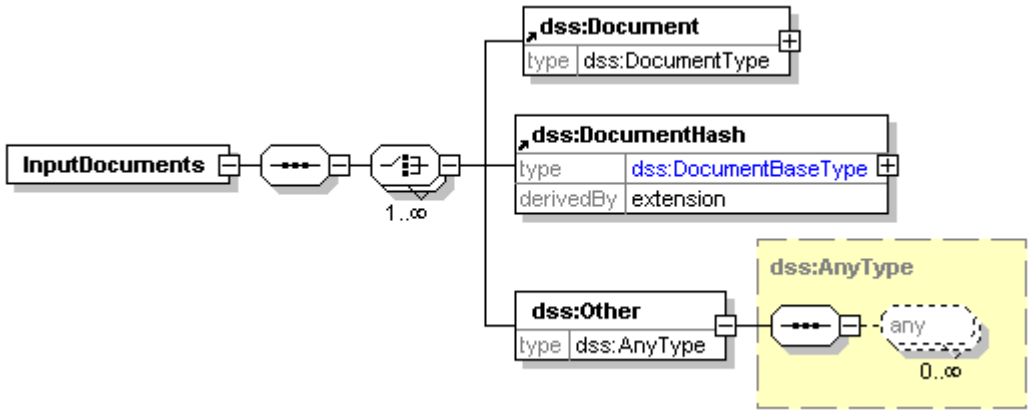
8.1.1.1.2 <dss:InputDocuments>

InputDocuments	
Diagrama	
Descripción	Este elemento contendrá el documento o datos que van a ser firmados/multifirmados (para el servicio de firma delegada) o bien aquellos que desean sean verificados (para el servicio de validación de firma).
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:Document*. Este documento se describe en el apartado 0 • *dss:DocumentHash.* Este documento se describe en el apartado 8.2.1.1.7. • *dss:Other.* Este documento se describe en el apartado 8.1.1.1.4

8.1.1.1.3 <dss:Document>

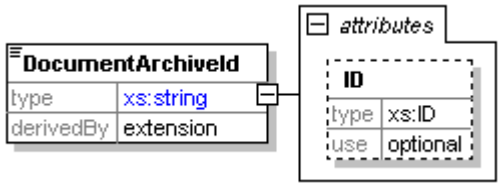
Document		
Diagrama		
Descripción	Si la operación a realizar es de generación de firma, este elemento contendrá los datos a firmar. En el caso de que el proceso sea de verificación, los datos corresponderán a los originalmente firmados para su verificación.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	Base64Data	Elemento que contiene los datos a firmar o verificar siempre que el formato del contenido no sea XML. El contenido debe estar codificado en Base64
	Base64XML	Elemento que contiene los datos a firmar o verificar cuando estos tienen formato XML. El contenido debe estar codificado en Base64
Atributos	Nombre	Descripción
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

8.1.1.1.4 <dss:InputDocuments>/<dss:Other>

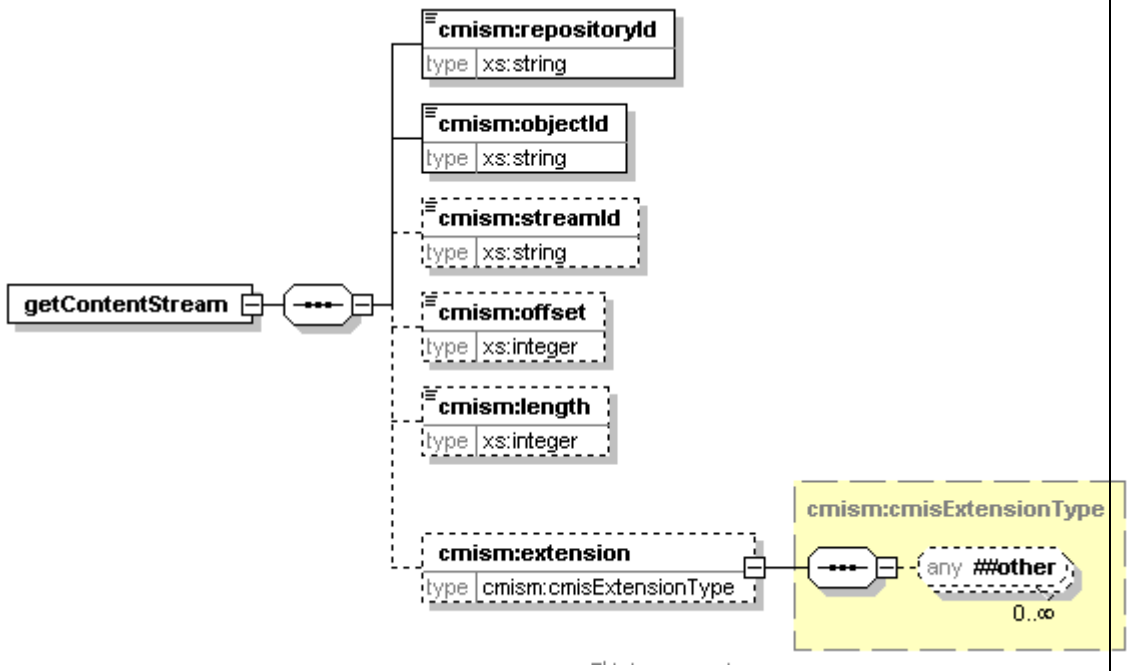
InputDocuments / Other	
Diagrama	
Descripción	El componente Other definido por OASIS esta destinado a soportar otras implementaciones futuras no recogidas en las especificaciones del Core [DSS Core]. La definición actual del perfil permite la utilización del elemento InputDocuments/Other: ▪ Permitir la inclusión del identificador del documento a firmar (que previamente debe haber sido custodiado). El elemento a incluir para esto será: *afxp:DocumentArchiveId* (Este componente se decribe en el apartado 8.1.1.1.5) ▪ Contener un elemento *cmism:getContentStream* con la localización de un documento en un gestor documental. (Este componente se describe en el apartado 0)
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

8.1.1.1.5 <afxp:DocumentArchiveId>

DocumentArchiveId

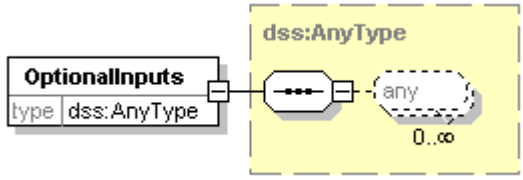
DocumentArchiveId		
Diagrama		
Descripción	Si el documento a firmar ya se encuentra custodiado este elemento deberá contener el identificador de documento. En procesos de multifirma este componente contendría el identificador de transacción de la firma origen.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Atributos	Nombre	Descripción
	ID	Identificador único que permite la identificación unívoca del elemento para su posterior referencia desde otros elementos incluidos en el mensaje XML.

8.1.1.1.6 <cmism:getContentStream>

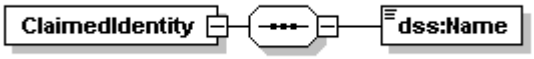
getContentStream		
Diagrama		
Descripción	Elemento definido en las especificaciones [OASIS CMIS] para obtener el contenido de un elemento localizado en un repositorio o gestor documental. Este perfil soporta su utilización para informar al servidor que debe obtener el contenido de un objeto (documento, firmas o certificado) almacenado en un gestor documental para realizar la operación asociada al servicio.	
Namespace	http://docs.oasis-open.org/ns/cmis/messaging/200908/	
Hijos	Nombre	Descripción
	repositoryId	Identificador del repositorio o gestor documental que aloja el objeto que se desea recuperar. Este elemento debe incluir el identificador con el que se ha dado de alta el gestor documental en la plataforma

getContentStream		
	objectId	Identificador único (UUID) del objeto del que se quiere obtener el contenido.
	streamId	Identificador del contenido concreto que debe recuperarse, por ejemplo en el caso que el objectId referecie a una carpeta o directorio es necesario indicar el "ContentStream" concreto que se desea recuperar. Actualmente este elemento no está soportado por la plataforma aunque no se descarta su utilización en futuras versiones.
	offset	Offset del conjunto de "bytes" que se desea recuperar. Actualmente este elemento no está soportado por la plataforma aunque no se descarta su utilización en futuras versiones.
	length	Longitud del conjunto de "bytes" que se desea recuperar Actualmente este elemento no está soportado por la plataforma aunque no se descarta su utilización en futuras versiones.
	extension	Elemento destinado a recoger elementos adicionales a la especificación [OASIS CMIS]. Esta implementación no añade ningún componente para este elemento. Actualmente este elemento no está soportado por la plataforma aunque no se descarta su utilización en futuras versiones.

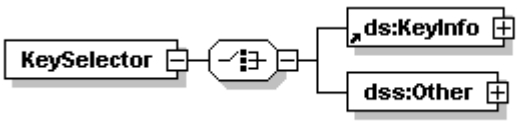
8.1.1.1.7 <dss:OptionalInputs>

OptionalInputs	
Diagrama	
Descripción	Contiene parámetros adicionales de la petición definidos en [DSS Core] u otros perfiles o implementaciones DSS. Los elementos que puede contener OptionalInputs dependen del contexto en el que se encuentre incluido. Por favor, consulte los esquemas específicos para cada servicio para obtener más información acerca de qué elementos puede contener en cada contexto: 8.1.1.1 Generación de Firma Simple de Servidor 8.1.2.1 Generacion de Firmas CoSign 8.1.3.1 Generacion de Firmas CounterSign 8.2.1.1 Verificación de Firmas 8.2.2.1 Upgrade de Firmas 8.3.1.1 Validación de Certificados 8.4.1.1 Validaciones en Lotes 8.5.1.1 Consulta de Peticiones Asíncronas 8.6.1.1 Obtención de Firma mediante Identificador de Transacción
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.1.1.1.8 <dss:ClaimedIdentity>

ClaimedIdentity		
Diagrama		
Descripción	Permite identificar a la aplicación cliente que realiza la petición, por medio de la inclusión del identificador de aplicación establecido en el proceso de alta de la misma en el sistema. Su inclusión es obligatoria debido a que la política de seguridad del sistema exige que la aplicación que realiza la petición se identifique previamente al uso del servicio.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	Name	Incluiría la identidad del cliente en nuestro caso el identificador de aplicación que realizó la petición.

8.1.1.1.9 <dss:KeySelector >

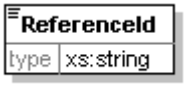
KeySelector		
Diagrama		
Descripción	Contiene el identificador de la clave a utilizar para la generación de una firma delegada. Es un elemento obligatorio para todos los procesos de firma delegada.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	ds:KeyInfo	Incluirá la información de la clave a utilizar siguiendo las especificaciones XML Signature Syntax and Processing. Este elemento

KeySelector		
		se describe en el apartado 8.1.1.1.10
	Other	Elemento definido para albergar otras implementaciones. No tiene uso en el perfil actual.

8.1.1.1.10 <ds:KeyInfo>

KeyInfo		
Diagrama		
Descripción	Contiene información sobre las claves que participan en una firma. En la especificación XML Signature un componente *ds:KeyInfo* puede incluir información muy diversa (claves, alias, certificados…) pero en la implementación actual del perfil, se restringirá su uso a la utilización del elemento *ds:KeyName*.	
Namespace	http://www.w3.org/2000/09/xmldsig#"	
Hijos	Nombre	Descripción
	ds:KeyName	El identificador de la clave con la que se desea generar la firma. Este identificador deberá se especificado por los Administradores de la plataforma tras su alta en el sistema.

8.1.1.1.11 <afxp:ReferenceId>

ReferenceId	
Diagrama	
Descripción	Este elemento es opcional, y puede contener una referencia o identificador externo generado por la aplicación cliente, de manera que puede ser utilizado como manera

ReferenceId	
	alternativa de identificar una transacción. En los servicios de generación de firmas, este identificador será asociado a la transacción de firma. En los servicios de consulta, permitirá especificar la transacción concreta a recuperar.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.1.1.1.12 <dss:SignatureType>

SignatureType	
Diagrama	
Descripción	Permite especificar un formato concreto de firma mediante una URI. En el anexo A.3.1 se detallan las URI aceptadas en la versión actual del perfil. En concreto, para esta operación, no se admite el formato PAdES.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

8.1.1.1.13 <ades:SignatureForm>

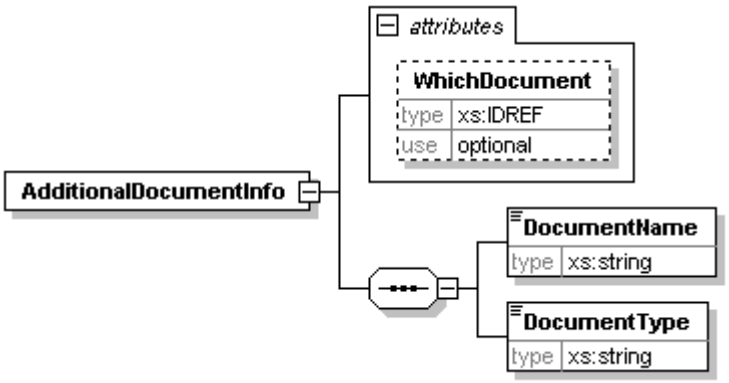
SignatureForm	
Diagrama	
Descripción	Especifica el modo de la firma, en relación a los formatos extendidos de firma. Este elemento complementa a *dss:SignatureType* especificando el formato de firma avanzado. En el anexo A.3.2 se detallan los valores que pueden incluirse en dicho elemento.

SignatureForm	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#

8.1.1.1.14 <afxp:HashAlgorithm>

HashAlgorithm	
Diagrama	
Descripción	Elemento opcional que indica el algoritmo de hash a emplear en el cálculo de la firma. En el anexo A.3.4 se especifican los algoritmos de hash soportados.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.1.1.1.15 <afxp:AdditionalDocumentInfo>

AdditionalDocumentInfo		
Diagrama		
Descripción	Contiene información adicional sobre el documento. Únicamente deberá incluirse en la petición, si está presente también el elemento Document, que incluye el documento original a firmar/firmado.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción

AdditionalDocumentInfo		
	DocumentName	Nombre del documento
	DocumentType	Tipo del documento a custodiar. Se recomienda incluir en este campo, bien el mime/type del documento referenciado, bien la extensión del fichero.
Atributos	Nombre	Descripción
	WichDocument	Atributo opcional que identificaría por referencia el documento al que pertenece la información adicional.

8.1.1.1.16 <afxp:XMLSignatureMode>

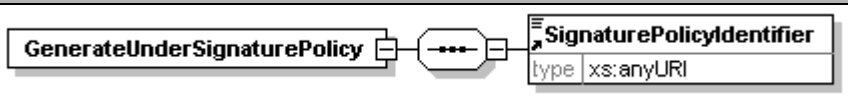
XMLSignatureMode	
Diagrama	
Descripción	En el caso que la firma a generar pertenezca a algunos de los formatos de la familia de firmas en XML (XMLDSig, XAdES), el cliente puede incluir el elemento "XMLSignatureMode" para determinar el modo de la firma a generar. Los valores admitidos son: 1. **Enveloping**. El servidor incluirá los datos a firmar dentro del elemento *ds:Object* de la firma generada. Para realizar este tipo de firma el valor de este componente debe ser **urn:afirma:dss:1.0:profile:XSS:XMLSignatureMode:EnvelopingMode** 2. **Enveloped**. El servidor firmaría los datos e introduciría la firma como hijo. Puede darse el caso que los datos a firmar no fuera un XML , en estos casos el servidor podría generar una envoltura XML propia que contuviera los datos a firmar, firmaría dicha estructura e incluiría la firma como hijo. Para la generación de una firma enveloped se debe incluir la URI

XMLSignatureMode	
	urn:afirma:dss:1.0:profile:XSS:XMLSignatureMode:EnvelopedMode 3. **Detached** (modo por defecto). Al igual que el modo anterior los datos a firmar se encuentran fuera de la estructura de firma generada pero no se firmaría todo el nodo padre del elemento *ds:Signature*, para realizar una firma detached se debe añadir la URI **urn:afirma:dss:1.0:profile:XSS:XMLSignatureMode:DetachedMode**
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.1.1.1.17 <dss:IncludeEContent>

IncludeEContent	
Diagrama	
Descripción	Este elemento se utiliza en formatos de firma ASN.1 (CMS y CAdES) para indicar que el modo de generación de la firma sea implícito (el documento se incluye dentro de la firma).
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

8.1.1.1.18 <sigpol:GenerateUnderSignaturePolicy>

GenerateUnderSignaturePolicy	
Diagrama	
Descripción	Este componente, siguiendo las especificaciones [DSS SIGPOL], indica la política de firma bajo la cual el servidor debe generar la firma. Actualmente la plataforma sólo contempla las políticas de la AGE y Facturae.

GenerateUnderSignaturePolicy		
Namespace	urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#	
Hijos	Nombre	Descripción
	SignaturePolicyIdentifier	Elemento que contienen el identificador de la política de firma como URI. Las políticas de firmas pueden ser identificadas mediante URI u OID, en el caso de querer especificar una política cuyo identificador sea un OID este componente contendrá una URN construida con el valor del OID tal como se especifica en la RFC 3001. Por ejemplo: OID → 1.3.6.1.4.1.14862.1.6.2.1.2 URN → urn:oid:1.3.6.1.4.1.14862.1.6.2.1.2

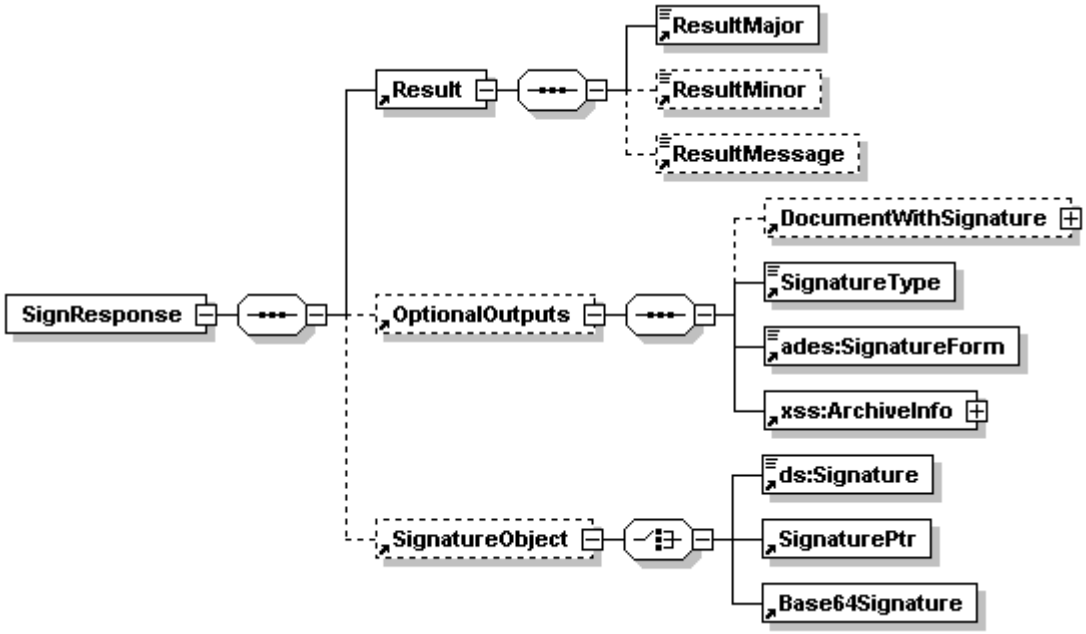
8.1.1.1.19 <afxp:IgnoreGracePeriod>

IgnoreGracePeriod	
Diagrama	
Descripción	Este elemento incluido en la petición informa al servidor que no se desea guardar un posible periodo de gracia.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.1.1.2 Mensaje XML de Respuesta

Dependiendo si el proceso de firma ha finalizado o sí por el contrario hay que aplicar un periodo de gracia el contenido de la respuesta DSS puede variar.

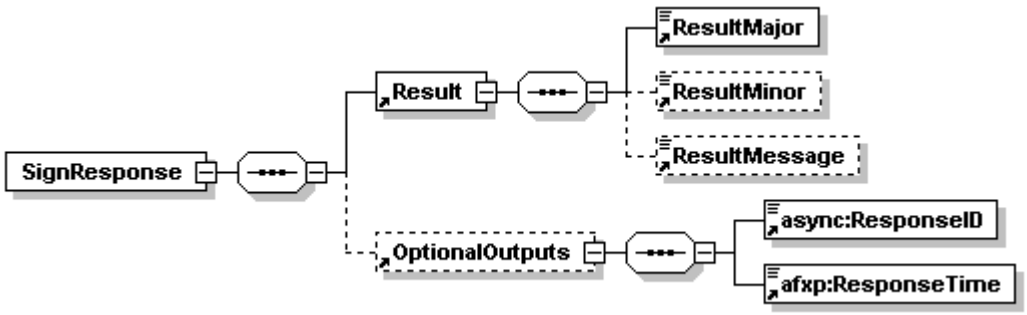
a) *Respuesta sin Periodo de Gracia.* En la siguiente figura podemos observar los distintos componentes que forman una respuesta de Firma de Servidor en la que no se aplica periodo de gracia.



El mensaje de respuesta, *dss:SignRequest*, esta compuesto por tres elementos diferenciados:

- *dss:Result.* Componente que recoge el resultado final del proceso.
- *dss:OptionalOutput*. Elemento que añade información adicional a la respuesta, formato generado, identificador de transacción, etc.
- *dss:SignatureObject*. Elemento que contiene la firma generada o referencia a la misma.

b) *Respuesta con Periodo de Gracia.* En aquellos casos en la que la generación de la firma necesite la aplicación de un periodo de gracia el contenido del mensaje de respuesta es el siguiente:



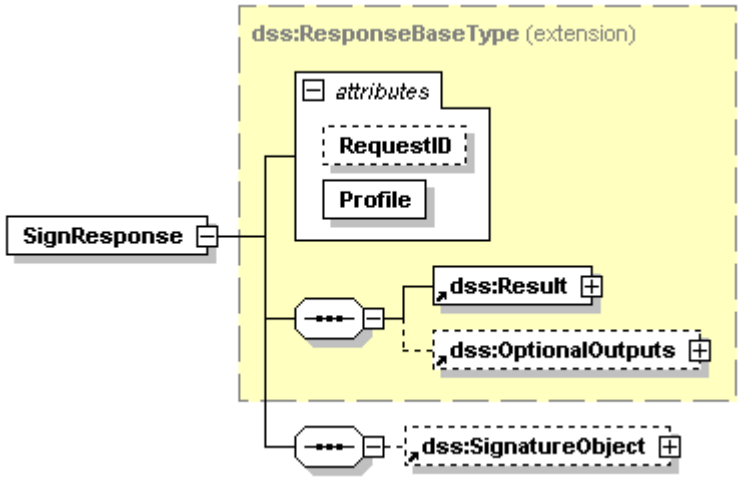
El mensaje de respuesta, *dss:SignRequest*, esta compuesto por dos elementos diferenciados:

dss:Result. Componente que recoge el resultado final del proceso. En aquellos casos en la que haya que aplicar un periodo de gracia en la generación de la firma el componente "*dss:Result*" tendrá el valor "**urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending"** en su componente "dss:ResultMayor" siguiendo las recomendaciones [DSS APAP]

- *dss:OptionalOutputs*. Elemento que añade información adicional a la respuesta. En este caso contendrá los elementos:
    - *async:ResponseID.* Componente que recoge el identificador de proceso asíncrono para su posterior consulta.
    - *afxp:ResponseTime.* Elemento que contiene una fecha estimada de finalización del proceso.

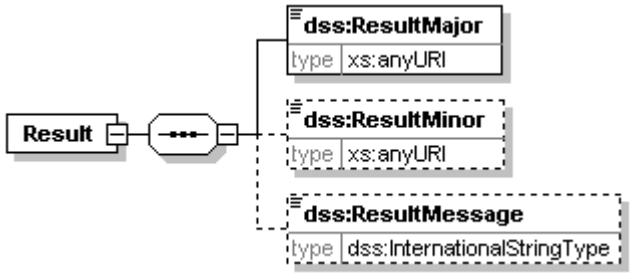
A continuación vamos a describir cada uno de los componentes expuestos.

8.1.1.2.1 <dss:SignResponse>

SignResponse	
Diagrama	
Descripción	Elemento raíz de la respuesta a una petición de firma
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:Result.* Este componente se describe en el apartado 8.1.1.2.2

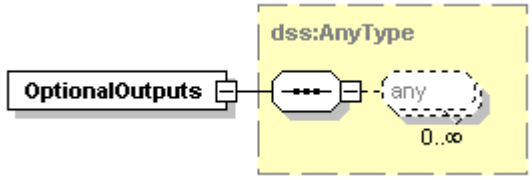
SignResponse		
	• *dss:OptionalOutput.* Este componente se describe en el apartado 8.1.1.2.3 • *dss:SignatureObject.* Este componente se describe en el apartado 8.1.1.2.4	
Atributos	Nombre	Descripción
	Profile	Perfil que implementa el servidor. Para respuestas de firma delegada a la plataforma el valor de este atributo será **urn:afirma:dss:1.0:profile:XSS**, esta URI identifica al perfil XSS de @Firma.
	RequestID	En caso de haberse especificado un identificador en la petición, se devolverá el mismo valor.

8.1.1.2.2 <dss:Result>

Result		
Diagrama		
Descripción	Elemento que contiene el resultado del proceso realizado.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	ResultMajor	Elemento que indica mediante una URI el resultado global del proceso. En el anexo A.3.5 se detallan los distintos valores que puede tomar este componente.

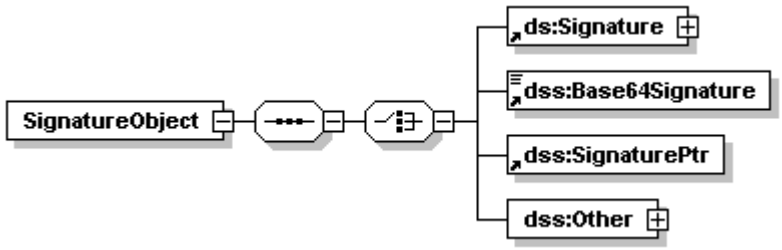
Result		
	ResultMinor	Elemento que especifica mediante una URI el resultado indicado en el componente anterior. En el anexo A.3.5 se detallan los distintos valores que puede tomar este componente.
	ResultMessage	Mensaje descriptivo del resultado del proceso.

8.1.1.2.3 <dss:OptionalOutputs>

OptionalOutputs	
Diagrama	
Descripción	Contiene parámetros adicionales de la respuesta definidos en [DSS Core] u otros perfiles o implementaciones DSS. Los elementos que puede contener OptionalInputs dependen del contexto en el que se encuentre incluido. Por favor, consulte los esquemas específicos para cada servicio para obtener más información acerca de qué elementos puede contener en cada contexto: 8.1.1.2 Respuesta de Firma Simple de Servidor 8.1.2.2 Respuesta de Firmas CoSign 8.1.3.1.12 Respuesta de Firmas CounterSign 8.2.1.1.21 Respuesta de Verificación de Firmas 8.2.2.2 Respuesta de Upgrade de Firmas 8.3.1.2 Respuesta de Validar Certificado

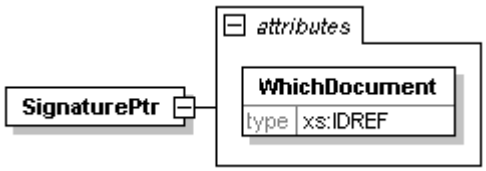
OptionalOutputs	
	8.4.2 Respuesta de Validaciones en Lotes 8.5.1.2 Respuesta de Consulta de Peticiones Asíncronas 8.6.1.2 Respuesta de Obtención de Firmas mediante Identificador de Transacción
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.1.1.2.4 <dss:SignatureObject>

SignatureObject		
Diagrama		
Descripción	Elemento que contiene o hace referencia a una firma electrónica.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	ds:Signature	Firma **XML Signature / XAdES** generada en modo **enveloping.** La firma va contenida sin codificar. Para más información sobre este elemento, se recomienda acudir a las especificaciones [XMLDSIG] / [XAdES]
	Base64Signature	Contiene la firma electrónica codificada en Base 64, en caso de tratarse de una firma que **no esté en formato XML**. Para mas información ver apartado 8.1.1.2.6
	SignaturePtr	Elemento que referencia a una firma XML Signature/ XAdES

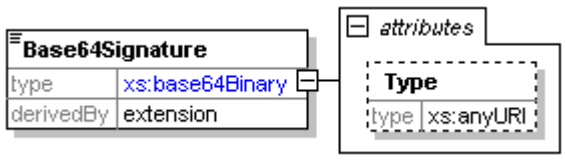
SignatureObject		
		enveloped o detached. Para más información ver apartado 8.1.1.2.5.
	Other	Elemento destinado a recoger nuevas implementaciones para contener información asociada a una firma electrónica. Para esta implementación este componente podrá contener una de estos tres elementos: ▪ Elemento *afxp:SignatureArchiveId* (apartado 8.2.2.1.3), conteniendo un identificador de transacción, en procesos de upgrade de firmas 8.2.2. ▪ Elemento cmism:getContentStream (apartado 0) con la localización de la firma electrónica en un gestor documental. Este componente se puede incluir en los servicios FirmaCoSign 8.1.2, FirmaCounterSign 8.1.3, Verificación de Firma 8.2.1 y Upgrade de Firma 8.2.2. ▪ Elemento ds:509Data (apartado 8.3.1.1.3) para contener un certificado en procesos de validación de certificados 8.3

8.1.1.2.5 <dss:SignaturePtr>

SignaturePtr	
Diagrama	
Descripción	Elemento que **referencia** a un elemento *dss:Document* que contiene una firma XML Signature / XAdES, dependiendo de si el mensaje es de petición o respuesta la firma estará localizada en componentes distintos:

SignaturePtr		
	- **Mensaje de petición**: En mensajes de petición la firma se incluirá en el elemento *dss:InputDocuments/dss:Document/dss:Base64XML*. Se puede obtener más información sobre este componente en el apartado 8.1.1.1.2. - **Mensajes de respuestas:** Para los XML de respuesta la firma XML enveloped o detached estará contenida en el elemento *dss:DocumentWithSignature dss:Document/dss:Base64XML*. Se puede obtener más información sobre este componente en el apartado 8.1.1.2.11	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	Nombre	Descripción
	WhichDocument	Contiene una referencia al documento, concretamente el valor del atributo *ID* del elemento *dss:Document* donde esta contenida la firma.

8.1.1.2.6 <dss:Base64Signature>

Base64Signature		
Diagrama		
Descripción	Elemento que contiene una firma de tipo ASN.1 (CMS o CAdES), ODF o PDF codificada en Base64	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	Nombre	Descripción
	Type	Especifica el formato de la firma contenida. Puede obtener más información acerca de las URI admitidas para

Base64Signature		
		este atributo en los anexos A.3.1 y A.3.2

8.1.1.2.7 <dss:SignatureType>

Especifica el formato base de la firma generada.

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.1.12

8.1.1.2.8 <ades:SignatureForm>

Especifica el modo (básico o extendido) de la firma generada.

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.1.13

8.1.1.2.9 <xss:ArchiveInfo>

ArchiveInfo	
Diagrama	
Descripción	Componente destinado a recoger información sobre el registro de una firma generada en el servidor. Este componente se encuentra definido en las especificaciones [DSS XSS].
Namespace	urn:oasis:names:tc:dss:1.0:profiles:XSS
Hijos	• arch:ArchiveIdentifier

8.1.1.2.10 <arch:ArchiveIdentifier>

ArchiveIdentifier	
Diagrama	
Descripción	Incluye el identificador de registro de una firma generado por la plataforma.
Namespace	urn:oasis:names:tc:dss:1.0:profiles:archive

8.1.1.2.11 <dss:DocumentWithSignature>

DocumentWithSignature		
Diagrama		
Descripción	Contiene firmas XML Signature / XAdES **enveloped** o **detached**, es decir, documentos XML que incluyen la firma electrónica.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:archive	
Hijos	Nombre	Descripción
	Document	En el contexto de una respuesta del servicio de generación de una firma XML detached o enveloped, el elemento *dss:Document* contendrá el documento XML que envuelve o contiene a la propia firma dentro de un componente "*dss:Base64XML*". Puede obtener información detallada sobre este elemento en el apartado 0.

8.1.1.2.12 <async:ResponseID>

ResponseID	
Diagrama	
Descripción	Elemento que contiene el "Identificador de Proceso Asíncrono" para obtener el resultado asociada a la petición mediante el servicio "DSSAsyncRequestStatus" (descrito en el apartado 8.5).
Namespace	urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:1.0

8.1.1.2.13 <afxp:ResponseTime>

ResponseTime	
Diagrama	
Descripción	Componente que recoge la fecha estimada a partir de la cual se podrá obtener la respuesta correspondiente a la petición realizada.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

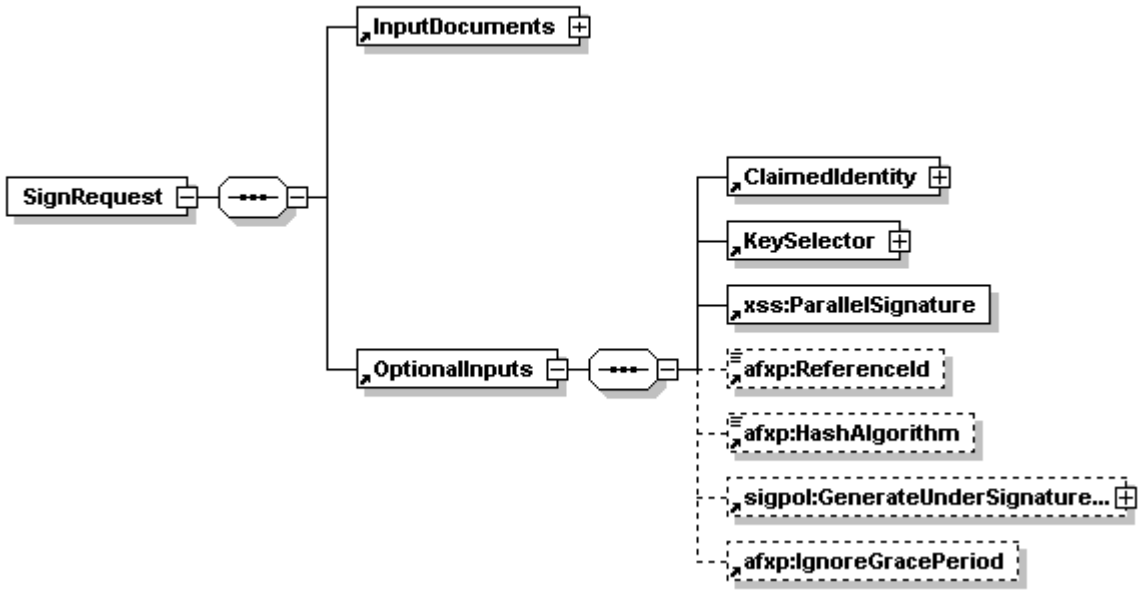
8.1.2 Firma Servidor CoSign

En este apartado se describirán las interfaces de petición y respuesta para un proceso de multifirma de servidor en paralelo (CoSign).

Esta operación no está permitida para los formatos de firma: CAdES-A, CAdES LTA-Level y XAdES-A.

8.1.2.1 Mensaje XML de Petición

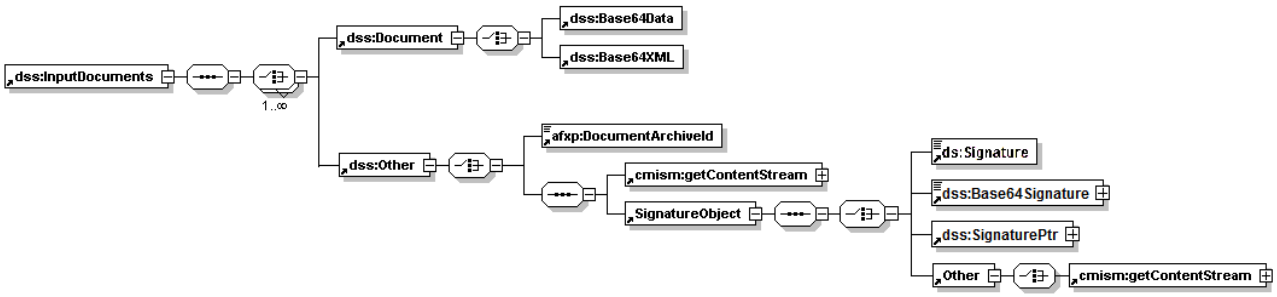
La figura mostrada a continuación detalla la sintaxis del mensaje XML de petición para la generación de una firma de servidor en modo cosign (cofirma o firma en paralelo). Como puede observar, la estructura de una petición de firma cosign es muy similar a la de una firma simple (8.1.1.1).



La inclusión de un elemento *xss:ParallelSignature* indica que los datos a firmar especificados en *dss:InputDocument* son, en realidad, una firma electrónica sobre la que desea realizarse una cofirma.

En una petición de cofirma no es necesario especificar información acerca del modo de generación de la firma, debido a que el sistema incluirá un nuevo firmante sobre la estructura de firma original, conservando su formato y modo.

El elemento *dss:InputDocument* recoge la información sobre la localización de la firma origen, en la siguiente figura se representa su contenido.



Dependiendo de si la firma origen se encuentra registrada en @firma, en un gestor documental, o se envía en la petición, el contenido del elemento *dss:InputDocuments* puede variar:

- Firma origen registrada en @firma. Se debe incluir en el componente *afxp:DocumentArchiveId* el valor del identificador de transacción origen.
- Firma origen registrada en un gestor documental. En este caso se debe incluir en la petición:
    - *cmism:getContentStream*. Con la localización de los datos originalmente firmados.
    - *dss:SignatureObject/dss:Other/cmism:getContentStream*. Con la localización de la firma origen.
- Firma enviada en la petición. Cuando la firma es enviada en la petición será necesario enviar también el documento original firmado en un elemento *dss:Document*. Dependiendo del tipo *de firma a procesar la petición debe hacerse de distinto modo.*
    - *Para firmas binarias, el contenido en base64 de la firma ha de incluirse en el elmento dss:SignatureObject/dss:Base64Signature.*
    - *Para firmas XML Enveloping, la firma debe incluirse en el elmento dss:SignatureObject/ds:Signature.*
    - *Para firmas XML Enveloped y Detached, se incluirá en el elemento dss:SignatureObject/dss:SignaturePtr una referencia al elemento dss:Document donde se incluirá la firma.*

A continuación se detallan únicamente aquellos elementos nuevos o que actúan de una forma particular para los procesos de multifirma CoSign. Puede consultar información más detallada sobre el resto de elementos especificados en la figura anterior en el apartado de Generación de una petición XML para firmas de servidor (8.1.1.1).

8.1.2.1.1 <dss:InputDocuments>

Componente que recoge los datos que van a ser firmados. Para obtener mas información sobre el elemento *dss:InputDocuments* puede consultarse el apartado 8.1.1.1.2

8.1.2.1.2 <dss:InputDocuments>/<dss:Other>

Dependiendo de si la firma origen se encuentra registrada en @firma, en un gestor documental, o se envía en la petición, el contenido del elemento *dss:InputDocuments/dss:Other* puede variar:

- Firma origen registrada en @firma. Se debe incluir en el componente afxp:DocumentArchiveId el valor del identificador de transacción origen.
- Firma origen registrada en un gestor documental. En este caso se debe incluir en la petición:
  - cmism:getContentStream. Con la localización de los datos originalmente firmados.
  - dss:SignatureObject/dss:Other/cmism:getContentStream. Con la localización de la firma origen.
- Firma enviada en la petición. Dependiendo del tipo de firma a procesar la petición debe hacerse de distinto modo.
  - Para firmas binarias, el contenido en base64 de la firma ha de incluirse en el elmento dss:SignatureObject/dss:Base64Signature.
  - Para firmas XML Enveloping, la firma debe incluirse en el elmento dss:SignatureObject/ds:Signature.
  - Para firmas XML Enveloped y Detached, se incluirá en el elemento dss:SignatureObject/dss:SignaturePtr una referencia al elemento dss:Document donde se incluirá la firma.

Para más información sobre este componente consultar el apartado 8.1.1.1.4

8.1.2.1.3 < dss:InputDocuments >/<dss:Document>

Permite incluir en la petición tanto el documento original firmado como la firma en caso de ser XML Detached o Enveloped.

Puede obtener información detallada sobre este elemento en el apartado 0

8.1.2.1.4 <afxp:DocumentArchiveId>

Permite especificar el identificador de transacción de la firma origen, generado por el sistema.

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.1.5

8.1.2.1.5 <cmism:getContentStream>

Elemento que permite incluir la localización de un elemento en un gestor documental externo, para este servicio los elementos referenciados serán el documento originalmente firmado y la firma que se desea multifirmar.

Puede obtener información detallada sobre este elemento en el apartado 0

8.1.2.1.6 <dss:ClaimedIdentity>

Componente obligatorio que contiene el identificador de aplicación. Para más información sobre este componente consultar el apartado 0

8.1.2.1.7 <dss:KeySelector>

Componente obligatorio que contiene el identificador de la clave a utilizar para la generación de una firma delegada. Para más información sobre este componente consultar el apartado 8.1.1.1.9

8.1.2.1.8 <afxp:ReferenceId>

Componente opcional que contiene una referencia o identificador externo generado por la aplicación cliente. Para más información sobre este componente consultar el apartado 8.1.1.1.11

8.1.2.1.9 <afxp:HashAlgorithm>

Componente opcional que contiene el algoritmo de resumen a utilizar en el proceso de firma. Para más información sobre este componente consultar el apartado 8.1.1.1.14

8.1.2.1.10 <xss:ParallelSignature>

ParallelSignature	
Diagrama	
Descripción	Especifica al motor de generación de firma que se debe realizar un proceso de cofirma. Este componente se encuentra definido en [DSS XSS].
Namespace	urn:oasis:names:tc:dss:1.0:profiles:XSS

8.1.2.1.11 <sigpol:GenerateUnderSignaturePolicy>

Componente opcional que indica que se desea realizar la multifirma en base a una determinada política de firma. Para más información sobre este componente consultar el apartado 8.1.1.1.18

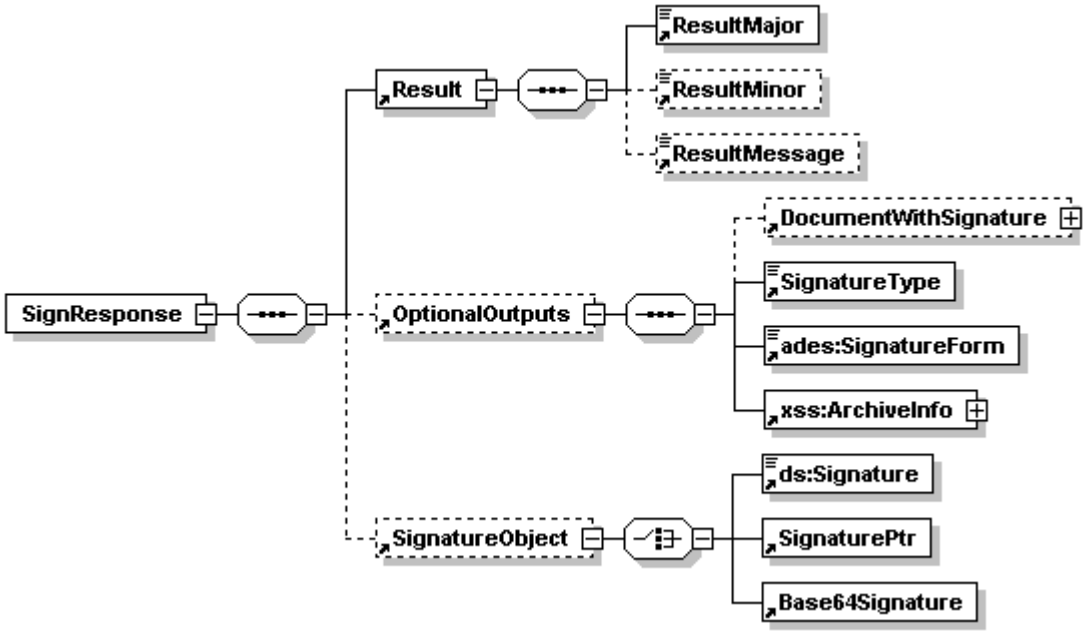
8.1.2.1.12 <afxp:IgnoreGracePeriod>

Componente opcional que indica que no se desea aplicar periodo de gracia. Para más información sobre este componente consultar el apartado 8.1.1.1.19

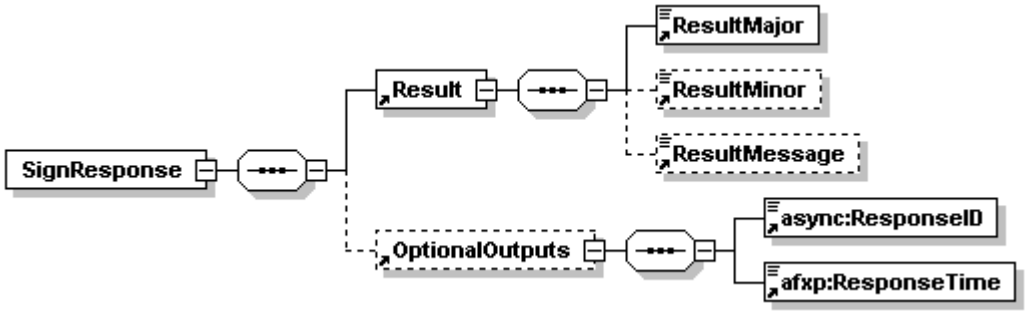
8.1.2.2 Mensaje XML de Respuesta

Las figuras mostradas a continuación especifica el formato de una respuesta a una petición de firma CoSign. Como puede observarse, la sintaxis es equivalente a la de un proceso de generación de firma de servidor simple.

a) *Respuesta sin Periodo de Gracia.*



b) *Respuesta con Periodo de Gracia.*



Puede obtener más información acerca de los mensajes de respuesta a este servicio en el apartado 8.1.1.2

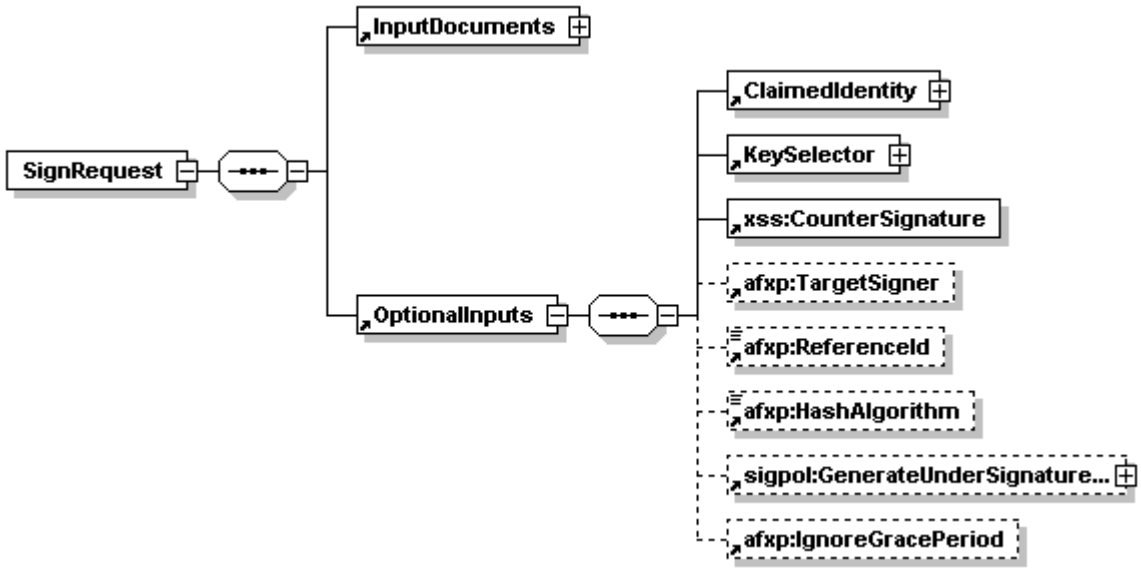
8.1.3 Firma Servidor CounterSign

En este apartado se describirán las interfaces de petición y respuesta para un proceso de generación de multifirma de servidor en cascada ó countersign.

Esta operación no está permitida para los formatos de firma: XMLDSIG, ODF, ODF-T, PDF, CAdES-A y XAdES-A.

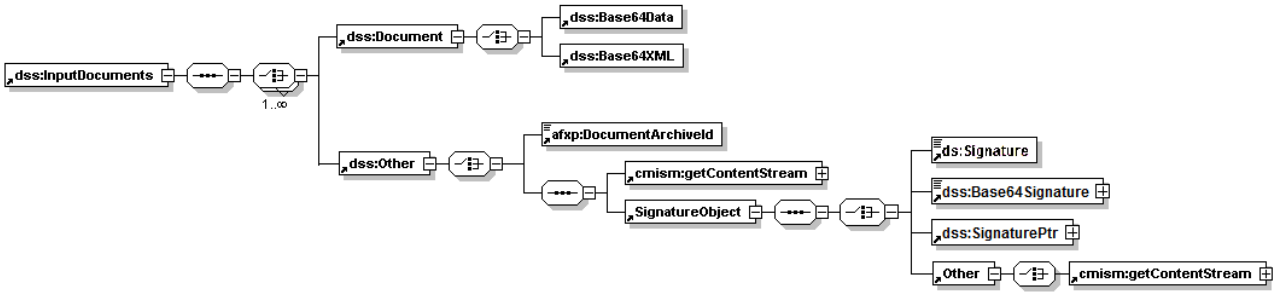
8.1.3.1 Mensaje XML de petición

La figura mostrada a continuación detalla la sintaxis del mensaje XML de petición para la generación de una firma de servidor en modo countersign (contrafirma o firma en cascada).



Como puede observar, la estructura de una petición de firma countersign es muy similar a la de una firma cosign (8.1.2.1), salvo por la inclusión de los elementos *xss:CounterSignature* (Obligatorio) y *afxp:TargetSigner* (Opcional).

Al incluir el elemento *xss:CounterSignature* en la petición se indica que se desea realizar una firma en cascada sobre la firma referenciada en el elemento *dss:InputDocuments*, a continuación se representa el contenido de este componente:



Como vemos el contenido de este último elemento dependerá de donde se encuentre alojada la firma origen, o si por otro lado se pasa en la petición:

- Firma origen registrada en @firma. Se debe incluir en el componente afxp:DocumentArchiveId el valor del identificador de transacción origen.
- Firma origen registrada en un gestor documental. Se incluye el elemento dss:SignatureObject/dss:Other/cmism:getContentStream con la localización de la firma origen.
- Firma enviada en la petición. Dependiendo del tipo de firma a procesar la petición debe hacerse de distinto modo.
    - Para firmas binarias, el contenido en base64 de la firma ha de incluirse en el elmento *dss:SignatureObject/dss:Base64Signature*.
    - Para firmas XML Enveloping, la firma debe incluirse en el elmento *dss:SignatureObject/ds:Signature*.
    - Para firmas XML Enveloped y Detached, se incluirá en el elemento *dss:SignatureObject/dss:SignaturePtr* una referencia al elemento *dss:Document* donde se incluirá la firma.

8.1.3.1.1 <dss:InputDocuments>

Componente que recoge los datos que van a ser firmado, en las peticiones de multifirma CounterSign este componente sólo podrá contener un elemento *dss:Other*. Para obtener mas información sobre el elemento *dss:InputDocuments* puede consultarse el apartado 8.1.1.1.2

8.1.3.1.2 <dss:InputDocuments>/<dss:Other>

Dependiendo de si la firma origen se encuentra registrada en @firma, en un gestor documental, o se envía en la petición, el contenido del elemento puede variar:

- Firma origen registrada en @firma. Se debe incluir en el componente afxp:DocumentArchiveId el valor del identificador de transacción origen.

- Firma origen registrada en un gestor documental. Se incluye el elemento dss:SignatureObject/dss:Other/cmism:getContentStream con la localización de la firma origen.

- Firma enviada en la petición. Dependiendo del tipo de firma a procesar la petición debe hacerse de distinto modo.

    - Para firmas binarias, el contenido en base64 de la firma ha de incluirse en el elmento *dss:SignatureObject/dss:Base64Signature*.

    - Para firmas XML Enveloping, la firma debe incluirse en el elmento *dss:SignatureObject/ds:Signature*.

    - Para firmas XML Enveloped y Detached, se incluirá en el elemento *dss:SignatureObject/dss:SignaturePtr* una referencia al elemento *dss:Document* donde se incluirá la firma.

Para más información sobre este componente consultar el apartado 8.1.1.1.4

8.1.3.1.3 < dss:InputDocuments >/<dss:Document>

Permite incluir en la petición la firma en caso de ser XML Detached o Enveloped.

Puede obtener información detallada sobre este elemento en el apartado 0

8.1.3.1.4 <afxp:DocumentArchiveId>

Permite especificar el identificador de transacción de la firma origen, generado por el sistema.

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.1.5

8.1.3.1.5 <cmism:getContentStream>

Elemento que permite incluir la localización de un elemento en un gestor documental externo, en este caso la firma electronica a multifirmar.

Puede obtener información detallada sobre este elemento en el apartado 0

8.1.3.1.6 <dss:ClaimedIdentity>

Componente obligatorio que contiene el identificador de aplicación. Para más información sobre este componente consultar el apartado 0

8.1.3.1.7 <dss:KeySelector>

Componente obligatorio que contiene el identificador de la clave a utilizar para la generación de una firma delegada. Para más información sobre este componente consultar el apartado 8.1.1.1.9

8.1.3.1.8 <afxp:ReferenceId>

Componente opcional que contiene una referencia o identificador externo generado por la aplicación cliente. Para más información sobre este componente consultar el apartado 8.1.1.1.11

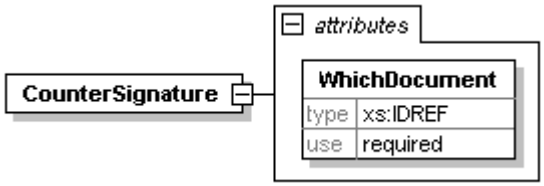
8.1.3.1.9 <afxp:HashAlgorithm>

Componente opcional que contiene el algoritmo de resumen a utilizar en el proceso de firma. Para más información sobre este componente consultar el apartado 8.1.1.1.14

8.1.3.1.10 <afxp:TargetSigner>

TargetSigner	
Diagrama	
Descripción	El elemento *TargetSigner* permite especificar un firmante que participó en la firma original para proceder a realizar la contrafirma sobre él. Para ello se incluirá, en codificación Base64, el certificado X.509 v3 del firmante objetivo. Este elemento puede ser utilizado en otros contextos para especificar el firmante objetivo sobre el que realizar una extensión de la firma, como puede ser añadir un sello de tiempo, etc.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.1.3.1.11 <xss:CounterSignature>

CounterSignature		
Diagrama		
Descripción	Especifica al motor de generación de firma que se debe realizar un proceso de contrafirma sobre la firma especificada en la petición. Este componente se encuentra definido en [DSS XSS].	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:XSS	
Hijos	Nombre	Descripción
	WhichDocument	Especifica el identificador único incluido en el elemento *afxp:DocumentArchiveId* (8.1.1.1.5), que contiene el identificador de transacción asociado a la firma a contrafirmar.

8.1.3.1.12 <sigpol:GenerateUnderSignaturePolicy>

Componente opcional que indica que se desea realizar la multifirma en base a una determinada política de firma. Para más información sobre este componente consultar el apartado 8.1.1.1.18

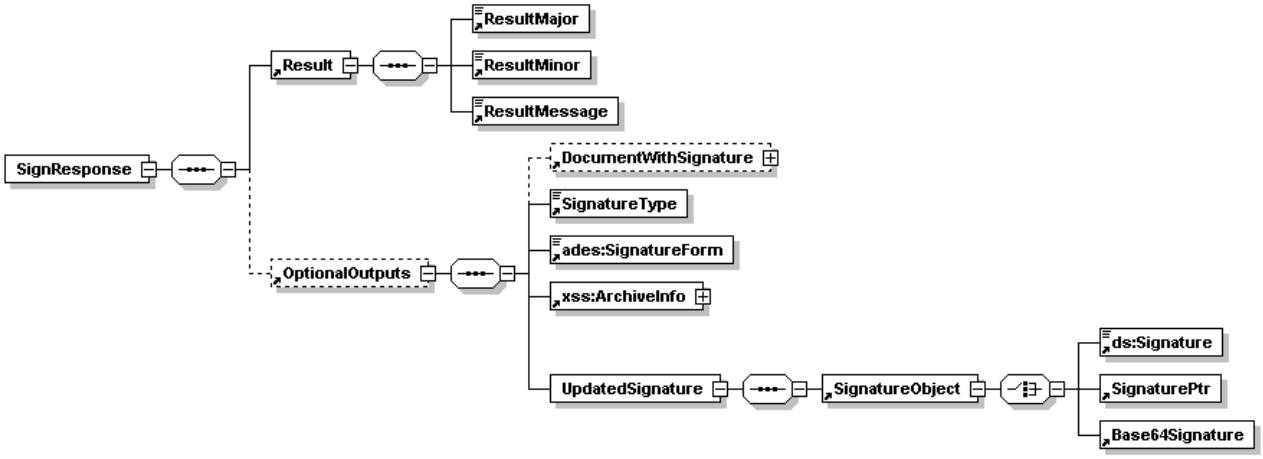
8.1.3.1.13 <afxp:IgnoreGracePeriod>

Componente opcional que indica que no se desea aplicar periodo de gracia. Para más información sobre este componente consultar el apartado 8.1.1.1.19

8.1.3.2 Mensaje XML de respuesta

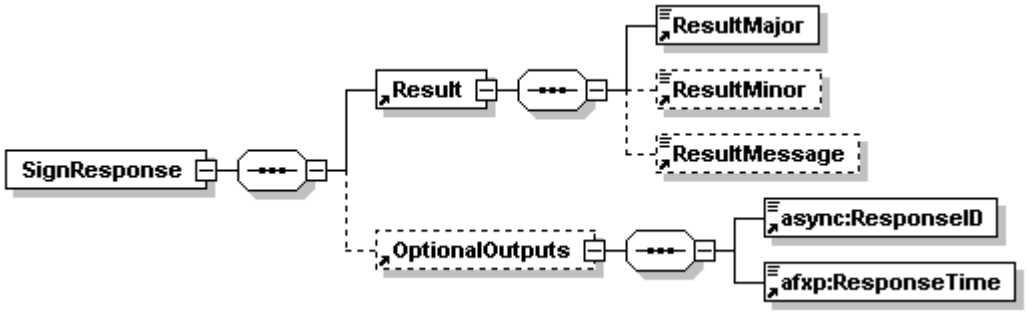
La figura mostrada a continuación especifica el formato de una respuesta a una petición de firma CounterSign.

a) Respuesta sin Periodo de Gracia.

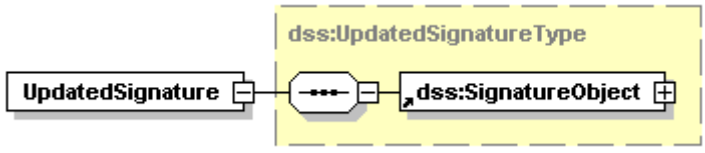


En este caso la firma generada se incluye dentro de un elemento “dss:UpdatedSignature”.

b) Respuesta con Periodo de Gracia.



8.1.3.2.1 <dss:UpdatedSignature>

UpdatedSignature	
Diagrama	

UpdatedSignature		
Descripción	Elemento encargado de recoger una firma actualizada, esta actualización puede haber sido realizada por dos vías: ▪ Contrafirma de una firma origen. ▪ Proceso de actualización de una firma origen a un formato mas avanzado.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:archive	
Hijos	Nombre	Descripción
	SignatureObject	Elemento DSS encagado de contene una firma electrónica. Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.4

8.2 Servicio de Validación y Actualización de Firmas

La interfaz Web Service *DSSAfirmaVerify* incorpora la siguiente funcionalidad:

- Validación de firmas electrónicas en los formatos admitidos por el sistema (ver apartado A.3.3)
- Actualización o upgrade de firmas electrónicas a un formato más avanzado.

FIRMAS ASN.1		FORMATO DE FIRMA DESTINO									
		CMS	CMS-T	CAdES-T	CAdES-C	CAdES-X	CAdES-XL	CAdES-A	CAdES T-Level	CAdES LT-Level	CAdES LTA-Level
FORMATO DE FIRMA ORIGEN	PKCS#7 v.1.5	☑	☑	☒	☒	☒	☒	☒	☒	☒	☒
	CMS	☒	☑	☒	☒	☒	☒	☒	☒	☒	☒
	CMS-T	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	CAdES	☒	☒	☑	☑	☑	☑	☑	☒	☒	☒
	CAdES-T	☒	☒	☒	☑	☑	☑	☑	☒	☒	☒
	CAdES-C	☒	☒	☒	☒	☑	☑*	☑*	☒	☒	☒
	CAdES-X	☒	☒	☒	☒	☒	☑*	☑[1]	☒	☒	☒
	CAdES-XL	☒	☒	☒	☒	☒	☒	☑*	☒	☒	☒
	CAdES-A	☒	☒	☒	☒	☒	☒	☑*	☒	☒	☒

[1] Por requisitos del formato, para elaborar una firma avanzada extendida a partir del formato –C se deberá reconstruir los atributos de validación de la firma electrónica.

FIRMAS ASN.1		FORMATO DE FIRMA DESTINO									
		CMS	CMS-T	CAdES-T	CAdES-C	CAdES-X	CAdES-XL	CAdES-A	CAdES T-Level	CAdES LT-Level	CAdES LTA-Level
	CAdES B-Level	☒	☒	☒	☒	☒	☒	☒	☑	☑	☑
	CAdES T-Level	☒	☒	☒	☒	☒	☒	☒	☒	☑	☑
	CAdES LT-Level	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑
	CAdES LTA-Level	☒	☒	☒	☒	☒	☒	☒	☒	☒	☑

En el caso de firmas ASiC-S, éstas pueden contener una firma CAdES B-Level, CadES T-Level, CAdES LT-Level o CAdES LTA-Level. En dicho caso, la actualización se realizaría sobre dicha firma CAdES, siguiendo la tabla anterior.

FIRMAS XML		FORMATO DE FIRMA DESTINO							
		XAdES-T	XAdES-C	XAdES-X	XAdES-XL	XAdES-A	XAdES T-Level	XAdES LT-Level	XAdES LTA-Level
FORMATO DE FIRMA ORIGEN	XAdES	☑	☑	☑	☑	☑	☒	☒	☒
	XAdES-T	☒	☑	☑	☑	☑	☒	☒	☒
	XAdES-C	☒	☒	☑*	☑*	☑*	☒	☒	☒
	XAdES-X	☒	☒	☒	☑*	☑*	☒	☒	☒
	XAdES-XL	☒	☒	☒	☒	☑*	☒	☒	☒
	XAdES-A	☒	☒	☒	☒	☑*	☒	☒	☒
	XAdES B-Level	☒	☒	☒	☒	☒	☑	☑	☑
	XAdES T-Level	☒	☒	☒	☒	☒	☒	☑	☑
	XAdES LT-Level	☒	☒	☒	☒	☒	☒	☒	☑
	XAdES LTA-Level	☒	☒	☒	☒	☒	☒	☒	☑

En el caso de firmas ASiC-S, éstas pueden contener una firma XAdES B-Level, XadES T-Level, XAdES LT-Level o XAdES LTA-Level. En dicho caso, la actualización se realizaría sobre dicha firma XAdES, siguiendo la tabla anterior.

Para versiones inferiores de XAdES v1.2.2 (véase, v1.1.1) no podrá llevarse a cabo operaciones de actualización a formatos superiores a XAdES-T, es decir, para firmas XAdES v1.1.1 sólo podrá llevarse a cabo la actualización a formato XAdES-T, nunca superior.

Para los procesos de actualización a XAdES-T se debe tener en cuenta la versión concreta de XAdES a la que se quiere extender. En la siguiente tabla se muestra la viabilidad de los distintos procesos de actualización entre formatos de firma en XML.

		FORMATO DE FIRMA DESTINO			
		XAdES-T v.1.1.1	XAdES-T v.1.2.2	XAdES-T v.1.3.2	XAdES-T v.1.4.2
FORMATO DE FIRMA ORIGEN	XMLDSIG	☒	☒	☒	☒
	XAdES v.1.1.1	☑	☒	☒	☒
	XAdES v.1.2.2	☒	☑	☒	☒
	XAdES v.1.3.2	☒	☒	☒	☑
	XAdES v.1.4.2	☒	☒	☒	☑

FIRMAS PDF		FORMATO DE FIRMA DESTINO				
		PAdES-LTV	PAdES B-Level	PAdES T-Level	PAdES LT-LEvel	PAdES LTA-Level
FORMATO DE FIRMA ORIGEN	PDF	☒	☒	☒	☒	☒
	PAdES-Basic	☑	☒	☒	☒	☒
	PAdES-BES	☑	☒	☒	☒	☒
	PAdES-EPES	☑	☒	☒	☒	☒
	PAdES-LTV	☑	☒	☒	☒	☒
	PAdES B-Level	☒	☒	☑	☑	☑
	PAdES T-Level	☒	☒	☒	☑	☑
	PAdES LT-Level	☒	☒	☒	☒	☑
	PAdES LTA-Level	☒	☒	☒	☒	☑

La mensajería de petición/respuesta para el servicio de validación y upgrade de firmas está definida por los siguientes elementos de la especificación [DSS Core] y los perfiles implementados.

- ***dss:VerifyRequest***: Elemento XML de petición del proceso de verificación/upgrade de firmas electrónicas.

- ***dss:VerifyResponse***: Elemento XML de respuesta del proceso de verificación/upgrade de firmas electrónicas.

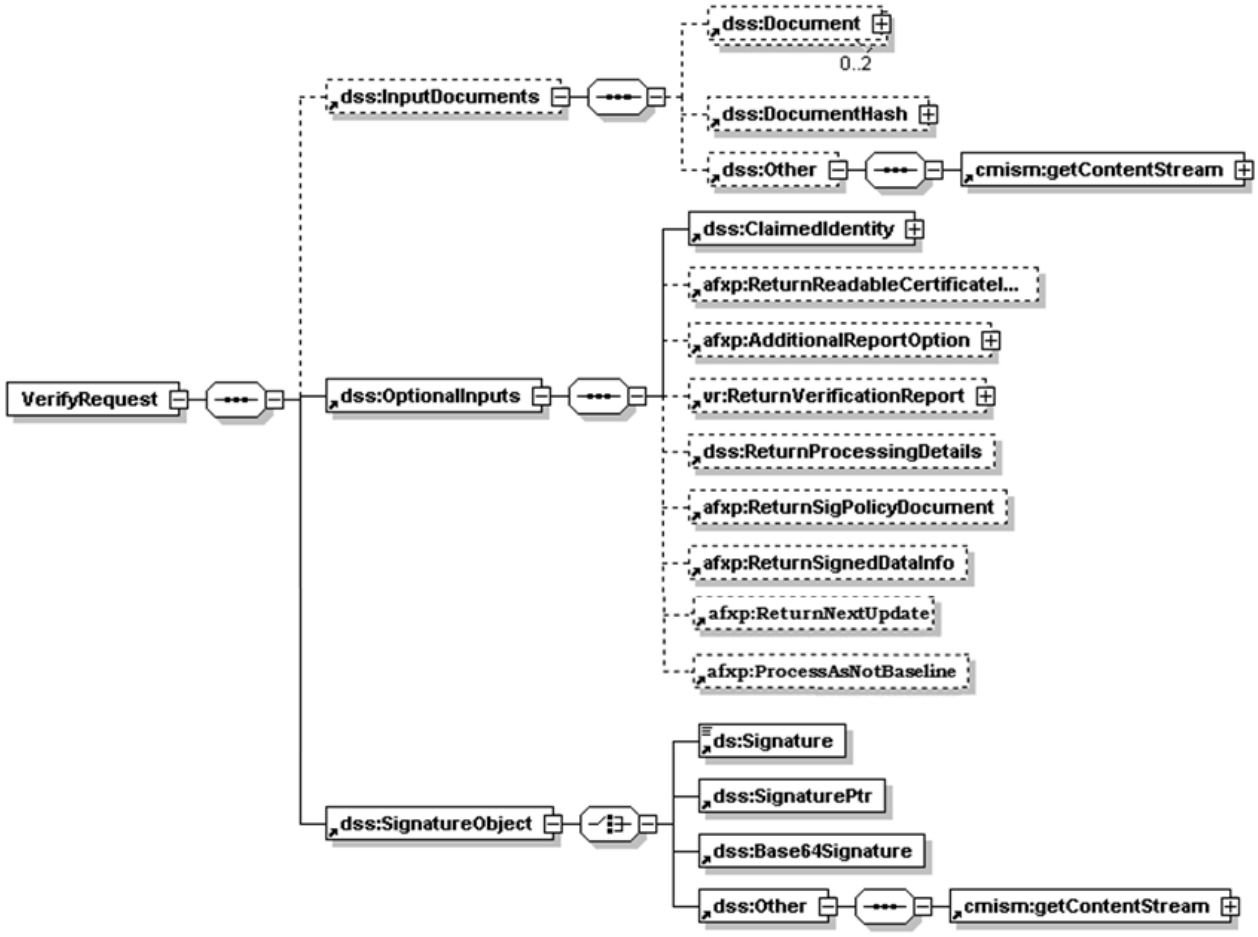
Para simplificar y hacer más clara la definición de los elementos de petición y respuesta del servicio, se han diferenciado las funcionalidades de Verificación y Upgrade.

8.2.1 Verificación de Firmas

El servicio de verificación de firmas permite validar de forma completa un firma electrónica, independientemente del formato y modo de la misma.

8.2.1.1 Mensaje XML de Petición

La figura a continuación define la estructura de una petición de validación de firma.



El elemento *dss:VerifyRequest* está compuesto por tres elementos:

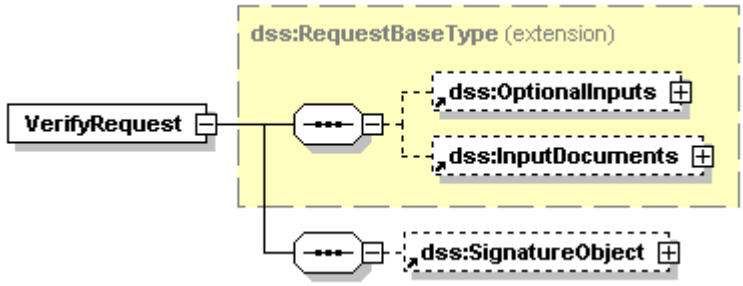
- *dss:InputDocument,* con los datos originalmente firmados y/o la firma a verifcar en el caso de firma XML detached o enveloped.

- *dss:OptionalInputs,* con información adicional para el uso de funcionalidades avanzadas del servicio de validación.

- *dss:SignatureObject,* con la firma electrónica a validar o referencia a la misma en el caso de firma XML detached o enveloped.

A continuación se detallará cada componente.

8.2.1.1.1 <dss:VerifyRequest>

VerifyRequest		
Diagrama		
Descripción	Elemento base de una petición de verificación o actualización de firma	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:SignatureObject,* con la firma electrónica a validar o referencia a la misma en el caso de firma XML enveloped o detached. • *dss:InputDocument,* con los datos originalmente firmados y/o la firma en el caso de firma XML detached o enveloped. • *dss:OptionalInputs,* con información adicional para el uso de funcionalidades avanzadas del servicio de validación.	
Atributos	Nombre	Descripción
	Profile	Identificador del perfil soportado por el servicio. Para peticiones de verificación de firma a la plataforma el valor de este atributo debe ser **urn:afirma:dss:1.0:profile:XSS**, esta URI identifica al perfil XSS de @Firma.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la

VerifyRequest		
		respuesta asociada a la misma. Si la aplicación cliente incluye este atributo, la respuesta generada por el servidor incluirá de igual manera un atributo con el mismo valor en el elemento *VerifyResponse*.

8.2.1.1.2 <dss:SignatureObject>

Contiene la firma electrónica a verificar o una referencia a la misma.

En el caso de que la firma se encuentre alojada en un gestor documental este componente solamente incluirá un componente *dss:Other* tal y como se especifica en el apartado 8.2.1.1.3.

En aquellos casos que la firma se incluya implícitamente en la petición la ubicación de la misma dependerá del formato de la firma en cuestión:

En caso de tratarse de una firma no XML (ASN.1, PDF u ODF), se incluirá en un elemento *dss:Base64Signature*. Para obtener más información sobre este componente consúltese el apartado 8.1.1.2.6

En el caso de firma XML **enveloping** se incluirá la firma sin codificar en un elemento *ds:Signature*

En el caso de firmas XML **enveloped** o **detached**, se incluirán un elemento *ds:SignaturePtr* el cual hará referencia al elemento dss:Base64XML que contendrá la firma. También se puede incluir de esta forma si la firma es XML **enveloping**, siempre que no se haya incluido anteriormente sin codificar en el elemento ds:Signature. Puede obtener más información sobre el componente *ds:SignaturePtr* en el apartado 8.1.1.2.5

Puede obtener más información sobre el componente *dss:SignatureObject* en el apartado 8.1.1.2.4

8.2.1.1.3 <dss:SignatureObject>/<dss:Other>

En el caso que la firma a validar se encuentre en un gestor documental se puede indicar su localización en un elemento *cmism:getContentStream* contenido dentro del componente *dss:Other* del elemento *dss:SignatureObject*

8.2.1.1.4 <dss:InputDocuments>

Componente que recoge los datos originalmente firmados y/o la firma en el caso de firma XML detached o enveloped. Puede obtener más información sobre el componente *dss:InputDocuments* en el apartado 8.1.1.1.2

8.2.1.1.5 <dss:InputDocuments>/<dss:Other>

Si el documento firmado se encuentra en un gestor documental podemos indicar su localización en un elemento cmism:getContentStream contenido dentro del componente dss:Other del elemento dss:InputDocuments

8.2.1.1.6 <dss:Document>

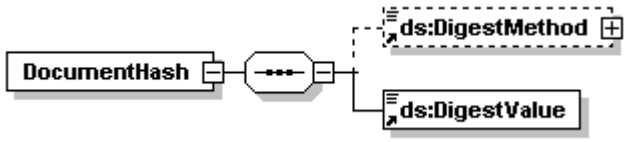
En el contexto de una petición al servicio de validación de firmas, puede contener el documento original firmado con el fin de que el proceso de validación verifique si el documento o referencia al mismo incluido en la firma electrónica coincide con el especificado. La inclusión de este elemento en este contexto es opcional.

En los caso que la firma a verificar sea XML Signature / XAdES **enveloped** o **detached,** este componente es obligatorio y debe contener al menos un elemento *dss:Base64XML* con la firma codificada en Base 64. También será obligatorio si la firma es XML Signature/XAdES **enveloping** y se ha incluido una referencia *ds:SignaturePtr* en el elemento *ds:SignatureObject*

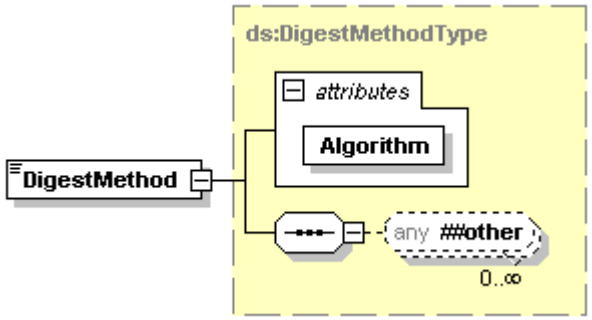
En el caso de firmas PAdES, el proceso de validación no verificará si el documento o referencia al mismo incluido en la firma electrónica coincide con el especificado.

Puede obtener información detallada sobre este elemento en el apartado **¡Error! No se encuentra el origen de la referencia.**.

8.2.1.1.7 <dss:DocumentHash>

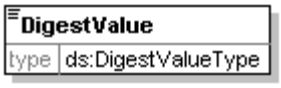
DocumentHash		
Diagrama		
Descripción	Contiene el resumen o hash de los datos originales, para su verificación con respecto a los datos incluidos en la firma. En el caso de firmas PAdES, no se realizará la verificación.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	ds:DigestMethod	Especifica el algoritmo de resumen utilizado, según se especifica en el apartado A.3.4. Si no se indica el algoritmo de resumen se supondrá que es SHA1
	ds:DigestValue	Contiene el valor del resumen o hash en codificación Base64.

8.2.1.1.8 <ds:DigestMethod>

DigestMethod	
Diagrama	

DigestMethod		
Descripción	Especifica el algoritmo de hash asociado al resumen al que referencia. Puede obtener más información sobre este elemento consultando [XMLDSIG]	
Namespace	http://www.w3.org/2000/09/xmldsig#	
Atributos	Nombre	Descripción
	Algorithm	URI que identifica el algoritmo de hash empleado. Consulte el anexo A.3.4 para obtener más información acerca de los algoritmos soportados y sus identificadores correspondientes.

8.2.1.1.9 <ds:DigestValue>

DigestValue	
Diagrama	
Descripción	Contiene el valor del resumen o hash en codificación Base64. Puede obtener más información sobre este elemento consultando [XMLDSIG]
Namespace	http://www.w3.org/2000/09/xmldsig#

8.2.1.1.10 <cmism:getContentStream>

Elemento que permite incluir la localización de un elemento en un gestor documental externo, en el caso de validación de firma podemos incluir la localización de:

- Firma a validar. Incluyendo este componente dentro de *dss:SignatureObject/dss:Other*
- Documento firmado. En cuyo caso, el elemento *cmism:getContentStream* se encuentra alojado en *dss:InputDocuments/dss:Other*

Puede obtener información detallada sobre este elemento en el apartado 0

8.2.1.1.11 <dss:ClaimedIdentity>

Permite identificar a la aplicación cliente que realiza la petición, por medio de la inclusión del identificador de aplicación establecido en el proceso de alta de la misma en el sistema.

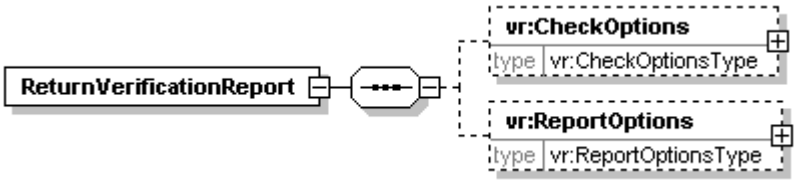
Su inclusión es obligatoria debido a que la política de seguridad del sistema exige que la aplicación que realiza la petición se identifique previamente al uso del servicio.

Puede obtener información detallada sobre este elemento en el apartado 0

8.2.1.1.12 <afxp:ReturnReadableCertificateInfo>

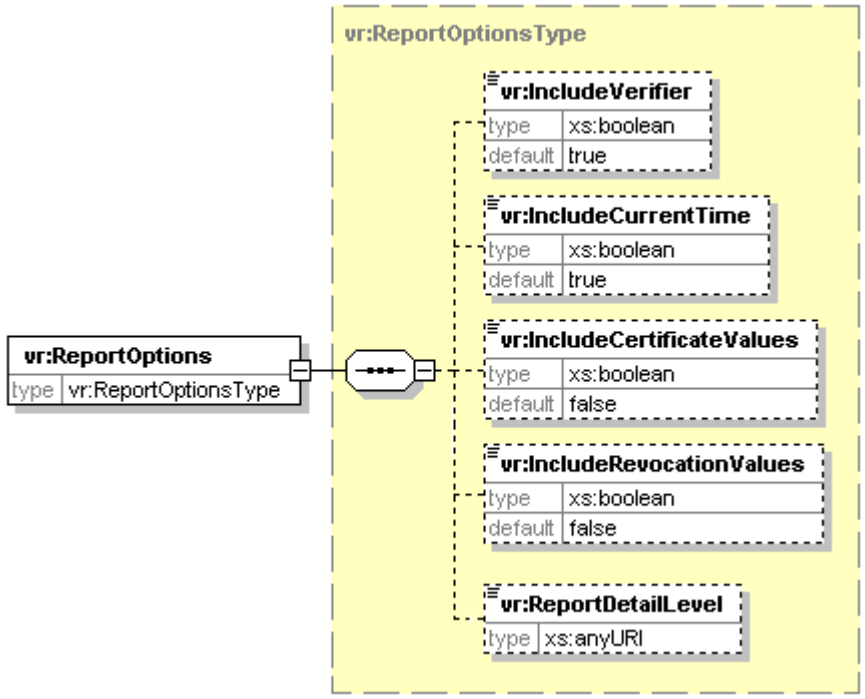
ReturnReadableCertificateInfo	
Diagrama	
Descripción	La inclusión de este elemento en una petición de verificación de firma o certificado indica al sistema que debe devolver información detallada de los certificados validados. Esta información se incluirá en la respuesta, en un elemento *afxp:ReadableCertificateInfo*. Para que se devuelva esta información es necesario que también se incluya el elemento vr:ReturnVerificationReport
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.2.1.1.13 <vr:ReturnVerificationReport>

ReturnVerificationReport	
Diagrama	
Descripción	Permite especificar las validaciones a realizar sobre la firma especificada, así como la

ReturnVerificationReport		
	información que debe ser devuelta en la respuesta, que será especificada en el elemento *vr:VerificationReport*	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	CheckOptions	Este elemento no se encuentra habilitado para los casos de verificación de firma. Su uso esta restringido a las peticiones de verificación de certificado.
	ReportOptions	Especifica qué información acerca del proceso de validación debe ser incluida en la respuesta.

8.2.1.1.14 <vr:ReportOptions>

ReportOptions	
Diagrama	

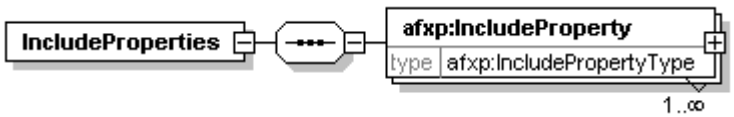
ReportOptions		
Descripción	Permite especificar qué información acerca del proceso de validación debe ser incluida en la respuesta.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	IncludeVerifier	Este elemento no se encuentra habilitado en la versión actual del perfil del sistema, aunque no se descarta su uso en versiones posteriores. Permite especificar en formato booleano si se desea que la respuesta incluya la identidad del verificador.
	IncludeCurrentTime	Este elemento no se encuentra habilitado en la versión actual del perfil del sistema, aunque no se descarta su uso en versiones posteriores. Permite especificar en formato booleano si se desea obtener fecha y hora local del servidor, del momento en el que se ha realizado la verificación de la firma.
	IncludeCertificateValues	Permite especificar en formato booleano si se desea que la respuesta incluya los certificados validados. Esta información aparecerá en la respuesta según el nivel de detalle especificado en *ReportDetailLevel*.
	IncludeRevocationValues	Permite especificar en formato booleano si se desea que la respuesta incluya los elementos de consulta de estado de revocación CRL u OCSP utilizados en la validación de los certificados. Esta información aparecerá en la respuesta según el nivel de detalle especificado en *ReportDetailLevel*.

ReportOptions		
	ReportDetailLevel	URI que especifica el nivel de detalle que se desea obtener en la respuesta del servicio. Para más información acerca de los valores que pueden ser incluidos en dicho elemento, consulte el anexo 0.

8.2.1.1.15 <afxp:AdditionalReportOption>

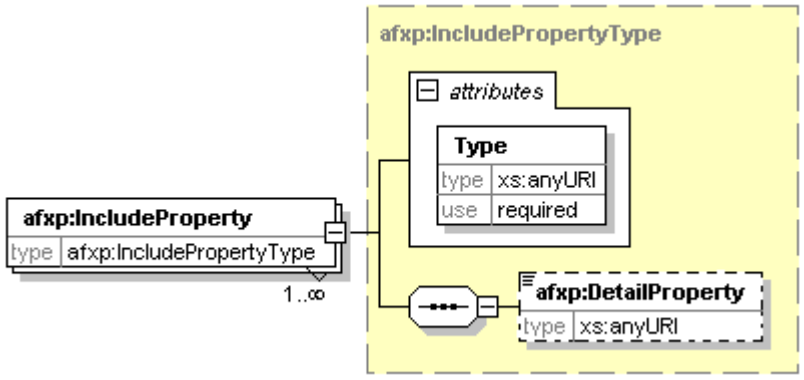
AdditionalReportOption		
Diagrama		
Descripción	Complementa al elemento *vr:ReportOptions* para indicar la inclusión en la respuesta del servicio de cierta información adicional sobre el proceso de validación, dicha información está asociada a atributos firmados y no firmados incluidos en la firma.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	IncludeProperties	Permite especificar atributos de la firma de los que se desea obtener información detallada en la respuesta del servicio.

8.2.1.1.16 <afxp:IncludeProperties>

IncludeProperties	
Diagrama	

IncludeProperties		
Descripción	Contiene la lista de atributos de la firma que sobre los que se desea obtener información detallada. Cada atributo vendrá definido en un elemento del tipo *afxp:IncludeProperty*	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	IncludeProperty	Identifica un atributo de firma del que se desea obtener información detallada. Se incluirán tantos elementos de este tipo como atributos deseen ser obtenidos de la firma.

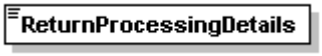
8.2.1.1.17 <afxp:IncludeProperty>

IncludeProperty		
Diagrama		
Descripción	Identifica un atributo de firma del que se desea obtener información detallada.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	DetailProperty	Permite especificar los detalles a obtener acerca del atributo de firma. La versión actual del perfil define un único valor para este atributo que permite obtener el "TimeStampToken" contenido en el atributo de

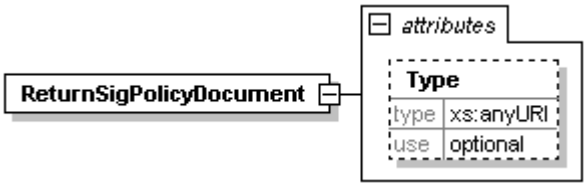
IncludeProperty		
		firma *SignatureTimestamp:* {id_perfil}:SignatureTimeStamp:IncludeTST Nota: id_perfil = urn:afirma:dss:1.0:profile:XSS:SignatureProperty
Atributos	Nombre	Descripción
	Type	Permite especificar el atributo de la firma del que se quiere obtener información detallada. Las URIs de los atributos de firma permitidos son: • **{id_perfil}:SignatureTimeStamp** - Atributo de firma que hace referencia al sello de tiempo. • **{id_perfil}:SigningTime** - Atributo de firma que hace referencia al instante de tiempo en el que el firmante afirma haber realizado la proceso de firma. • **{id_perfil}:CommitmentTypeIndication-** Atributo de firma que hace referencia al compromiso asumido por el firmante en la firma de los datos firmados en el contexto de la política de firma seleccionada (cuando se está utilizando un compromiso explícito). • **{id_perfil}:SignerRole-** Atributo de firma que hace referencia al reclamo o los roles certificados asumidos por el firmante en la creación de la firma. Nota: id_perfil = urn:afirma:dss:1.0:profile:XSS:SignatureProperty

8.2.1.1.18 <dss:ReturnProcessingDetails>

ReturnProcessingDetails

ReturnProcessingDetails	
Diagrama	
Descripción	Componente definido en las especificaciones [DSS Core] que permite obtener el resultado de cada tarea de verificación que forma el proceso de validación de una firma electrónica. En caso de incluirse en la petición la respuesta debera contener por cada firma verificada un componente "*dss:ProcessingDetails*"
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

8.2.1.1.19 <afxp:ReturnSigPolicyDocument>

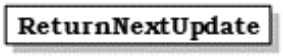
ReturnSigPolicyDocument		
Diagrama		
Descripción	Componente que incluido en la petición indica que desea obtener el documento de la politica de firma. En esta versión del perfil solamente se podrá obtener el documento formal de la política (en formato ASN1 o XML)	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Atributos	Nombre	Descripción
	Type	URI que identifica el tipo de documento de la politica que se desea obtener (formal, legible…).

ReturnSigPolicyDocument		
		Actualmente este perfil define el siguiente valor: urn:afirma:dss:1.0:profile:XSS:SigPolicyDocument:FormalDocument

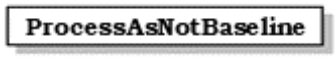
8.2.1.1.20 <afxp:ReturnSignedDataInfo>

ReturnSignedDataInfo	
Diagrama	
Descripción	Componente que permite al cliente solicitar información sobre los datos firmados. En el caso de incluir este componente en la petición la respuesta deberá incluir un componente "*afxp:SignedDataInfo*" con la información sobre los datos firmados. En el caso de firmas PAdES la información retornada corresponderá a la firma ASN1 contenida en el diccionario.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.2.1.1.21 <afxp:ReturnNextUpdate>

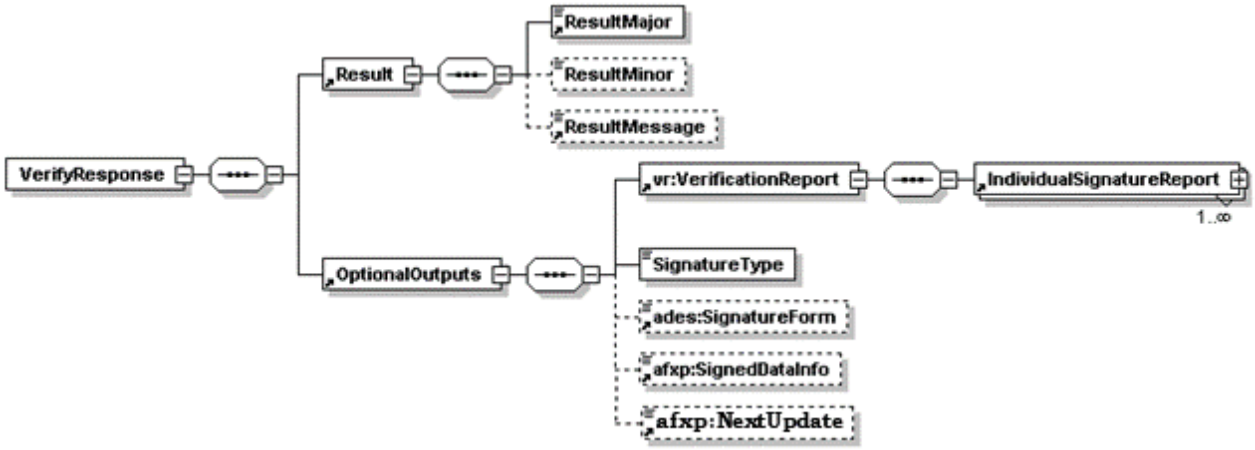
ReturnNextUpdate	
Diagrama	
Descripción	Componente que permite conocer la fecha de próxima actualización de la firma, esto es, la fecha a partir dela cual la firma dejará de ser válida. En el caso de incluir este componente en la petición, la respuesta deberá incluir un componente "*afxp: NextUpdate*" con la fecha de expiración de la firma.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.2.1.1.22 <afxp:ProcessAsNotBaseline>

ProcessAsNotBaseline	
Diagrama	
Descripción	Componente que permite realizar el proceso de validación como no baseline, ignorando la configuración general de la plataforma al respecto. En el caso de incluir este componente en la petición, la validación se realizará como no baseline.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.2.1.2 Mensaje XML de Respuesta

La figura a continuación define la estructura de una respuesta de verificación de firma. El contenido de la respuesta dependerá de la información incluida en la petición.



De forma genérica, una respuesta de verificación puede incluir los siguientes elementos:

- *dss:Result*, con el resultado del proceso de verificación. Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.2.

- *dss:OptionalOutputs,* elementos adicionales

- *vr: VerificationReport,* que contendrá información detallada sobre los procesos de verificación realizados. Este elemento únicamente se incluirá en la respuesta en el caso de que la petición haya incorporado un *vr:ReturnVerificationReport.*

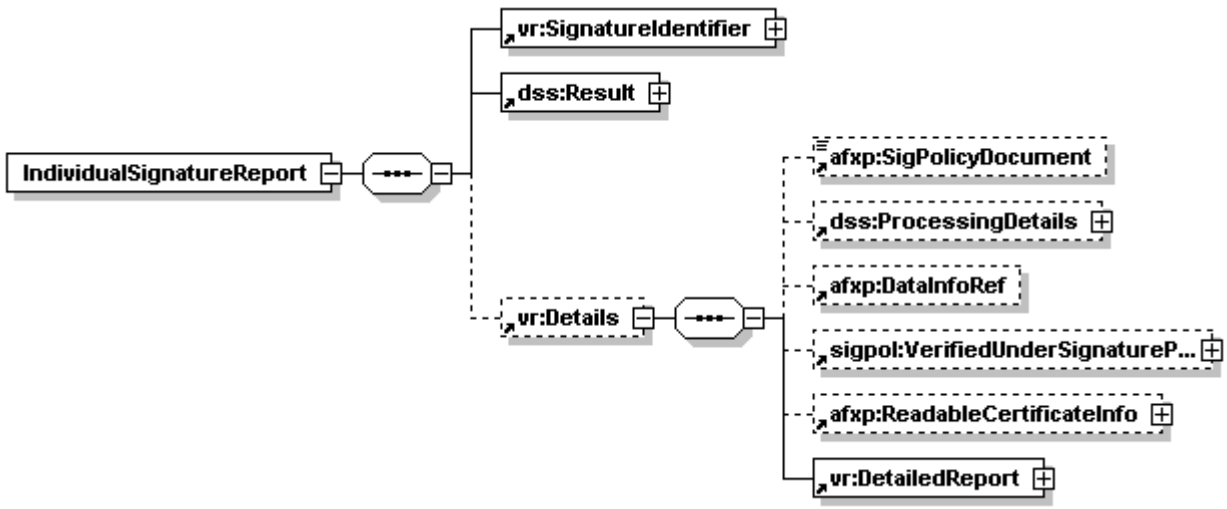
- *dss:SignatureType,* especifica el tipo de firma (formato) que corresponde con la firma validada.

- *ades:SignatureForm,* en aquellos casos que la firma validada sea una firma avanzada (AdES-T, AdES-C, etc) este componente indicara cual es el formato avanzado que implementa la firma.

- *afxp:SignedDataInfo,* contiene información sobre los datos firmados este componente se incluirá en la respuesta sí se ha solicitado en la petición.

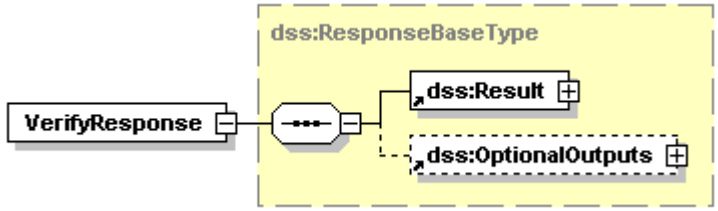
- *afxp:NextUpdate,* Contiene la fecha de expiración de la firma.

Por cada firma verificada se incluirá un componente *vr:IndividualSignatureReport con el* resultado del proceso de validación y la información adicional solicitada de la misma, en la siguiente figura se muestra el contenido de este componente.



En los siguientes apartados se detalla cada uno de los elementos que puede contener la respuesta del servicio de verificación de firmas.

8.2.1.2.1 <dss:VerifyResponse>

VerifyResponse		
Diagrama		
Descripción	Elemento raíz de la respuesta a una petición de Verificación de Firma	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *Result.* Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.2. • *OptionalOutput.* Componente que recoge aquella información adicional sobre el proceso de validación. Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.3	
Atributos	Nombre	Descripción
	Profile	Identificador del perfil soportado por el servicio. Para peticiones de verificación de firma a la plataforma el valor de este atributo debe ser **urn:afirma:dss:1.0:profile:XSS**, esta URI identifica al perfil XSS de @Firma.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma. Si la aplicación cliente incluye este atributo, la respuesta generada por el servidor incluirá de igual manera un atributo con el mismo valor en el elemento *VerifyResponse*.

8.2.1.2.2 <dss:Result>

Componente que informa sobre el resultado del proceso, en las respuestas de verificación existen dos tipos de resultados:

- Resultado global del proceso (es hijo del componente *dss:VerifyRequest*) que indica el resultado final de la operación.
- Resultado parcial (es hijo de *vr:IndividualSignatureReport*) que nos informa del resultado de la operación de verificación de una determinada firma.

Para más información sobre este componente véase el apartado 8.1.1.2.2

8.2.1.2.3 <dss:SignatureType>

El servicio de validación de firma incluye en su respuesta el formato de la firma validada, para facilitar esta información se recurre a la utilización de los componentes "dss:SignatureType" y "ades:SignatureForm" siguiendo las recomendaciones OASIS-DSS.

El componente "dss:SignatureType" especifica el tipo de firma o familia (formato) a la que pertenece la firma validada.

Podemos consultar una descripción formal de este componente en el apartado 8.1.1.1.12

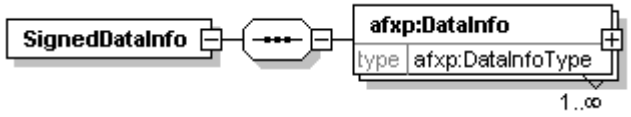
8.2.1.2.4 <ades:SignatureForm>

Si la firma validada es una firma avanzada (CAdES o XAdES) este componente especifica el tipo de firma avanzada que implementa.

Podemos consultar una descripción formal de este componente en el apartado 8.1.1.1.13

8.2.1.2.5 <afxp:SignedDataInfo>

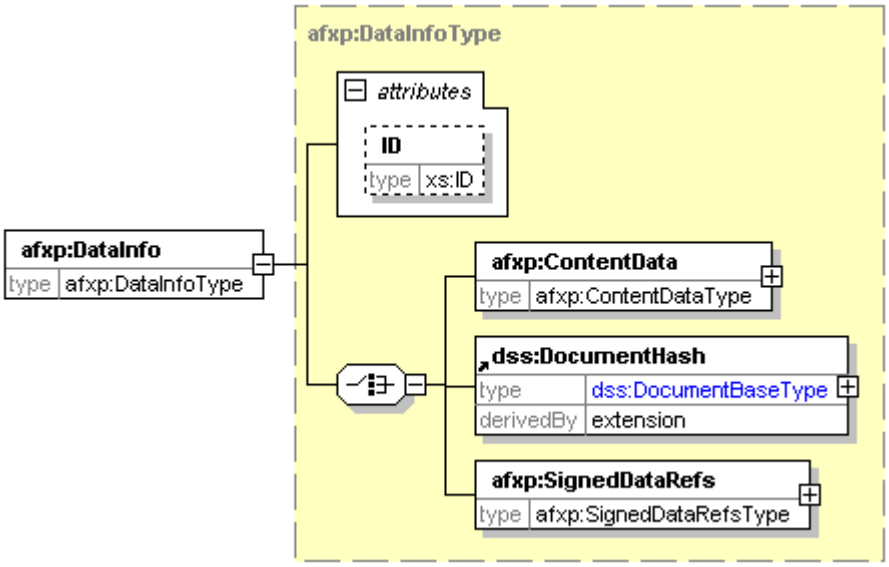
SignedDataInfo

SignedDataInfo		
Diagrama		
Descripción	Componente que contiene la información sobre los datos firmados.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	DataInfo	Componente que contiene la información de los datos firmados por los firmantes de la firma verificada. Para representar esta información, el elmento *afxp:SignedDataInfo* contiene una serie de elementos *afxp:DataInfo*, correspondiente con los contenidos firmados de cada firma validada. **Si dos firmantes comparten un mismo contenido firmado se repetirá el elemento**. Este elemento asocia los contenidos firmados con las firmas y **no** sirve para detectar la jerarquía de las mismas (simple, paralela o cascada).

8.2.1.2.6 <afxp:NextUpdate>

NextUpdate		
Diagrama		
Descripción	Componente que contiene la fecha de expiración de la firma.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	NextUpdate	Componente que contiene la fecha en la cual la firma deja de ser válida.

8.2.1.2.7 <afxp:DataInfo>

<table>
<tr><th colspan="3">DataInfo</th></tr>
<tr><td>Diagrama</td><td colspan="2"> 
</td></tr>
<tr><td>Descripción</td><td colspan="2">Componente que contiene la información de los datos firmados por un firmante particular de la firma verificada.</td></tr>
<tr><td>Namespace</td><td colspan="2">urn:afirma:dss:1.0:profile:XSS:schema</td></tr>
<tr><td rowspan="3">Hijos</td><td>Nombre</td><td>Descripción</td></tr>
<tr><td>ContentData</td><td>Componente que contiene los datos originalmente firmados.

Este componente está contenido en el elemento “afxp:DataInfo” si la firma verificada es implícita (contiene los datos firmados) y su formato de firma no es de tipo XML.

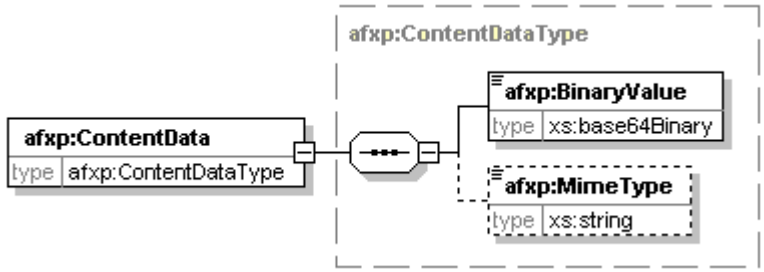
Este componente se devolverá también si el formato de la firma es PDF del tipo “approval signature”, siempre que el pdf no sea linearized y se hayan realizado actualizaciones incrementales.

Puede obtenerse más información de este componente en el apartado 8.2.1.2.8</td></tr>
<tr><td>DocumentHash</td><td>Componente que contiene el resumen de los datos originalmente firmados.

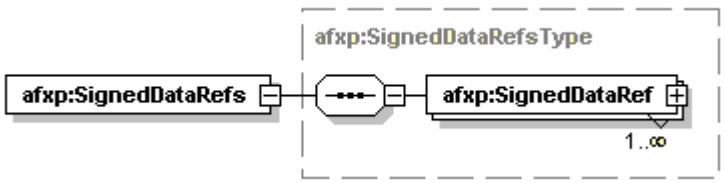
Este componente está contenido en el elemento “afxp:DataInfo” si</td></tr>
</table>

DataInfo		
		la firma verificada es explícita (no contiene los datos firmados) y su formato de firma no es de tipo XML. Si el formato de la firma es PADES también se incluye este componente, ya que la firma incluida en el diccionario se corresponde con el formato CADES. Se puede obtener mas información sobre este componente en el apartado 8.2.1.1.7
	SignedDataRefs	Componente que contiene información sobre las referencias firmadas por un firmante. Este componente está contenido en el elemento "*afxp:DataInfo*" si el formato de la firma verificada es de tipo XML Puede obtenerse más información de este componente en el apartado 8.2.1.2.9
Atributos	Nombre	Descripción
	ID	Identificador único que permitirá identificar el componente "*afxp:DataInfo*" y hacer referencia al mismo desde uno o varios firmantes mediante la utilización del componente "*afxp:DataInfoRef*". Puede obtenerse una información detallada del componente "*afxp: DataInfoRef*" en el apartado 8.2.1.2.18

8.2.1.2.8 <afxp:ContentData>

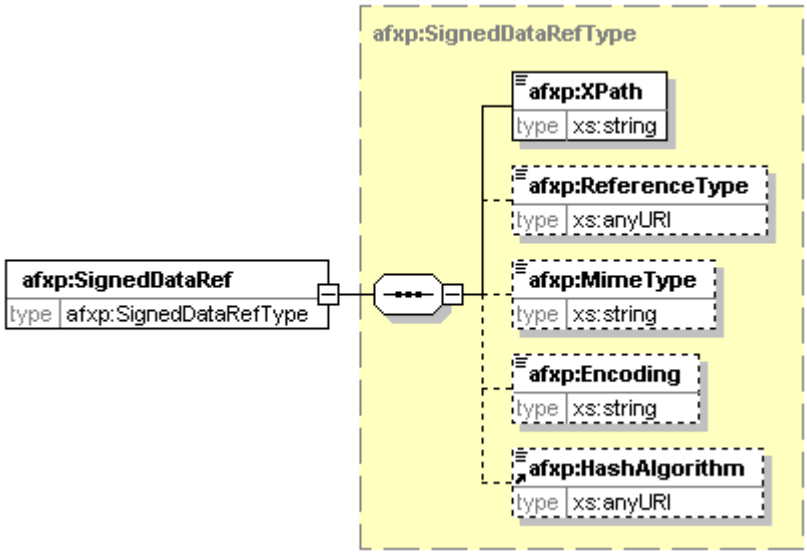
ContentData		
Diagrama		
Descripción	Componente que contiene los datos originalmente firmados.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	BinaryValue	Elemento que contiene los datos originalmente firmados en Base64.
	MimeType	Elemento que contiene el Mime-Type de los datos. Este componente aparecerá en la respuesta si la firma incluye esta información.

8.2.1.2.9 <afxp:SignedDataRefs>

SignedDataRefs	
Diagrama	
Descripción	Componente que contiene la información sobre las referencias firmadas por un firmante particular en una firma XML.

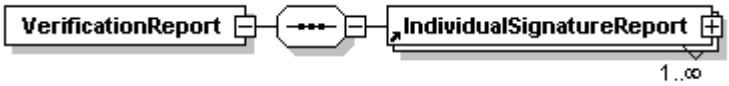
SignedDataRefs		
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	SignedDataRef	Elemento que recoge información sobre una referencia firmada.

8.2.1.2.10 <afxp:SignedDataRef>

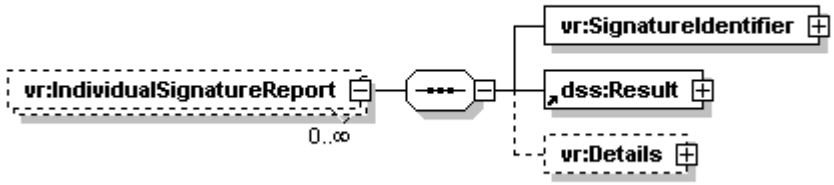
SignedDataRef		
Diagrama		
Descripción	Componente que contiene la información asociada a un elemento "*ds:Reference*" de una firma XML.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	XPath	Ruta XPath al elemento referenciado por el componente "*ds:Reference*" validado
	ReferenceType	Elemento que contiene el valor del atributo "Type" del componente "ds:Reference" validado

SignedDataRef		
	MimeType	Elemento que contiene el Mime Type de los datos firmados (en el caso que la firma verificada incluye esta información)
	Encoding	Elemento que contiene la codificación de los datos firmados (en el caso que la firma verificada incluye esta información)
	HashAlgorithm	Algoritmo de hash utilizado para la creación del componente "*ds:Reference*"

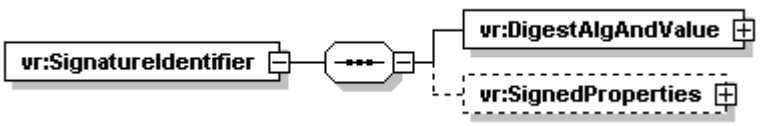
8.2.1.2.11 <vr:VerificationReport>

VerificationReport		
Diagrama		
Descripción	Contiene el resultado e información adicional generada durante el proceso de verificación de una firma. Para cada firma individual (multifirmas) incluida dentro de la firma especificada en la petición, se incluirá un elemento del tipo *vr:IndividualSignatureReport* El elemento *vr:VerificationReport* será incluido en la respuesta únicamente si la petición incorpora un elemento *vr:ReturnVerificationReport*	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	IndividualSignatureReport	Incluye información detallada sobre el procesamiento de una firma concreta contenida en la firma original.

8.2.1.2.12 <vr:IndividualSignatureReport>

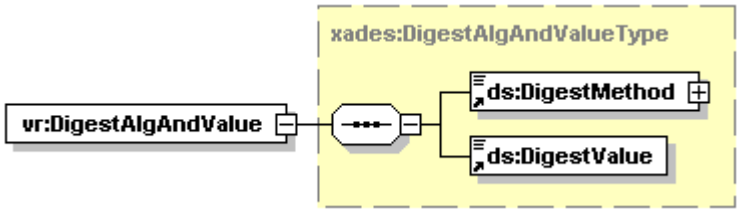
IndividualSignatureReport		
Diagrama		
Descripción	Incluye información detallada sobre el procesamiento de una firma concreta contenida en la firma original.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	SignatureIdentifier	Contiene un identificador a la firma referenciada.
	dss:Result	Contiene información detallada sobre el resultado del procesamiento de una firma en particular.
	Details	Contiene aquellos item de información adicional solicitados en la petición

8.2.1.2.13 <vr:SignatureIdentifier>

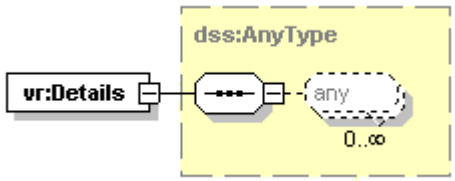
SignatureIdentifier	
Diagrama	
Descripción	Identificador de la firma específica que ha sido procesada.
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#

SignatureIdentifier		
Hijos	Nombre	Descripción
	vr:DigestAlgAndValue	Contiene el resumen de la firma particular procesada y el algoritmo con el que se calculó.
	vr:SignedProperties	Elemento que contiene algún atributo firmado que permite identificar a la firma procesada. Este elemento no tiene uso en la versión actual del perfil implementado por el sistema.

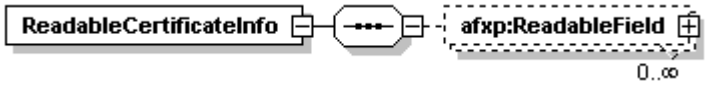
8.2.1.2.14 <vr:DigestAlgAndValue>

DigestAlgAndValue	
Diagrama	
Descripción	Contiene el valor resumen a partir del cual se creó la firma particular procesada y el algoritmo con el que se calculó. Para firmas ASN.1 el resumen se calcula sobre el elemento *SignerInfo*. En el caso de firmas XML, el resumen se calculará a partir del elemento *ds:Signature*. Con el fin de evitar ambigüedades en firmas XML, el sistema aplicará la transformada "http://www.w3.org/2001/10/xml-exc-c14n#" (canonicalización exclusiva sin comentarios) previamente al calculo del resumen.
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#
Hijos	• ds:DigestMethod • ds:DigestValue

8.2.1.2.15 <vr:Details>

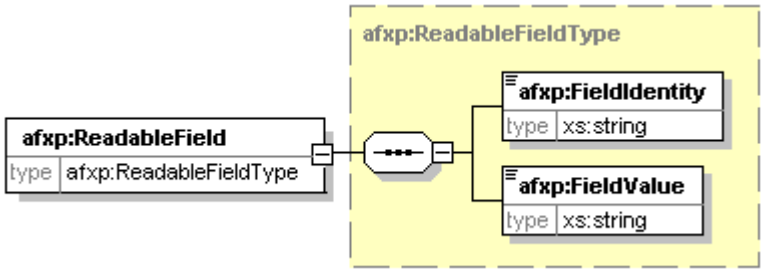
Details	
Diagrama	
Descripción	Componente que contiene aquella información adicional solicitada en la petición. Para esta implementación este componente puede contener los elementos : • *afxp:ReadableCertificateInfo* (descrito en el apartado 8.2.1.2.16) • *afxp:DataInfoRef* (descrito en el apartado 8.2.1.2.18) • *sigpol:VerifiedUnderSignaturePolicy* (descrito en el apartado 8.2.1.2.19) • *afxp:SigPolicyDocument* (descrito en el apartado 8.2.1.2.22) • *dss: ProcessingDetails* (descrito en el apartado 8.2.1.2.23) • *vr: DetailedReport* (descrito en el apartados 8.2.1.2.27)
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#

8.2.1.2.16 <afxp:ReadableCertificateInfo>

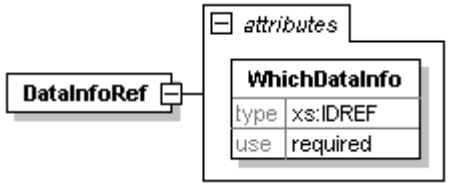
ReadableCertificateInfo	
Diagrama	
Descripción	Incluye información detallada del certificado firmante. Esta información será una lista de campos del tipo atributo/valor con el resultado de haber parseado el certificado según la configuración del sistema. Este componente únicamente se incluirá en la respuesta si la petición incorporaba

ReadableCertificateInfo		
	explícitamente un elemento *afxp:ReturnReadableCertificateInfo*	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	ReadableField	Contiene información acerca de un campo concreto extraído del certificado. Sería el equivalente a un campo lógico del certificado.

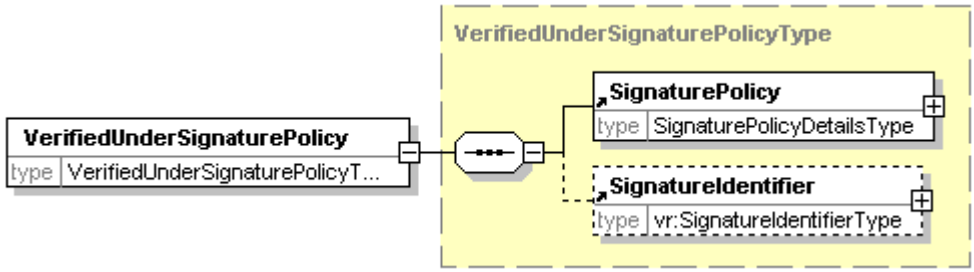
8.2.1.2.17 <afxp:ReadableField>

ReadableField		
Diagrama		
Descripción	Contiene información acerca de un campo concreto extraído del certificado. Sería el equivalente a un campo lógico del certificado.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	FieldIdentity	Nombre del atributo resultante del parseo del certificado. Es el identificador del campo lógico.
	FieldValue	Valor correspondiente al atributo especificado.

8.2.1.2.18 <afxp:DataInfoRef>

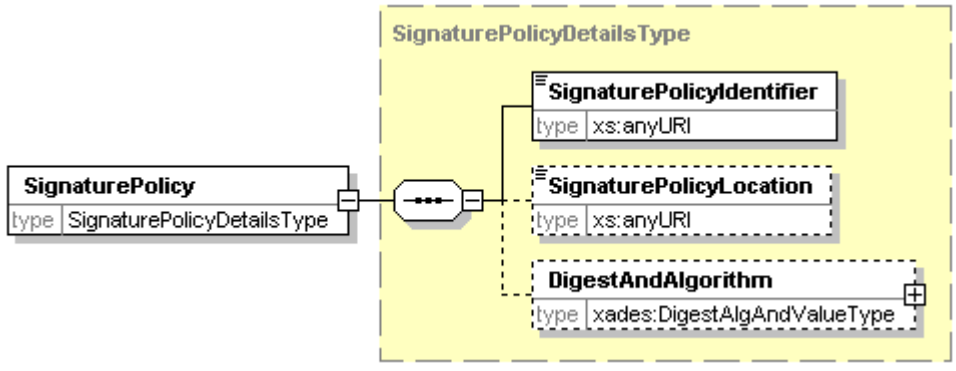
DataInfoRef		
Diagrama		
Descripción	Componente que referencia al elemento "*afxp:DataInfo*" que contiene la información sobre los datos firmados por el firmante validado. Este elemento se incluirá en la respuesta si la petición incluye el componente "*afxp:ReturnSignedDataInfo*"	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Atributos	Nombre	Descripción
	WhichDataInfo	Este atributo permite referenciar a los datos firmados para ello el valor será el mismo que el del atributo ID del componente "*afxp:DataInfo*" que contiene la información sobre los datos firmado.

8.2.1.2.19 <sigpol:VerifiedUnderSignaturePolicy>

VerifiedUnderSignaturePolicy	
Diagrama	
Descripción	Este elemento, definido en [DSS SIGPOL], especifica la política de firma utilizada en el proceso de verificación.

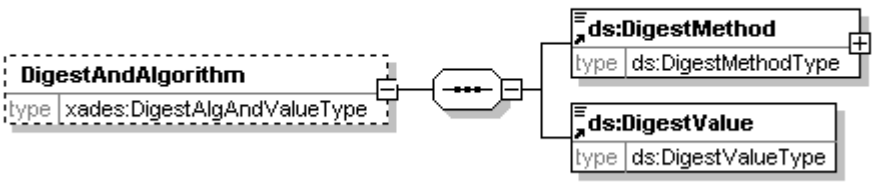
VerifiedUnderSignaturePolicy		
	Actualmente la plataforma sólo contempla las políticas de la AGE y Facturae. Este componente solamente se incluirá en la respuesta si la firma validada se ha generado en base a una política de firma soportada por el servidor.	
Namespace	urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#	
Hijos	Nombre	Descripción
	SignaturePolicy	Elemento que identifica la política utilizada.
	SignatureIdentifier	Componente que identifica la firma particular validada en base a la política especificada en el anterior componente. En esta implementación del perfil la respuesta no contendrá este elemento ya que la firma validada ya está identificada con el componente "*vr:SignatureIdentifier*" del elemento "*vr:IndividualSignatureReport*".

8.2.1.2.20 <sigpol:SignaturePolicy>

SignaturePolicy	
Diagrama	
Descripción	Componente que permite identificar la política de firma. Actualmente la plataforma sólo contempla las políticas de la AGE y Facturae.

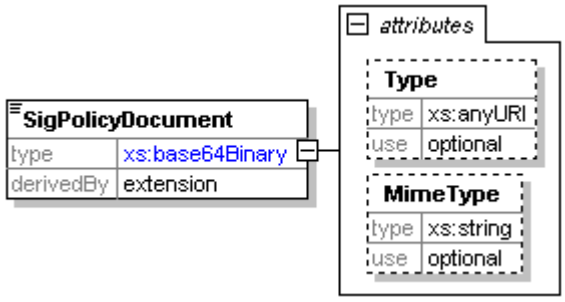
SignaturePolicy		
Namespace	urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#	
Hijos	Nombre	Descripción
	SignaturePolicyIdentifier	Elemento que contienen el identificador de la política de firma como URI. Las políticas de firmas pueden ser identificadas mediante URI u OID, en el caso de querer especificar una política cuyo identificador sea un OID este componente contendrá una URN construida con el valor del OID tal como se especifica en la RFC 3001. Por ejemplo: OID → 1.3.6.1.4.1.14862.1.6.2.1.2 URN → urn:oid:1.3.6.1.4.1.14862.1.6.2.1.2
	SignaturePolicyLocation	Este elemento contiene la localización del documento electrónico donde se describe la política de firma. Para esta implementación del perfil este elemento no está incluido en la respuesta de verificación.
	DigestAndAlgorithm	Elemento que contiene el resumen de la política de firma y el algoritmo utilizado para la realización del mismo.

8.2.1.2.21 <sigpol:DigestAndAlgorithm>

DigestAndAlgorithm	
Diagrama	

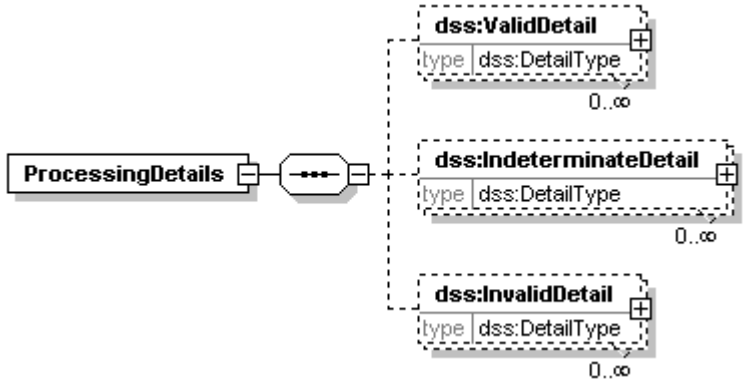
DigestAndAlgorithm		
Descripción	Elemento que contiene el resumen de la política de firma y el algoritmo utilizado para la realización del mismo.	
Namespace	urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#	
Hijos	Nombre	Descripción
	ds:DigestMethod	Componente que contiene el algoritmo de resumen utilizado. Se puede consultar una información detallada sobre este elemento en el apartado 8.2.1.1.8
	ds:DigestMethod	Componente que contiene el hash realizado en el algoritmo especificado en el anterior elemento. Se puede consultar una información detallada sobre este elemento en el apartado 8.2.1.1.9

8.2.1.2.22 <afxp:SigPolicyDocument>

SigPolicyDocument	
Diagrama	
Descripción	Componente que incluye el documento que especifica la política de firma codificado en Base 64. Para esta versión del perfil el documento devuelto coincide con el documento formal de la política.

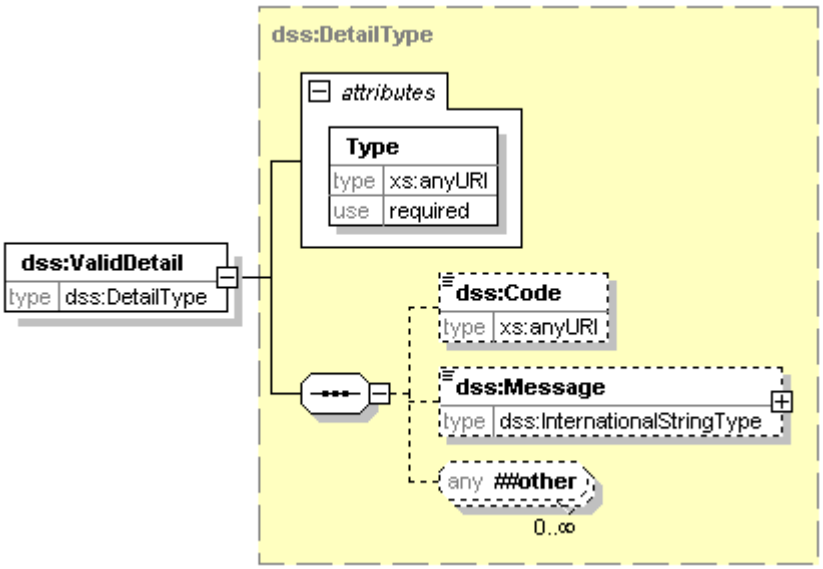
SigPolicyDocument		
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Atributos	Nombre	Descripción
	Type	Atributo que especifica el tipo de documento que se devuelve. En esta versión del perfil el servidor devolverá el documento formal de la política por lo que su valor será: urn:afirma:dss:1.0:profile:XSS:SigPolicyDocument :FormalDocument
	MimeType	Atributo que especifica el Mime Type del documento de la política. En esta implementación del perfil los documentos formales de la política solamente pueden ser de dos tipos: • application/octet-stream. Para políticas de firma implementadas en ASN.1 • text/xml. Para políticas de firma implementadas en formato XML.

8.2.1.2.23 <dss:ProcessingDetails>

ProcessingDetails	
Diagrama	
Descripción	Elemento que contiene el resultado de los distintos pasos que forman el proceso de

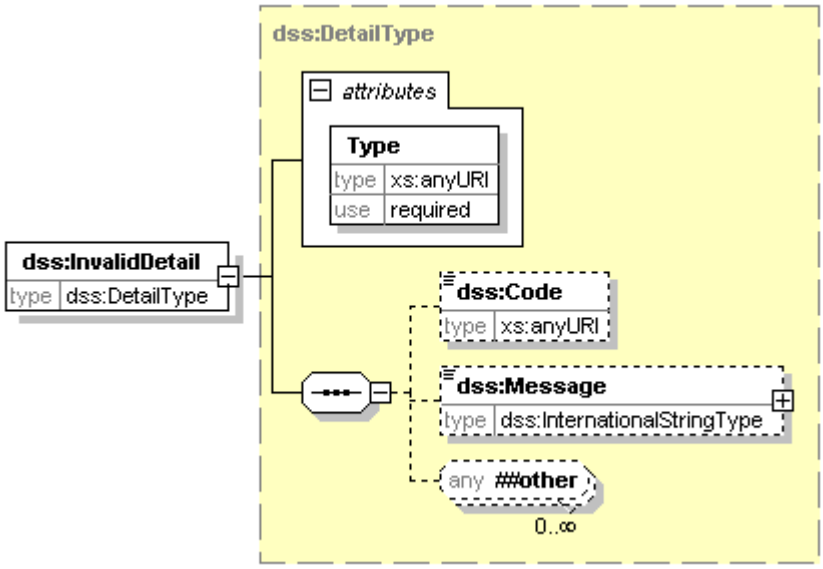
ProcessingDetails		
	verificación de una firma electrónica	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	ValidDetail	Componente que contiene una tarea de validación que ha arrojado un resultado satisfactorio.
	IndeterminateDetail	Componente que contiene una tarea de validación que ha arrojado un resultado indeterminado.
	InvalidDetail	Componente que contiene una tarea de validación que ha arrojado un resultado no satisfactorio.

8.2.1.2.24 <dss:ValidDetail>

ValidDetail	
Diagrama	
Descripción	Elemento que contiene la información asociada a una tarea de validación que arroja un resultado satisfactorio.

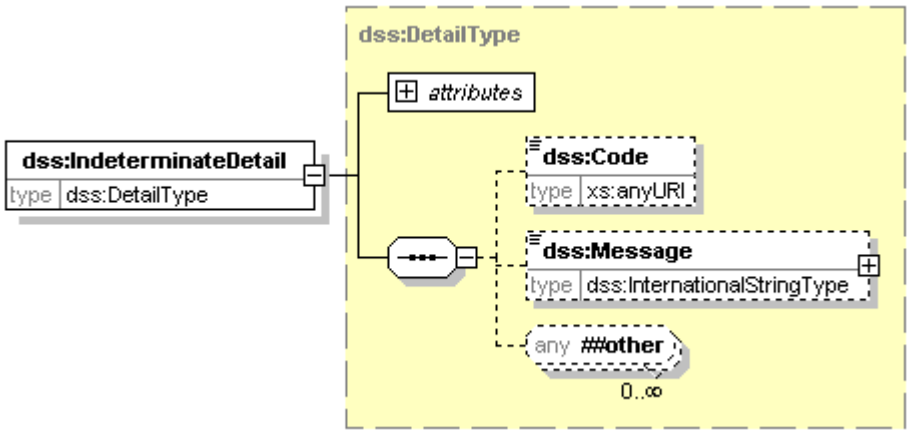
ValidDetail		
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	Code	URI que especifica el resultado anterior. En este perfil no se especifica valores para los casos de validación satisfactoria.
	Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	URI que identifica la tarea de validación ejecutada. En el anexo A.3.7 se detallan los valores posible para este atributo

8.2.1.2.25 <dss:InvalidDetail>

InvalidDetail	
Diagrama	
Descripción	Elemento que contiene la información asociada a una tarea de validación que arroja un

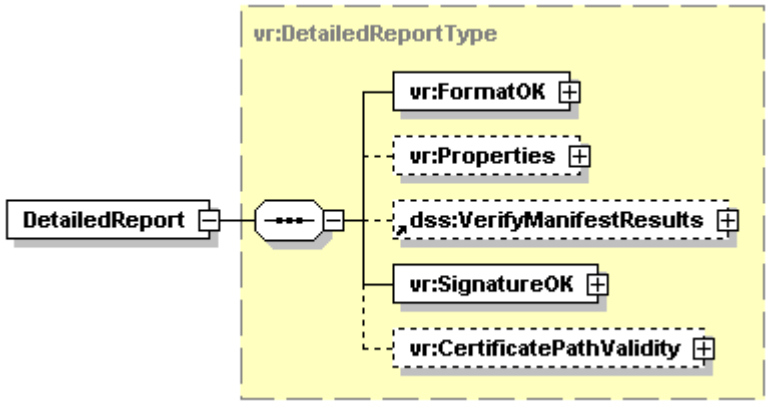
InvalidDetail		
	resultado no satisfactorio.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	Code	URI que especifica el motivo por el que el resultado no ha sido satisfactorio. En el anexo A.3.7 se detallan las URI´s que puede tomar como valor este elemento.
	Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	URI que identifica la tarea de validación ejecutada. En el anexo A.3.7 se detallan los valores posible para este atributo

8.2.1.2.26 <dss:IndeterminateDetail>

IndeterminateDetail	
Diagrama	
Descripción	Componente que contiene información sobre la ejecución de una tarea de validación que arroja un resultado indefinido.

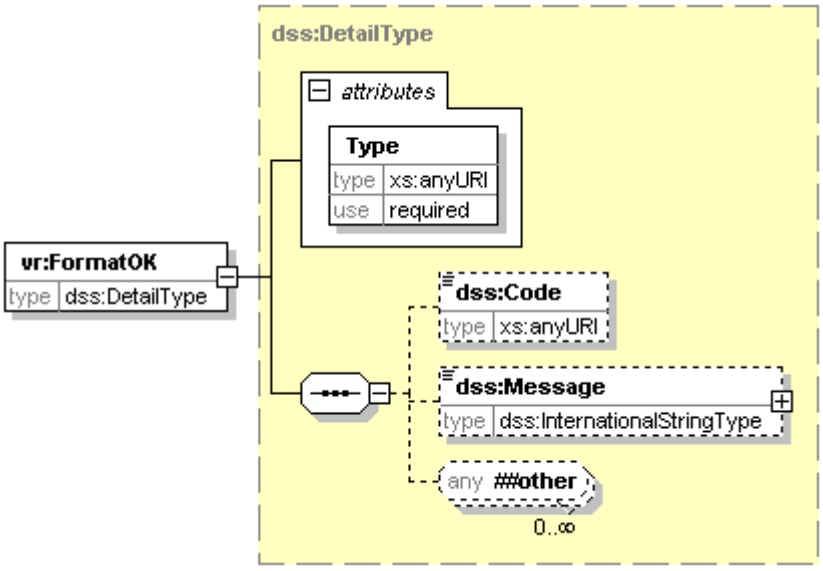
IndeterminateDetail		
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	Code	URI que especifica el resultado arrojado por la tarea. En el anexo A.3.7 se detallan las URI´s que puede tomar como valor este elemento.
	Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	URI que identifica la tarea de validación ejecutada. En el anexo A.3.7 se detallan los valores posible para este atributo

8.2.1.2.27 <vr:DetailedReport>

DetailedReport	
Diagrama	
Descripción	Contiene información adicional resultante del procesado de la firma. Únicamente será incluido en la respuesta si se especificó como valor de *vr:ReportDetailLevel* cualquier valor diferente a *urn:oasis:names:tc:dss:1.0:reportdetail:noDetails*

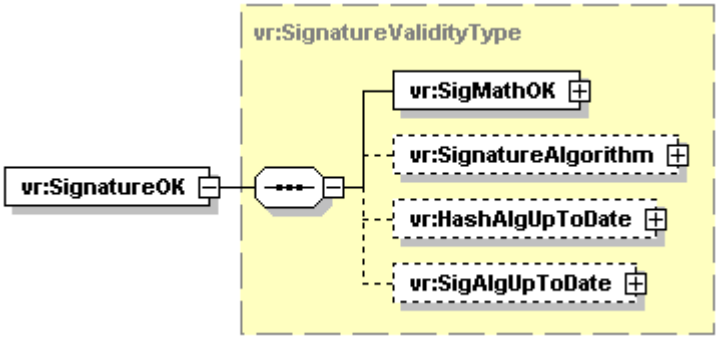
DetailedReport		
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	FormatOK	Especifica si el formato de la firma esta correcto.
	Properties	Contiene información sobre los atributos de firma contenidos en la firma validada. La inclusión de este elemento estará supeditada a que la petición haya incluido un elemento *afxp:AdditionalReportOption* Se puede consultar este elemnto en el apartado 8.2.1.2.47
	dss:VerifyManifestResults	Especifica el resultado de verificar los objetos *ds:Manifest* que pueda incluir la firma. La versión actual del perfil no contempla la inclusión de dicho elemento, al no realizar el sistema ninguna verificación sobre elementos *ds:Manifest*.
	SignatureOK	Contiene el resultado de validar la firma con la clave pública del certificado firmante, así como información sobre el modo de realización de la misma.
	CertificatePathValidity	Contiene información sobre el proceso de validación del certificado firmante así como otra información adicional.

8.2.1.2.28 <vr:FormatOK>

FormatOK		
Diagrama		
Descripción	Contiene el resultado de validar el formato de la firma electrónica.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	dss:Code	Especifica si el formato de la firma es correcto o no. Para más información acerca de los valores de URI que puede tomar este elemento, puede consultar el anexo A.3.8.
	dss:Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	Identificador de la tarea de validación del formato de la firma. Puede consultar los posibles valores para este atributo en

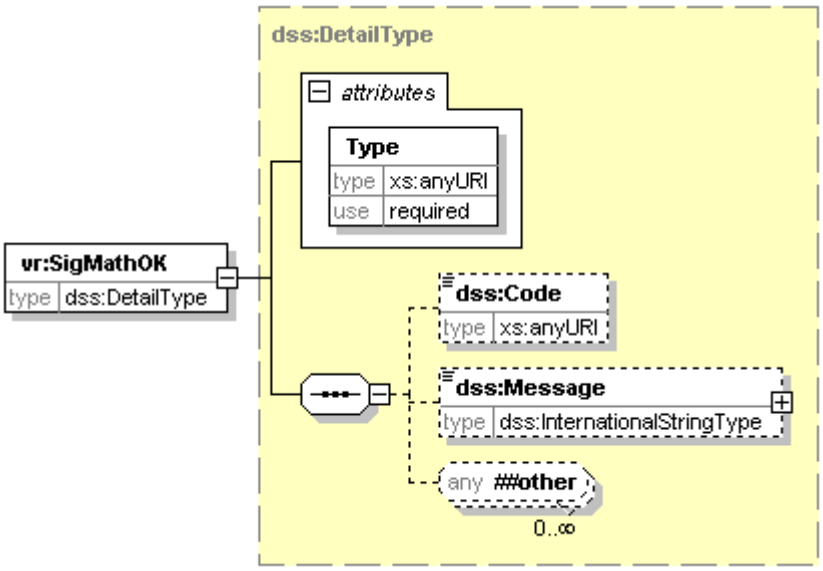
FormatOK		
		el anexo A.3.8.

8.2.1.2.29 <vr:SignatureOK>

SignatureOK		
Diagrama		
Descripción	Contiene el resultado de validar la firma con la clave pública del certificado firmante, así como información adicional sobre el modo de realización de la misma.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	SigMathOk	Especifica el resultado final de la verificación sobre el valor de la firma.
	SignatureAlgorithm	Contiene el algoritmo con el que se realizo la firma. En la versión actual del perfil no se contempla la inclusión de esta información.
	HashAlgUpToDate	Informa sobre la idoneidad del algoritmo de resumen utilizado. En la versión actual del perfil no se contempla la inclusión de esta información.

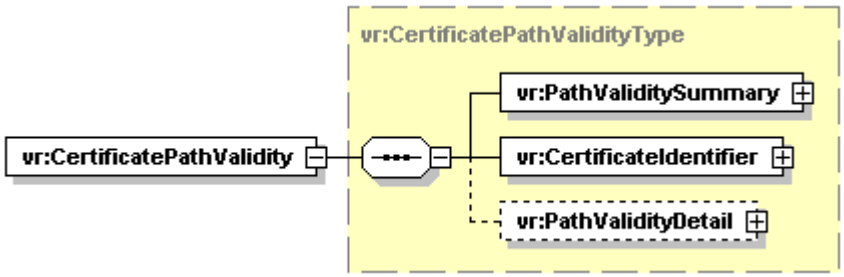
SignatureOK		
	SigAlgUpToDate	Informa sobre la idoneidad del algoritmo de firma utilizado. En la versión actual del perfil no se contempla la inclusión de esta información.

8.2.1.2.30 <vr:SigMathOk>

SigMathOk		
Diagrama		
Descripción	Especifica el resultado de validar la firma realizada con la clave pública del certificado firmante.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	dss:Code	Contiene el resultado de la validación sobre el SignatureValue. Puede obtener más información acerca de los valores que puede tomar este elemento en el anexo A.3.9

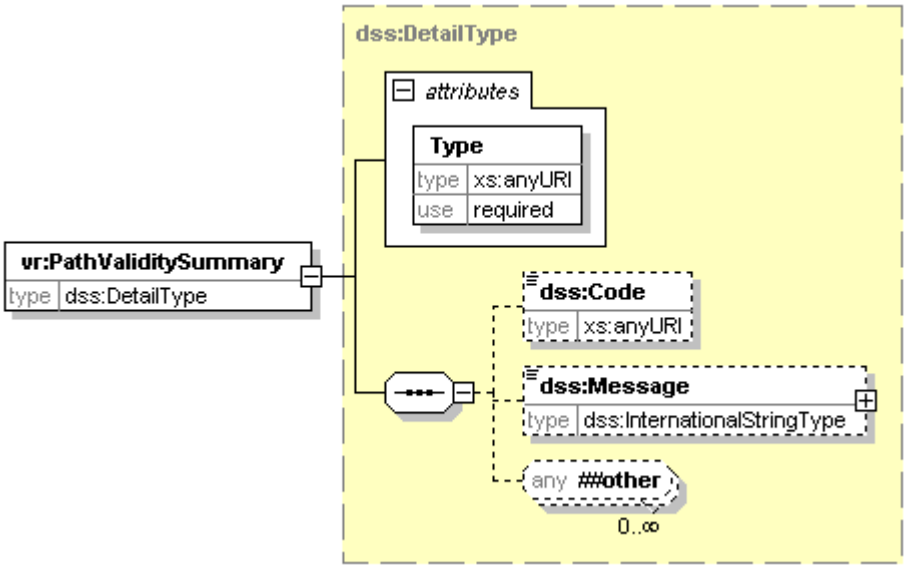
SigMathOk		
	dss:Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	Identificador de la tarea de validación del formato de la firma. Puede consultar los posibles valores para este atributo en el anexo A.3.9.

8.2.1.2.31 <vr:CertificatePathValidity>

CertificatePathValidity		
Diagrama		
Descripción	Contiene información asociada a la validación del certificado firmante.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	PathValiditySummary	Especifica el resultado global de la validación del certificado
	CertificateIdentifier	Identifica el certificado concreto.
	PathValidityDetail	Contiene información adicional sobre la validación del certificado. Este elemento será incluido en la respuesta si es solicitado en

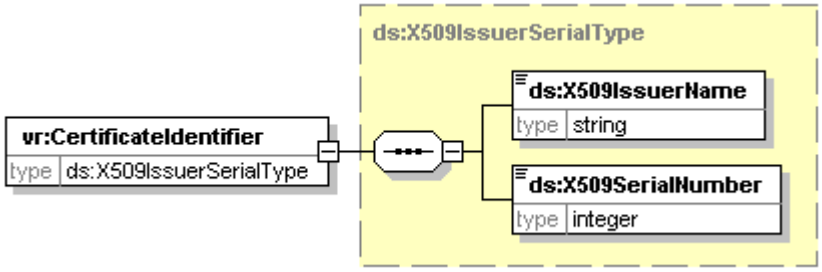
CertificatePathValidity		
		la petición, por medio de la inclusión del elemento *vr:ReportDetailLevel* con el valor ***urn:oasis:names:tc:dss:1.0:reportdetail:allDetails*** y del elemento afxp:ReturnReadableCertificateInfo

8.2.1.2.32 <vr:PathValiditySummary>

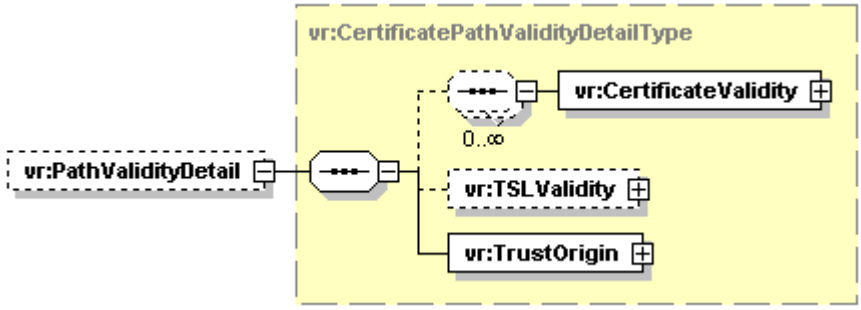
PathValiditySummary		
Diagrama		
Descripción	Especifica el resultado global de verificar el certificado firmante.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	dss:Code	Especifica si la tarea de verificación del certificado firmante ha sido satisfactoria. En el caso de validación satisfactoria el valor devuelto será: urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:Valid En caso contrario, el sistema devolverá un error, según se

PathValiditySummary		
		define en el anexo A.3.10.
	dss:Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	Identificador de la tarea de validación. El valor de este atributo será: urn:afirma:dss:1.0:profile:XSS:detail:Certificate

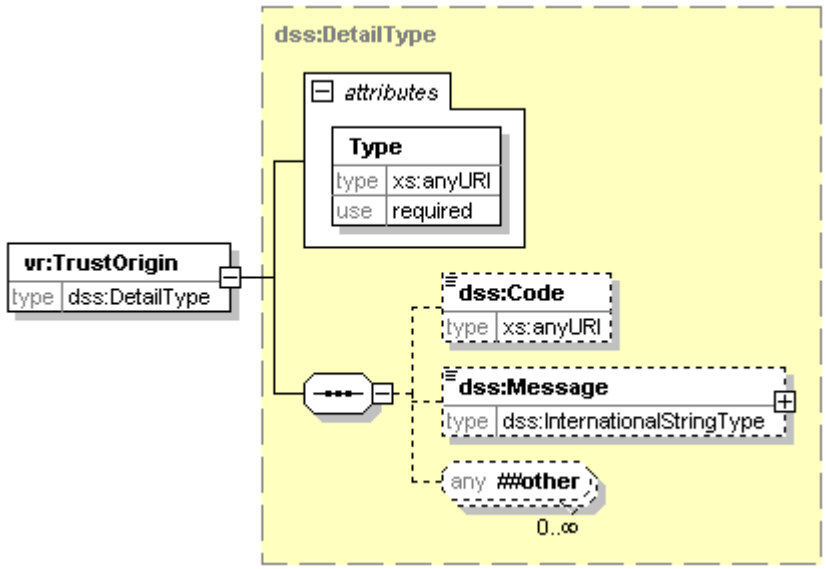
8.2.1.2.33 <vr:CertificateIdentifier>

CertificateIdentifier		
Diagrama		
Descripción	Especifica el identificador de un certificado que forma parte de la firma.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	ds:X509IssuerName	Contiene el campo *IssuerName* del certificado.
	ds:X509SerialNumber	Contiene el campo *SerialNumber* del certificado.

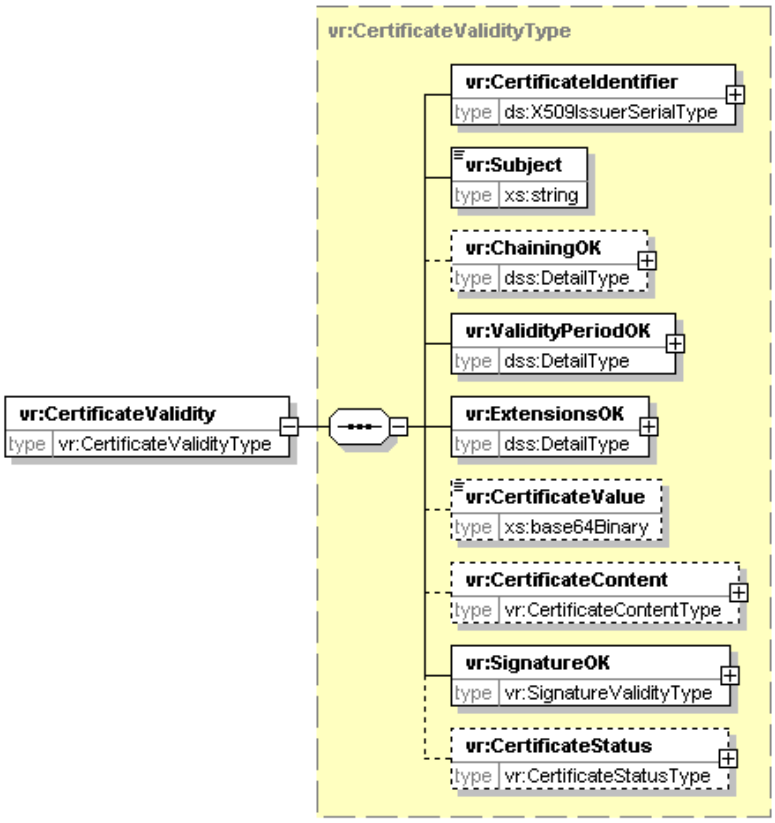
8.2.1.2.34 <vr:PathValidityDetail>

CertificateIdentifier		
Diagrama		
Descripción	Contiene información adicional sobre la validación del certificado. Este elemento únicamente se incluirá en la respuesta si es solicitado explícitamente en la petición mediante la inclusión del elemento *vr:ReportDetailLevel*, con el valor: ***urn:oasis:names:tc:dss:1.0:reportdetail:allDetails*** y del elemento afxp:ReturnReadableCertificateInfo	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	CertificateValidity	Por cada certificado que forma la cadena de certificación se incluye un elemento "*vr:CertificateValidity*" el cual proporciona información sobre la verificación del mismo.
	TSLValidity	Contiene información adicional sobre la TSL (Trust-Service List) en la que se encuentra incluido el certificado. La implementación actual no contempla el uso de este elemento, aunque no se descarta su introducción en implementaciones futuras.
	TrustOrigin	Informa acerca del método utilizado por el sistema para almacenar de forma confiable los certificados de la CA del certificado firmante.

8.2.1.2.35 <vr:TrustOrigin>

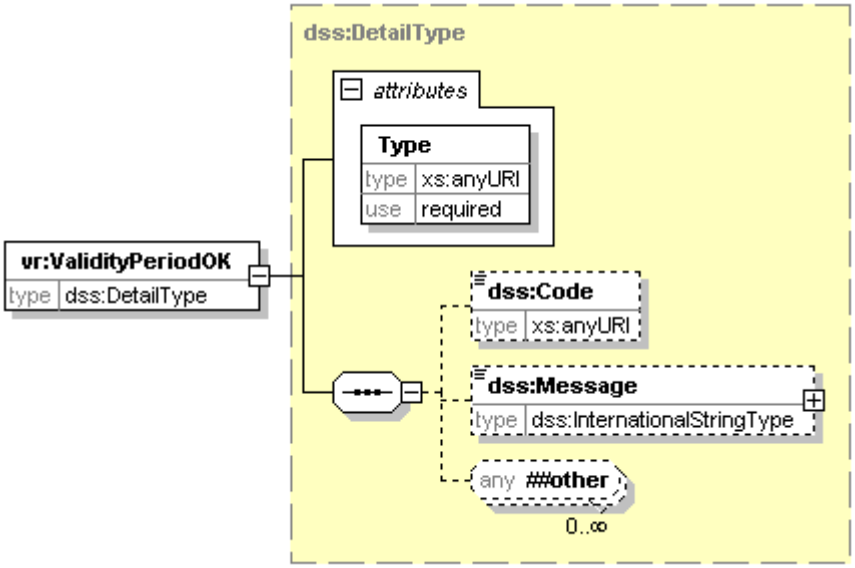
TrustOrigin		
Diagrama		
Descripción	Informa acerca del método utilizado por el sistema para almacenar de forma confiable los certificados de la CA del certificado firmante.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	dss:Code	No se definen valores para este elemento en el perfil actual.
	dss:Message	Cadena literal que contiene información acerca del método de almacenamiento.
Atributos	Nombre	Descripción
	Type	Identificador del método de almacenamiento utilizado. El valor por defecto utilizado por el sistema es: ***urn:oasis:names:tc:dss:1.0:trustorigin:certDataBase***.

8.2.1.2.36 <vr:CertificateValidity>

CertificateValidity		
Diagrama		
Descripción	Devuelve información sobre un certificado que ha sido validado.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	CertificateIdentifier	Identificador del certificado. Se puede obtener mas información sobre este componente en el apartado 8.2.1.2.33
	Subject	Especifica el campo *Subject* del certificado validado.
	ChainingOK	Indica si el certificado previo en la cadena de certificación es válido. La implementación actual no devuelve este elemento, aunque

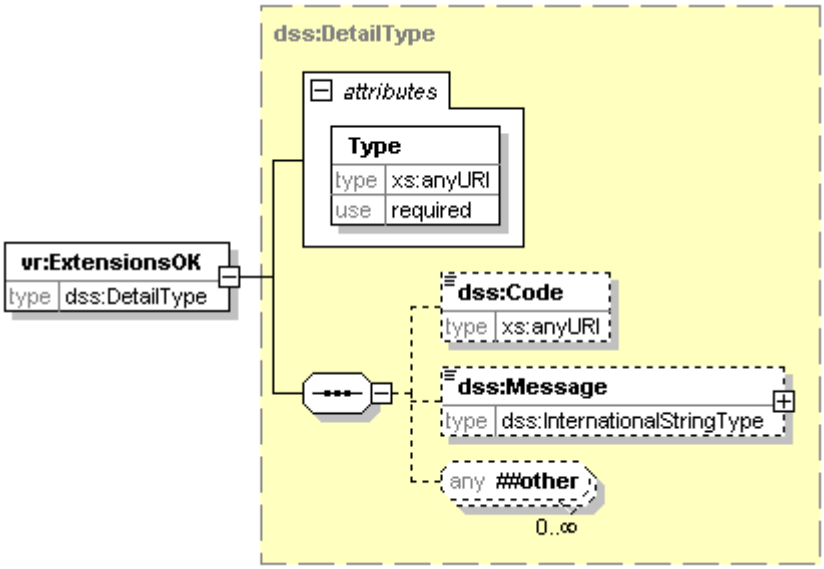
CertificateValidity		
		no se descarta su inclusión futura.
	ValidityPeriodOK	Indica si el certificado era válido en el instante de tiempo en el cual fue validado.
	ExtensionsOK	Indica si existen extensiones no válidas en el certificado.
	CertificateValue	Devuelve el certificado en codificación Base64. Este elemento únicamente se incluirá en la respuesta de validación si la petición incluía un elemento del tipo *vr:IncludeCertificateValues*, con el valor *true* y el elemento *ReportDetailLevel* con el nivel de detalle *"NoPathDetails"* o *"AllDetails"*
	CertificateContent	Incluye una representación en XML sobre la información contenida en el certificado**.** El sistema no emplea este elemento para devolver información sobre el certificado. Para obtener información sobre el certificado, se incluye el elemento *afxp:ReadableCertificateInfo.*
	SignatureOK	Contiene el resultado del proceso de validación de la firma del certificado.
	CertificateStatus	Contiene información adicional sobre el estado del certificado.

8.2.1.2.37 <vr:ValidityPeriodOK>

ValidityPeriodOK		
Diagrama		
Descripción	Indica si el certificado específico era válido en un instante de tiempo. La validez del certificado en este sentido se refiere a si se encontraba entre sus fechas de comienzo y fin de validez, con independencia de su estado de revocación. En un proceso de validación de una firma, dicho instante de tiempo dependerá de si la firma incorpora un sello de tiempo, o un atributo del tipo SigningTime, que permita aproximar la fecha y hora en la que se llevó a cabo.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	dss:Code	Detalla el resultado del proceso. Los valores que puede tener este componente son: - Periodo válido: "**ValidPeriod**" - Certificado caducado: "**Expired**" - Certificado aun no válido: "**NotValidYet**"

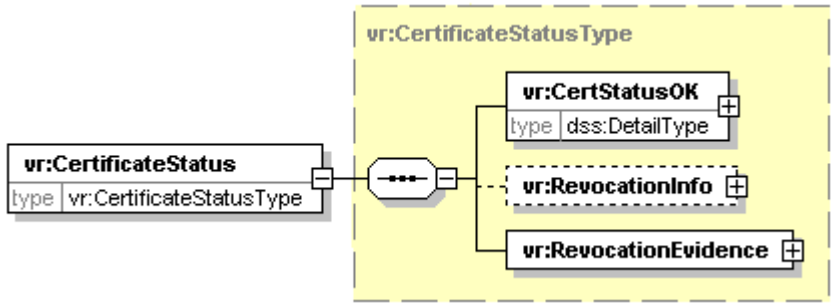
ValidityPeriodOK		
		- No se ha podido verificar: "**UnknownStatusPeriod**" En todos los casos el identificador irá precedido por la cadena "**urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:**"
	dss:Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	Identificador de la tarea realizada. En este caso: urn:afirma:dss:1.0:profile:XSS:detail:Certificate.

8.2.1.2.38 <vr: ExtensionsOK>

ExtensionsOk	
Diagrama	
Descripción	Indica si las extensiones incluidas en el certificado son válidas
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#

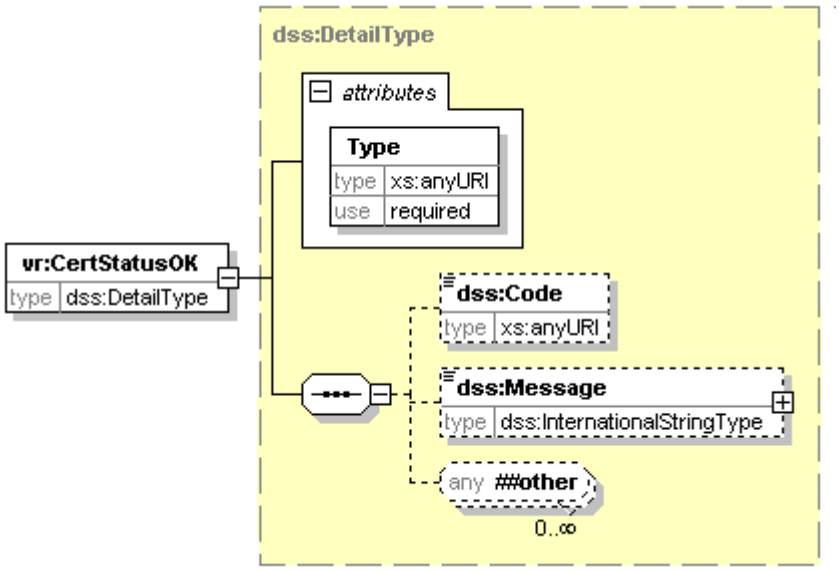
ExtensionsOk		
Hijos	Nombre	Descripción
	dss:Code	Especifica si las extensiones del certificado son válidas. Se puede dar los siguientes valores: - Todas las extensiones válidas: "**ValidExtension**" - Alguna extensión no valida: "**InvalidExtension"** - No se ha podido verificar:"**UnknownStatusExtensions**" En todos los casos los identificadores irán precedido de la cadena "**urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:**"
	dss:Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	Identificador de la tarea realizada. En este caso: urn:afirma:dss:1.0:profile:XSS:detail:Certificate.

8.2.1.2.39 <vr:CertificateStatus>

CertificateStatus	
Diagrama	

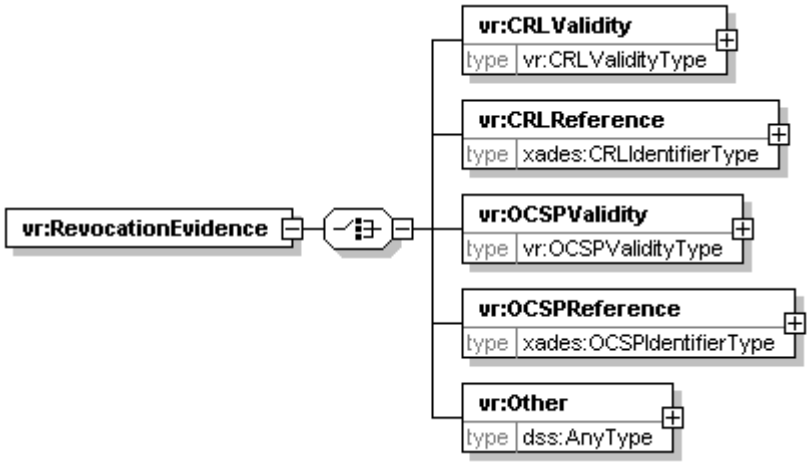
CertificateStatus		
Descripción	Este componente está destinado a recoger la información asociada a la validación del estado de revocación de un certificado.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	vr:CertStatusOK	Elemento que recoge el resultado final de la validación del estado de revocación
	vr:RevocationInfo	Componente que añade información adicional sobre la verificación del estado de revocación del certificado. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
	vr:RevocationEvidence	Elemento que recoge las evidencias del estado de revocación utilizadas en la verificación.

8.2.1.2.40 <vr:CertStatusOK>

CertStatusOK	
Diagrama	

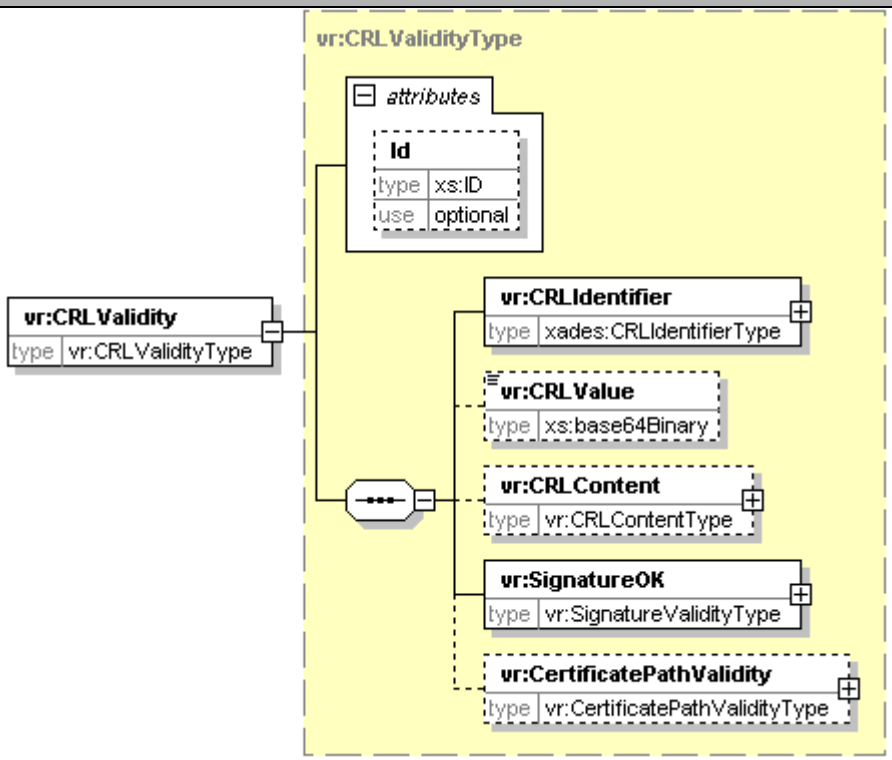
CertStatusOK		
Descripción	Elemento que recoge el resultado final de la validación del estado de revocación	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	dss:Code	Elemento que especifica el resultado de validar el estado de revocación del certificado. Los valores posibles de este componente son: - Estado de revocación válido: "**ValidStatus**" - Estado revocado: "**Revoked"** - Certificado en observación:"**OnHoldStatus**" - No se ha podido determinar el estado del certificado: **"UnknownStatus"** En todos los casos los identificadores irán precedido de la cadena "**urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:**"
	dss:Message	Cadena literal con un mensaje descriptivo del resultado del proceso.
Atributos	Nombre	Descripción
	Type	Identificador de la tarea realizada. En este caso: urn:afirma:dss:1.0:profile:XSS:detail:Certificate.

8.2.1.2.41 <vr:RevocationEvidence>

RevocationEvidence		
Diagrama		
Descripción	Elemento que recoge las evidencias del estado de revocación utilizadas en la verificación.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	vr:CRLValidity	Elemento que contiene información sobre la CRL utilizada para validar el certificado.
	vr:CRLReference	Elemento que contiene una referencia de la CRL utilizada para validar el certificado. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
	vr:OCSPValidity	Elemento que recoge la respuesta OCSP utilizada en la verificación del certificado.
	vr:OCSPReference	Elemento que recoge una referencia de la respuesta OCSP utilizada para validar el certificado La implementación actual no devuelve este elemento,

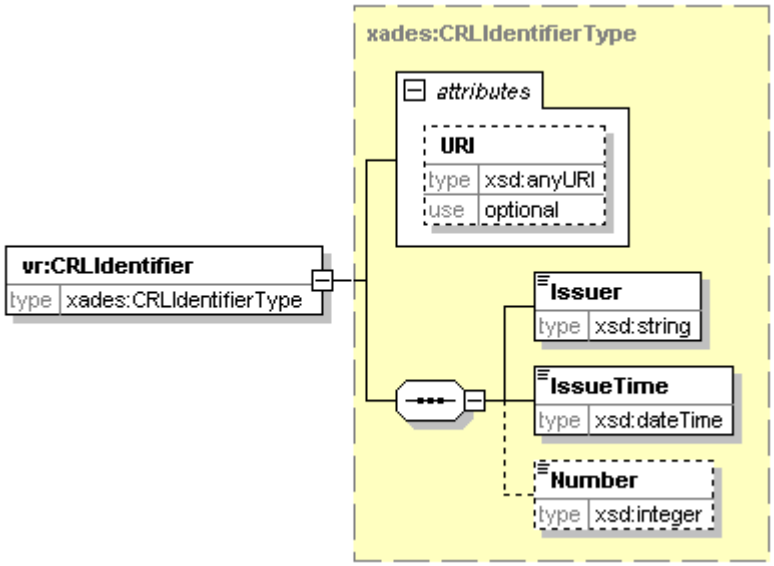
RevocationEvidence		
		aunque no se descarta su inclusión futura.
	vr:Other	Componente diseñado para recoger otra implementación. Este perfil no añade implementación adicional para este elemento.

8.2.1.2.42 <vr:CRLValidity>

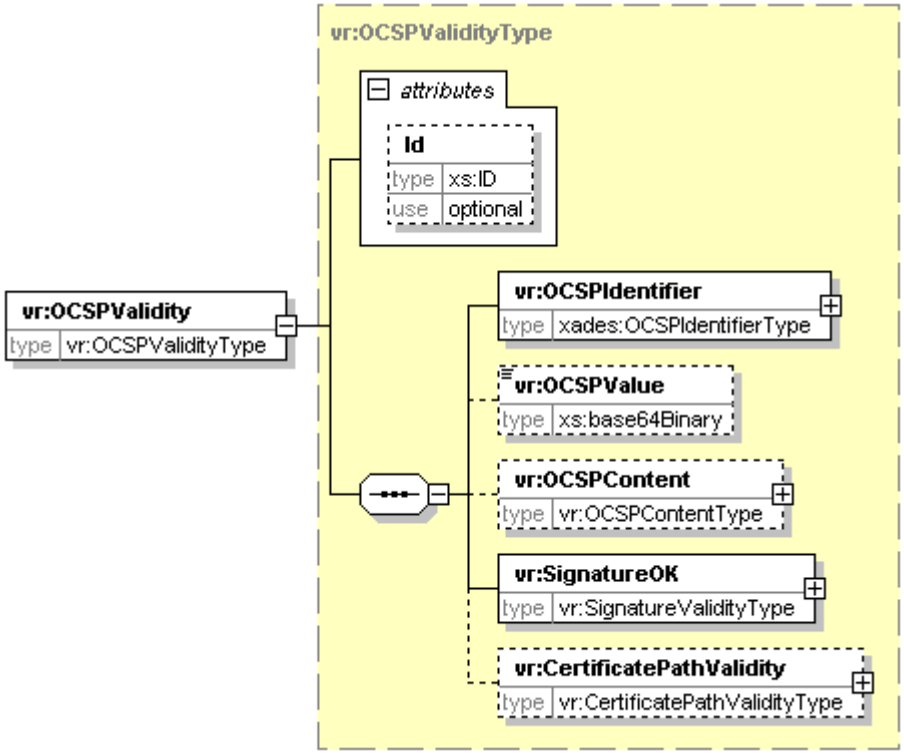
CRLValidity		
Diagrama		
Descripción	Componente que recoge información sobre la CRL utilizada en la validación del certificado.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción

CRLValidity		
	vr:CRLIdentifier	Elemento que recoge el identificador de la CRL utilizada.
	vr:CRLValue	Componente que contiene la CRL utilizada. Este elemento únicamente se incluirá en la respuesta de validación si la petición incluía un elemento del tipo *vr:IncludeRevocationValues*, con el valor *true*.
	vr:CRLContent	Este elemento contiene una representación XML de la CRL utilizada. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
	vr:SignatureOK	Elemento que recoge el resultado de validar la firma de la CRL. Podemos obtener información sobre este componente en el apartado 8.2.1.2.29
	vr:CertificatePathValidity	Componente que recoge la cadena de certificación del certificado firmante de la CRL. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
Atributos	Nombre	Descripción
	ID	Atributo que contiene un identificador del elemento.

8.2.1.2.43 <vr:CRLIdentifier>

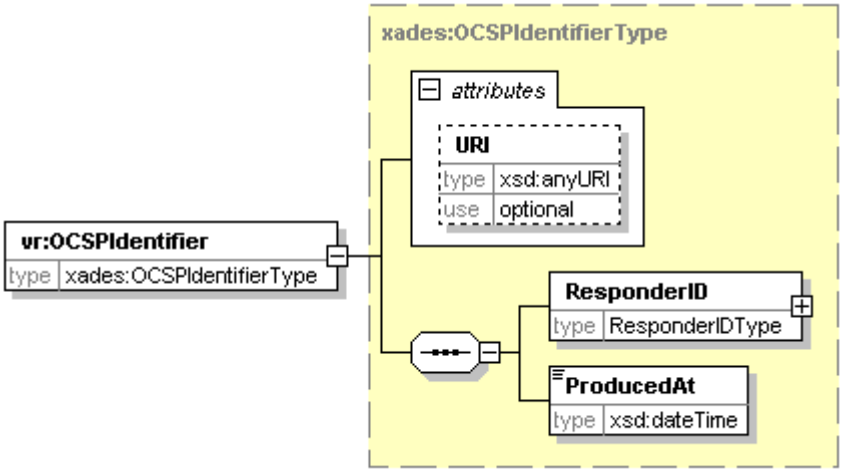
CRLIdentifier		
Diagrama		
Descripción	Componente que identifica la CRL utilizada.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	xades:Issuer	Elemento que recoge el emisor de la CRL.
	xades:IssuerTime	Elemento que contiene la fecha de emisión de la CRL.
	xades:Number	Este componente incluye el número de la CRL
Atributos	Nombre	Descripción
	URI	Atributo que indicar dónde se ha publicado la CRL. La implementación actual no devuelve este atributo, aunque no se descarta su inclusión futura.

8.2.1.2.44 <vr:OCSPValidity>

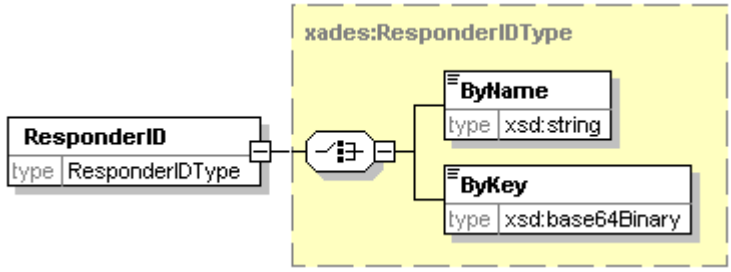
OCSPValidity		
Diagrama		
Descripción	Componente que recoge información sobre la respuesta OCSP utilizada en la validación del certificado.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	vr:OCSPIdentifier	Elemento que recoge el identificador de la respuesta OCSP utilizada.
	vr:OCSPValue	Elemento que contiene la respuesta OCSP. Este elemento únicamente se incluirá en la respuesta de validación si la petición incluía un elemento del tipo *vr:IncludeRevocationValues*, con el valor *true*.

OCSPValidity		
	vr:OCSPContent	Este elemento contiene una representación XML de la respuesta OCSP utilizada. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
	vr:SignatureOK	Elemento que recoge el resultado de validar la firma de la respuesta OCSP. Podemos obtener información sobre este componente en el apartado 8.2.1.2.29
	vr:CertificatePathValidity	Componente que recoge la cadena de certificación del certificado firmante de la respuesta OCSP. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
Atributos	Nombre	Descripción
	ID	Atributo que contiene un identificador del elemento.

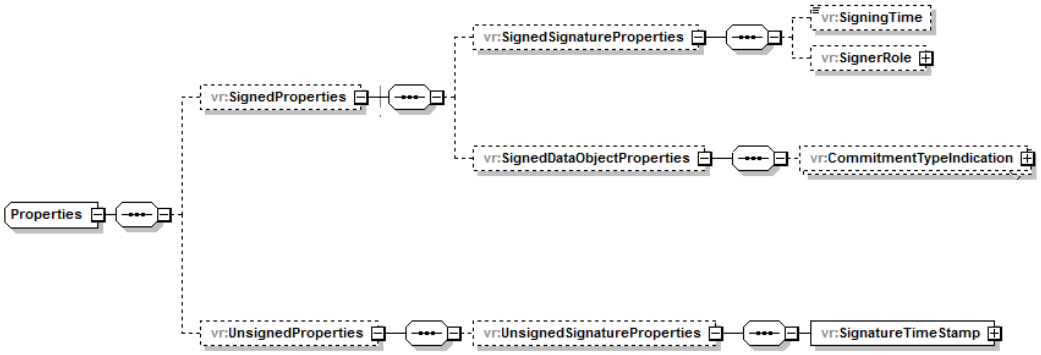
8.2.1.2.45 <vr:OCSPIdentifier>

OCSPIdentifier		
Diagrama		
Descripción	Componente que identifica la respuesta OCSP obtenida.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	xades:ResponderID	Elemento que informa sobre el campo “ResponderID” incluido en la respuesta OCSP
	xades:ProducedAt	Fecha de generación de la respuesta.
Atributos	Nombre	Descripción
	URI	Atributo que indicar dónde se ha publicado el servicio OCSP. La implementación actual no devuelve este atributo, aunque no se descarta su inclusión futura.

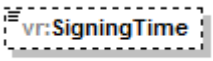
8.2.1.2.46 <xades:ResponderId>

ResponderId		
Diagrama		
Descripción	Componente que recoge el valor del atributo “ResponderID” contenido en la respuesta OCSP.	
Namespace	http://uri.etsi.org/01903/v1.3.2#"	
Hijos	Nombre	Descripción
	xades:ByName	Elemento que recoge el valor del campo “ByName” de la respuesta OCSP.
	xades:ByKey	Elemento que recoge el valor del campo “ByKey” de la respuesta OCSP.

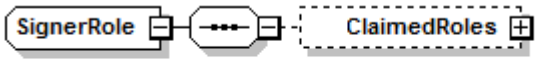
8.2.1.2.47 <vr:Properties>

Properties	
Diagrama	
Descripción	Contiene información obtenida durante el proceso de verificación sobre los atributos firmados y no firmados presentes en la firma. La inclusión de estos elemento estará supeditada a que la petición haya incluido un elemento *afxp:AdditionalReportOption*
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#

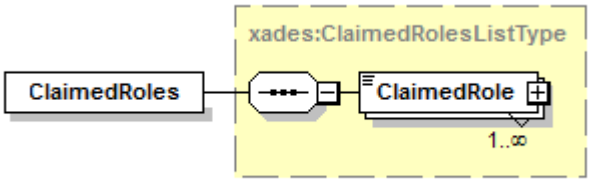
8.2.1.2.48 <vr:SigningTime>

SigningTime	
Diagrama	
Descripción	Contiene el instante de tiempo en el que el firmante afirma haber realizado la proceso de firma. El formato de la fecha será UTC.
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#

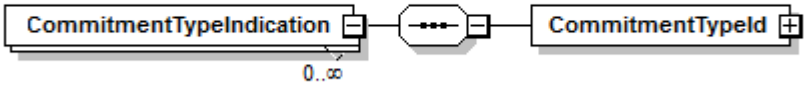
8.2.1.2.49 <vr:SignerRole>

SignerRole		
Diagrama		
Descripción	Contiene los roles asumidos por el firmante en la creación de la firma.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	ClaimedRoles	Elemento que contiene una secuencia de roles asumidos por el firmante pero no certificados.

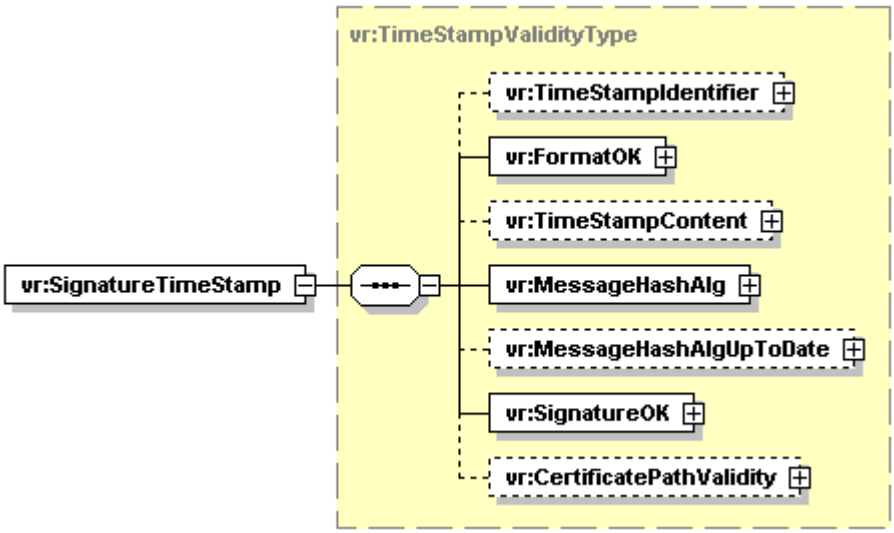
8.2.1.2.50 <xades:ClaimedRoles>

ClaimedRoles		
Diagrama		
Descripción	Contiene una secuencia de roles asumidos por el firmante pero no certificados.	
Namespace	http://uri.etsi.org/01903/v1.3.2#"	
Hijos	Nombre	Descripción
	ClaimedRole	Elemento que representa un rol asumido por el firmante pero no certificado.

8.2.1.2.51 <xades:CommitmentTypeIndication>

CommitmentTypeIndication		
Diagrama		
Descripción	Contiene el compromiso asumido por el firmante en la firma de datos firmados en el contexto de la política de firma seleccionada (cuando se está utilizando un compromiso explícito).	
Namespace	http://uri.etsi.org/01903/v1.3.2#"	
Hijos	Nombre	Descripción
	CommitmentTypeId	Elemento que identifica unívocamente el compromiso asumido por el firmante.

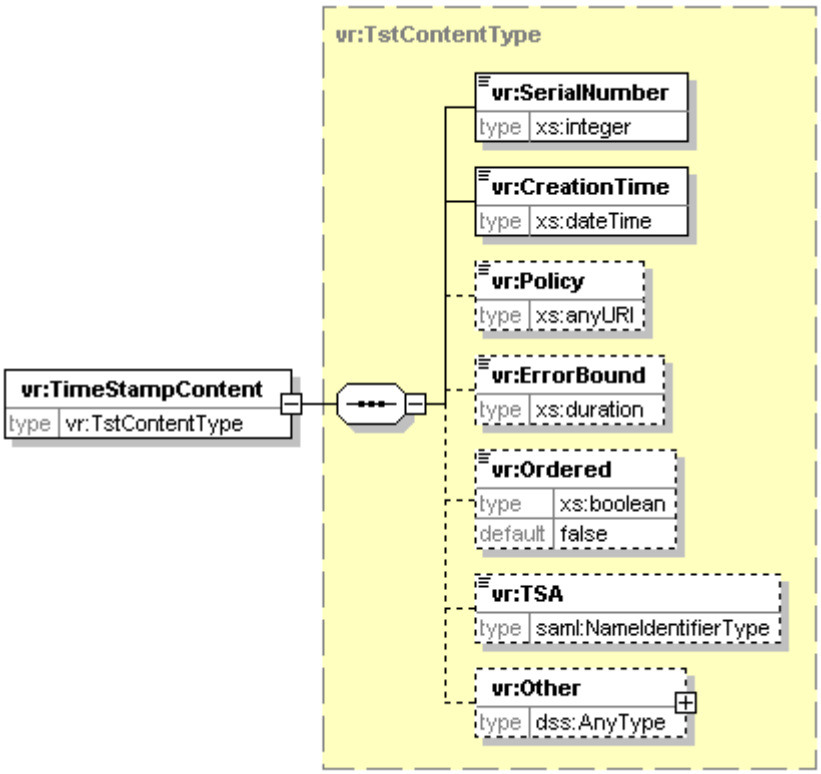
8.2.1.2.52 <vr:SignatureTimeStamp>

SignatureTimeStamp	
Diagrama	

SignatureTimeStamp		
Descripción	Contiene información asociada al atributo *SignatureTimeStamp* que se ha obtenido durante la verificación de la firma.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	TimeStampIdentifier	Identificador del Sello de Tiempo. La implementación actual no devuelve ningún identificador para el sello de tiempo.
	FormatOK	Contiene el resultado de validar el formato de la firma del Sello de Tiempo. Podemos obtener información detallada de este componente en el apartado 0
	TimeStampContent	Componente que recoge algunos de los campos contenidos en el Sello de Tiempo
	MessageHashAlg	Especifica el algoritmo de resumen utilizado para la creación de la firma del Sello de Tiempo
	MessageHashAlgUpToDate	Componente que informa sobre la idoneidad del algoritmo de hash utilizado. Este elemento no es soportado por la implementación actual.
	SignatureOK	Recoge el resultado de validar la firma del Sello de Tiempo. Podemos obtener información detallada de este componente en el apartado 8.2.1.2.29
	CertificatePathValidity	Especifica el resultado del proceso de validación del certificado firmante utilizado por la TSA para la

SignatureTimeStamp		
		generación del Sello de Tiempo. Podemos obtener información detallada de este componente en el apartado 8.2.1.2.31

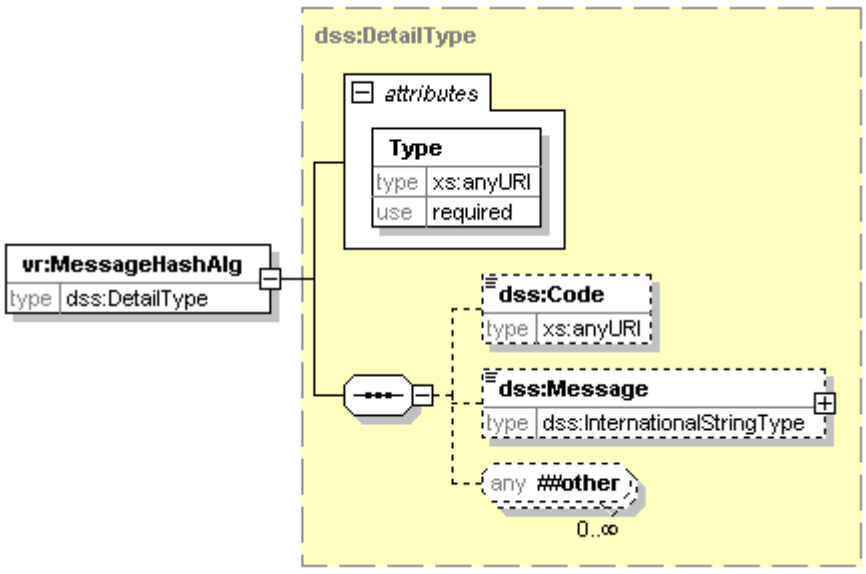
8.2.1.2.53 <vr:TimeStampContent>

TimeStampContent		
Diagrama		
Descripción	Devuelve el valor de los campos más relevantes contenidos en el Sello de Tiempo.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	SerialNumber	Número de serie generado por la TSA.

TimeStampContent		
	CreationTime	Fecha y hora de creación del Sello de Tiempo. La fecha se devuelve en el siguiente formato: YYYY-MM-DDThh:mm:ss.SSSTZD Donde: YYYY – Cuatro dígitos correspondientes al año. MM – Dos dígitos correspondientes al mes DD – Dos dígitos correspondientes al día del mes hh – Dos dígitos correspondientes a la hora (del 00 al 23) mm - Dos dígitos correspondientes a los minutos (del 00 al 59) ss - Dos dígitos correspondientes a los segundos (del 00 al 59) SSS – Tres dígitos correspondientes a milésima de segundos. TZD – Zona horaria (Z ó +hh:mm ó -hh:mm)
	Policy	Identifica la política bajo la que se generó el Sello de Tiempo. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
	ErrorBound	Recoge información de la TSA acerca del desfase máximo estimado entre la hora real y la detallada en el sello de tiempo. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
	Ordered	Detalla si la fecha de creación se ajusta a la política bajo la cual se ha generado el Sello de Tiempo. La implementación actual no devuelve este elemento, aunque no se

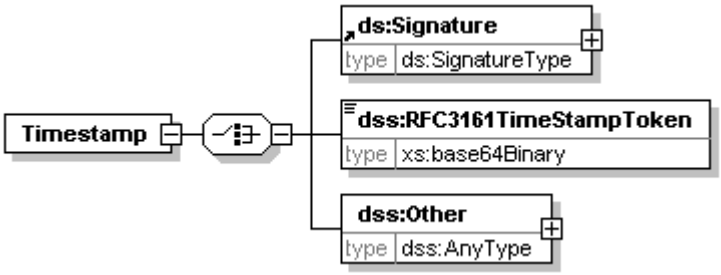
TimeStampContent		
		descarta su inclusión futura.
	TSA	Nombre de la TSA. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
	Other	Elemento definido para incluir nuevos detalles en futuras implementaciones. Este perfil contempla la posibilidad de incluir en este elemento un componente "*dss:Timestamp*" (ver apartado 8.2.1.2.55) con el Sello de Tiempo validado en la firma. Solamente se incluirá el Sello de Tiempo en la respuesta si se solicito en la petición mediante el componente "*afxp:AdditionalReportOption*"

8.2.1.2.54 <vr:MessageHashAlg>

MessageHashAlg	
Diagrama	
Descripción	Especifica el algoritmo de hash o resumen utilizado en la generación del Sello de

MessageHashAlg		
	Tiempo.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	dss:Code	Contiene el algoritmo de hash utilizado en la generación del Sello de Tiempo. Los valores que puede tomar se definen en el anexo A.3.4. En caso de algoritmos no soportados, se retornará el valor: urn:afirma:dss:1.0:profile:XSS:detail:MessageHashAlg:code:Unknown
	dss:Message	Cadena literal con el resultado del proceso.
Atributos	Nombre	Descripción
	Type	Identificador de la operación realizada. En este caso: urn:afirma:dss:1.0:profile:XSS:detail:MessageHashAlg

8.2.1.2.55 <dss:Timestamp>

Timestamp	
Diagrama	
Descripción	Componente definido en las especificaciones [DDS Core] que permite incluir un Sello de Tiempo.

Timestamp		
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	ds:Signature	Elemento que recoge un XML TimeStampToken. La implementación actual no devuelve este elemento, aunque no se descarta su inclusión futura.
	dss: RFC3161TimeStampToken	Elemento que recoge un TimeStampToken según las especificaciones RFC 3161
	dss:Other	Elemento destinado a recoger nuevas implementaciones DSS para incluir Sello de Tiempo. No se contemplan en estas especificaciones nuevas implementaciones para este componente.

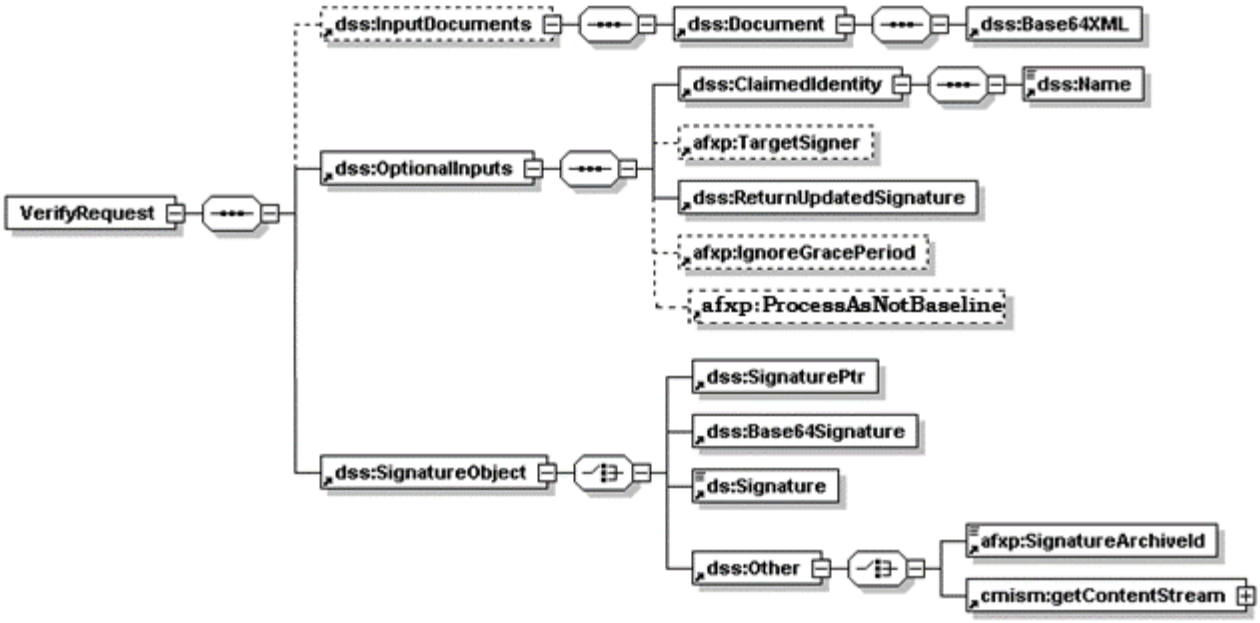
8.2.2 Upgrade de Firmas

En los siguientes apartados analizaremos la mensajería XML utilizada para la realización de procesos de actualización o upgrade de firmas.

8.2.2.1 Mensajería XML de Petición

En la figura a continuación se detalla la estructura de una petición de upgrade de firma. Su estructura es similar a la de una petición de verificación de firma, con las siguientes salvedades:

- La adición de elementos como *dss:ReturnUpdateSignature,* que indicará al sistema que se desea actualizar la firma y el formato al que se desea extender.
- La no inclusión de elementos explícitos del proceso de validación de una firma (*Base64Data* , *DocumentHash, afxp:ReturnReadableCertificateInfo, etc.)*



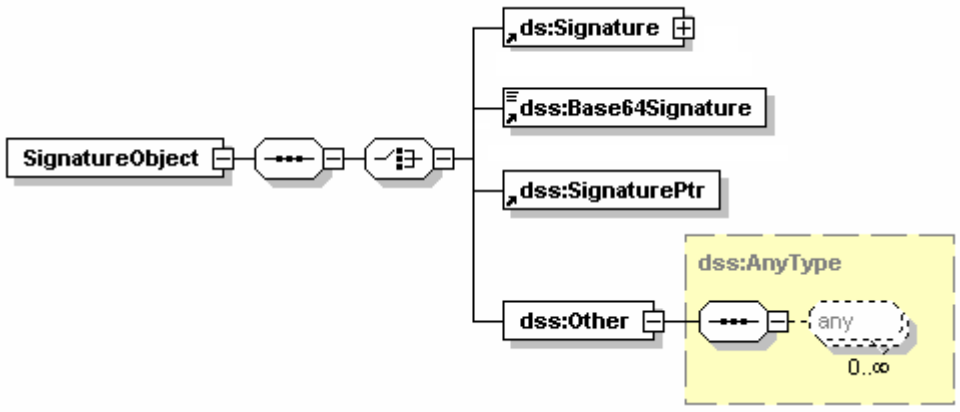
A continuación, se detallan los elementos que conforman la petición. Para obtener información acerca de los elementos comunes con el servicio de validación de firma y que no vengan detallados aquí, puede consultar el apartado 8.2.1.1

8.2.2.1.1 <dss:SignatureObject>

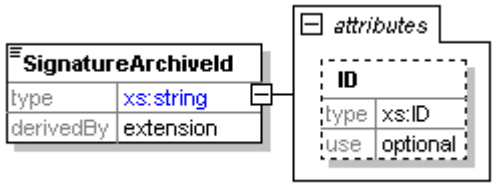
Este componente debe contener la firma que se desea actualizar o un identificador de registro que permita al servidor recuperarla.

En el apartado 8.1.1.2.4 se puede apreciar con mayor detalle el contenido de este componente.

8.2.2.1.2 <dss:SignatureObject>/<dss:Other>

SignatureObject / Other	
Diagrama	
Descripción	El elemento *Other* definido por OASIS esta destinado a soportar otras implementaciones futuras no recogidas en [DSS Core]. Para aquellos casos en los que no se desea incluir la firma en la petición, la implementación actual define dos posibles elementos que puede contener este componente: ▪ afxp:SignatureArchiveId. Elemento que permitirá especificar el identificador de una transacción de firma, para aquellos casos en los que se desee que la firma sea recuperada del sistema de custodia ▪ cmis:getContentStream. Elemento que permite especificar la localización de la firma en un gestor documental externo.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

8.2.2.1.3 <afxp:SignatureArchiveId>

SignatureArchiveId		
Diagrama		
Descripción	Identificador de transacción de la firma que va ha ser actualizada.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Atributos	Nombre	Descripción
	ID	Identificador único que permite referenciar el elemento desde otro elemento incluido en la petición XML. Su inclusión es opcional.

8.2.2.1.4 <cmism:getContentStream>

Este componente permite indicar la localización de la firma a actualizar dentro de un gestor documental externo.

Puede obtener información detallada sobre este elemento en el apartado 0

8.2.2.1.5 <dss:ReturnUpdatedSignature>

ReturnUpdatedSignature	
Diagrama	
Descripción	La inclusión de este elemento indica al sistema que debe llevar a cabo un proceso de

ReturnUpdatedSignature		
	actualización sobre la firma electrónica especificada. La actualización siempre será respecto al formato deseado, es decir, no se permite actualizar la versión de la firma, solo su formato.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	Nombre	Descripción
	Type	Permite especificar el formato al que se desea extender la firma. En el anexo A.3.2 se detallan los distintos valores posibles. Deben tenerse en cuenta, además, las restricciones existentes para la extensión de una firma electrónica, según se detalla en la tabla del apartado 8.2

8.2.2.1.6 <afxp:TargetSigner>

Permite identificar el firmante a actualizar (en caso de incluir más de un firmante en la firma enviada). Si no se incluye en la petición se actualizará todos los firmantes en aquellos casos que todos los firmantes incluidos en la firma tengan un formato de firma menos avanzado al que se quiere actualizar. En el caso de no especificar el atributo “afxp:TargetSigner” y que exista algún firmante que tenga un formato igual o superior al que se desea actualizar el servicio devolverá una respuesta de petición errórnea indicando que la firma ya posee un formato igual o superior al que se desea actualizar.

Para obtener más información sobre este elemento, véase el apartado 8.1.3.1.10

8.2.2.1.7 <afxp:UpdatedSignatureMode>

Este componente no está contemplado en estas especificaciones sin embargo se admite por compatibilidad con versiones anteriores siendo ignorado por el servidor.

UpdatedSignatureMode	
Diagrama	
Descripción	Con este elemento, se indica al sistema las operaciones de validación que debe realizar sobre la firma antes de proceder a su actualización. Estas operaciones permiten al sistema garantizar que únicamente se actualizarán firmas correctas. Por defecto, se realiza siempre una validación completa de la firma. En caso de desear que dicha validación no verifique el/los certificados firmantes, debe especificar como valor del elemento UpdatedSignatureMode, el valor: urn:afirma:dss:1.0:profile:XSS:upgrade:NoCertificateValidation Este valor podrá ser ignorado por el sistema, en caso de que la configuración del mismo haya sido establecida en modo Estricto. Consulte con su Administrador para obtener más información acerca de ello.
Namespace	urn:afirma:dss:1.0:profile:XSS:schema

8.2.2.1.8 <afxp:IgnoreGracePeriod>

Este componente informa al servidor que no se desea aplicar periodo de gracia.

Para obtener más información sobre este elemento, véase el apartado 8.1.3.1.13

8.2.2.1.9 <afxp:ProcessAsNotBaseline>

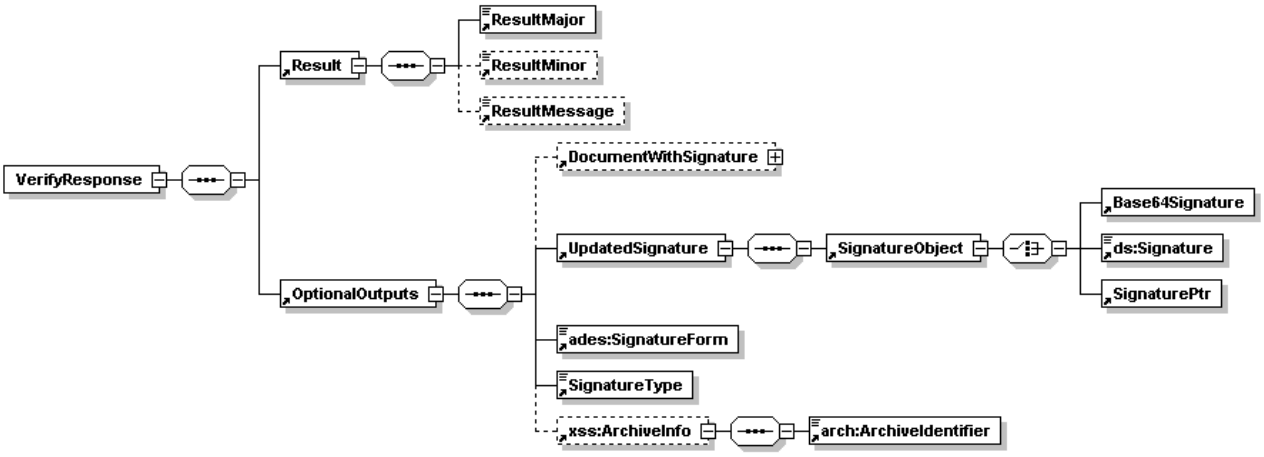
Este componente informa al servidor que se debe forzar el uso de los formatos no baseline.

Para obtener más información sobre este elemento, véase el apartado 8.2.1.1.22

8.2.2.2 Mensajería XML de Respuesta

El mensaje de respuesta puede variar dependiendo de si el proceso de actualización se completa o por el contrario se debe aplicar un periodo de gracia.

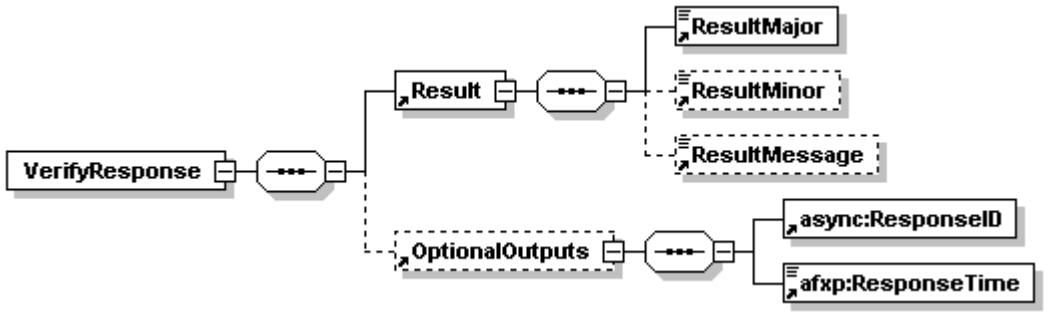
a) *Respuesta sin Periodo de Gracia.* En la siguiente figura podemos observar los distintos componentes que forman una respuesta de Actualización de Firma en la que no se aplica periodo de gracia.



El mensaje de respuesta, *dss:SignRequest*, esta compuesto por tres elementos diferenciados:

- *dss:Result.* Componente que recoge el resultado final del proceso.
- *dss:OptionalOutput*. Elemento que añade información adicional a la respuesta, formato generado, identificador de transacción, etc.
- *dss:SignatureObject*. Elemento que contiene la firma generada o referencia a la misma.

b) *Respuesta con Periodo de Gracia*. En aquellos casos en la que la actualización de la firma necesite la aplicación de un periodo de gracia el contenido del mensaje de respuesta es el siguiente:



El mensaje de respuesta, *dss:VerifyRequest*, esta compuesto por dos elementos diferenciados:

- *dss:Result*. Componente que recoge el resultado final del proceso. En aquellos casos en la que haya que aplicar un periodo de gracia en la actualización de la firma el componente "*dss:Result*" tendrá el valor "**urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending"** en su componente "*dss:ResultMayor*" siguiendo las recomendaciones [DSS APAP]

- *dss:OptionalOutput*. Elemento que añade información adicional a la respuesta. En este caso contendrá los elementos:

    - *async:ResponseID.* Componente que recoge el identificador de proceso asíncrono para su posterior consulta.

    - *afxp:ResponseTime.* Elemento que contiene una fecha estimada de finalización del proceso.

A continuación vamos a describir cada uno de los componentes expuestos.

8.2.2.2.1 <dss:Result>

Una respuesta del servicio de upgrade de firma contiene, al menos, el elemento *dss:Result* que detalla el resultado del proceso.

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.2

8.2.2.2.2 <dss:UpdatedSignature>

Este elemento es el encargado de recoger la firma actualizada.

Puede obtener información detallada sobre este elemento en el apartado 8.1.3.2.1

8.2.2.2.3 <dss:DocumentWithSignature>

Si la firma actualizada es del tipo **XML Signature / XAdES** en modo **enveloped** o **detached**, es decir, documentos XML que *envuelven* a la firma electrónica, la firma actualizada será retornada en un elemento *dss:DocumentWithSignature.*

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.11.

8.2.2.2.4 <ds:Signature>

Si la firma actualizada es del tipo **XML Signature / XAdES** en modo **enveloping**, la firma actualizada será devuelta en un elemento *ds:Signature*, conforme a la especificación [XMLDSIG] / [XAdES]

8.2.2.2.5 <dss:SignaturePtr>

Elemento que **referencia** a una firma XML Signature / XAdES **enveloped o detached** que esta contenida en un elemento *dss:DocumentWithSignature* o *dss:Document*.

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.5.

8.2.2.2.6 <dss:Base64Signature>

Si la firma actualizada es de tipo **ASN.1** (**CMS ó CAdES**), **PDF** u **ODF**, la firma actualizada será retornada en un elemento *dss:Base64Signature.*

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.6.

8.2.2.2.7 <xss:ArchiveInfo>

Si la firma ha sido custodiada o registrada en el sistema, este elemento Incluirá el identificador de registro de la firma generado por la plataforma.

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.9.

8.2.2.2.8 <dss:SignatureType>

Este componente informará sobre el tipo de firma a la que se ha actualizado la firma electrónica.

Puede obtenerse información detallada sobre este componente en el apartado 8.1.1.1.12

8.2.2.2.9 <ades:SignatureForm>

Este elemento informa sobre el formato de firma avanzada al que se ha extendido la firma electrónica.

Puede obtenerse información detallada sobre este componente en el apartado 8.1.1.1.13

8.2.2.2.10 <async:ResponseID>

Este componente recoge el identificador del proceso asíncrono para su posterior consulta

Puede obtenerse información detallada sobre este componente en el apartado 0

8.2.2.2.11 <afxp:ResponseTime>

Elemento que recoge una fecha aproximada en la que la petición ya ha podido se procesada.

Puede obtenerse información detallada sobre este componente en el apartado 0

8.3 Servicio de Validación de Certificados

La interfaz Web Service *DSSAfirmaVerifyCertificate* permite tanto la verificación de certificados X509 finales como de entidades intermedias. Igualmente, valida los certificados de CA's intermedias como raíces.

Adicionalmente, de forma interna, este servicio hace uso de la validación ligera de certificados mediante TSL en el caso de haber solicitado la verificación del estado de revocación y que el certificado no haya sido reconocido.

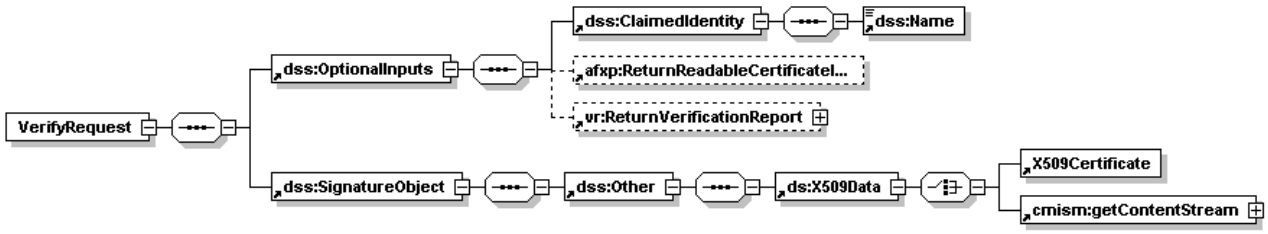
Para el diseño de este servicio se ha partido del las especificaciones [DSS XSS] que permiten la verificación de certificados en su protocolo de verificación.

8.3.1 Validación de Certificados

En los siguientes apartados se analizarán las interfaces XML de petición y respuesta para este servicio.

8.3.1.1 Mensajería XML de Petición

En la siguiente figura se puede observar los elementos DSS que forman una petición de verificación de certificado.



Como observamos la petición de validación de certificado es similar a la de validación de firma. En los siguientes apartados se analizará cada uno de los elementos expuestos.

8.3.1.1.1 <dss:VerifyRequest>

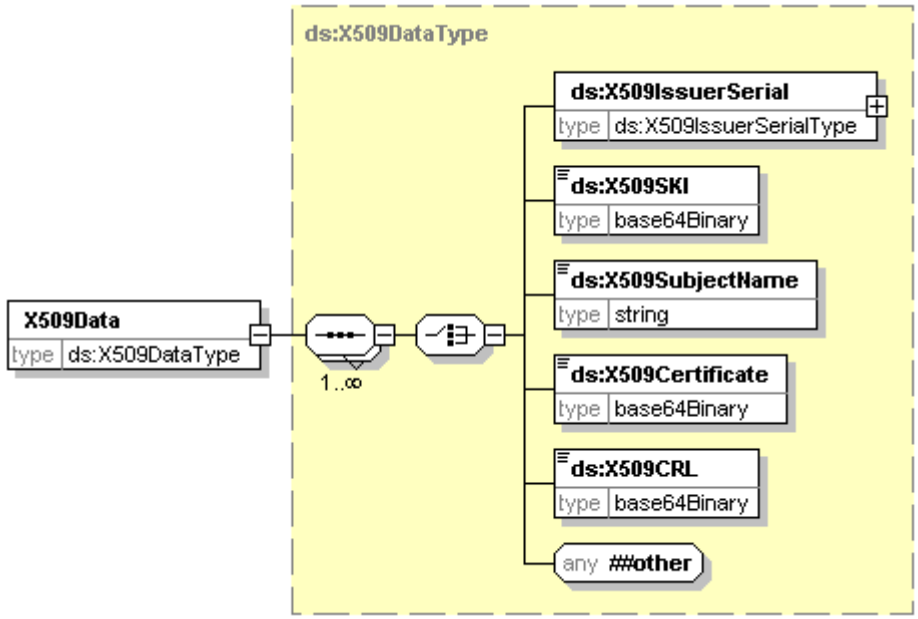
Elemento raíz de una petición de verificación, puede consultarse mas información sobre este elemento en el apartado 8.2.1.1.1

8.3.1.1.2 <dss:SignatureObject>/<dss:Other>

Siguiendo las especificaciones [DSS XSS] el elemento "*dss:SignatureObject*" puede contener un elemento "*ds:X509Data*" incluido en el elemento "*dss:Other*". Esta particularidad permite incluir en la petición de verificación un certificado para su validación.

Se puede obtener mas información sobre el componente "*dss:SignatureObject*" en el apartado 8.1.1.2.4.

8.3.1.1.3 <ds:X509Data>

X509Data		
Diagrama		
Descripción	Elemento definido en las especificaciones [XMLDSIG] que contiene una o mas identificadores de clave, certificados o CRL.	
Namespace	http://www.w3.org/2000/09/xmldsig#	
Hijos	Nombre	Descripción
	ds:X509IssuerSerial	Elemento que contiene "X.509 issuer distinguished name" y "X509 serial number" La implementación actual no soporta este componente, aunque no se descarta su inclusión futura.
	ds:X509SKI	Elemento que contiene el valor del atributo "X509 V.3 SubjectKeyIdentifier" codificado en Base64 La implementación actual no soporta este componente, aunque no se descarta su inclusión futura.

X509Data		
	ds:X509SubjectName	Componente que recoge el valor del componente "X.509 subject distinguished name" del certificado. La implementación actual no soporta este componente, aunque no se descarta su inclusión futura.
	ds:X509Certificate	Componente que contiene un certificado digital codificado en Base64
	ds:X509CRL	Componente que contiene una CRL codificada en Base64. La implementación actual no soporta este componente, aunque no se descarta su inclusión futura.
	##other	El elemento *ds:509Data* permite la adición de elementos definido en otras especificaciones. En esta implementación vamos a contemplar la posibilidad de que el componente *ds:509Data* pueda incluir un elemento *cmism:getContentStream* con la localización en un gestor documental de un certificado digital.

8.3.1.1.4 <cmism:getContentStream>

Para el servicio de validación de certificados, este componente permite referenciar a un certificado alojado en un gestor documental externo.

Puede consultarse más información sobre este elemento en el apartado 0

8.3.1.1.5 <dss:OptionalInputs>

Elemento destinado a recoger los componentes adicionales de petición.

Puede consultarse más información sobre este elemento en el apartado 8.1.1.1.7

8.3.1.1.6 <dss:ClaimedIdentity>

Componente obligatorio que contiene el identificador de aplicación. Para más información sobre este componente consultar el apartado 0

8.3.1.1.7 <afxp:ReturnReadableCertificateInfo>

Mediante este componente se puede solicitar información del certificado. Esta información será una lista de campos del tipo atributo/valor con el resultado de haber parseado el certificado según la configuración del sistema.

NOTA: En el caso de indicar que se extraiga la información del certificado, y realizarse una validación ligera del certificado mediante alguna de las TSL disponibles, siempre se extraen como mínimo los siguientes mapeos/campos:

- **certQualified**: Mapeo que indica si se considera qualified el certificado validado:
  - *NO*: El certificado no es qualified.
  - *YES*: El certificado es qualified.
  - *UNKNOWN*: Se desconoce si el certificado es qualified.

- **certClassification**: Mapeo que determina el tipo del certificado:
  - *NATURAL_PERSON*: Certificado de persona física.
  - *LEGAL_PERSON*: Certificado de persona jurídica.
  - *ESEAL*: Certificado de sello electrónico (de tiempo).
  - *ESIG*: Certificado para firma electrónica (persona física).
  - *WSA*: Certificado para autenticación de servidor web (de componentes).
  - *UNKNOWN*: Se desconoce el tipo del certificado.

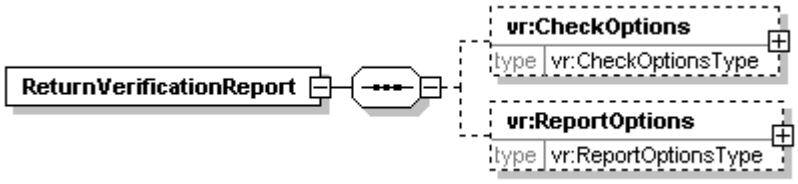
- **qscd**: Mapeo que determina si el certificado se encuentra almacenado en un SSCD/QSCD:
  - *NO*: El certificado no se encuentra en un SSCD/QSCD.
  - *YES*: El certificado se encuentra en un SSCD/QSCD.
  - *YES_MANAGED_ON_BEHALF*: El certificado se encuentra en un SSCD/QSCD controlado por un tercero autorizado.

- *UNKNOWN*: Se desconoce si el certificado está en un SSCD/QSCD.En el siguiente apartado se muestran los identificadores para cada uno de los campos.

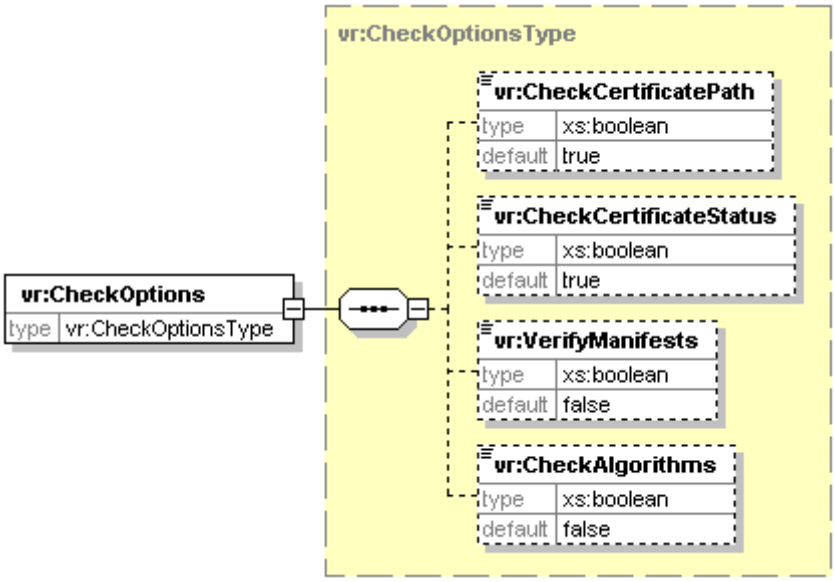
Puede consultarse más información sobre este componente en el apartado 8.2.1.1.12

8.3.1.1.8 <vr:ReturnVerificationReport>

Formalmente este componente es igual al definido en el apartado 8.2.1.1.13 para la verificación de firma, pero el significado de los componentes que lo forman cambia sustancialmente.

ReturnVerificationReport		
Diagrama		
Descripción	Permite especificar las validaciones a realizar sobre el certificado, así como la información que debe ser devuelta en la respuesta. Para los casos de verificación de certificado la inclusión de este componente no implica una inclusión del componente "vr: VerificationReport" en la respuesta.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	CheckOptions	Elemento que contiene las opciones de validación.
	ReportOptions	Especifica qué información acerca del proceso de validación debe ser incluida en la respuesta.

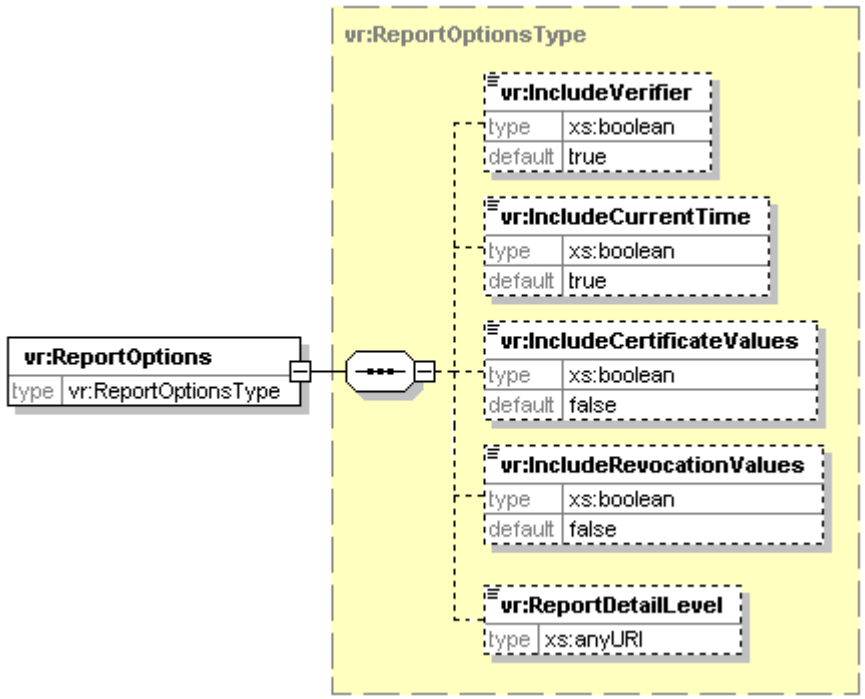
8.3.1.1.9 <vr:CheckOptions>

CheckOptions		
Diagrama		
Descripción	Este elemento recoge las opciones de validación que deben aplicarse sobre el certificado.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#	
Hijos	Nombre	Descripción
	CheckCertificatePath	Elemento que informa si se desea validar la cadena de certificación del certificado enviado. Valor por defecto “true”. La implementación actual no soporta este componente, aunque no se descarta su inclusión futura.
	CheckCertificateStatus	Elemento que informa si se desea verificar el estado de revocación del certificado. Valor por defecto “true”. Dedido a que una CA no puede garantizar la información acerca de un certificado caducado y a su vez una CRL no almacena información sobre certificados caducados, solo se verificará el estado de revocación para certificados no caducados.

CheckOptions		
	vr:VerifyManifest	Componente que indica si se desea validar los elemento "*ds:Manifest*" de una firma XML. Este componente está orientado para peticiones de verificación de firma por lo que no tiene utilidad en verificaciones de certificado.
	vr:CheckAlgorithms	Elemento que informa si se desea validar los algoritmos utilizados. Valor por defecto "false". La implementación actual no soporta este componente, aunque no se descarta su inclusión futura

8.3.1.1.10 <vr:ReportOptions>

Formalmente este componente es igual al definido en el apartado 8.2.1.1.14 para la verificación de firma, pero el significado de los componentes que lo forman cambia sustancialmente en el contexto de validación de certificado.

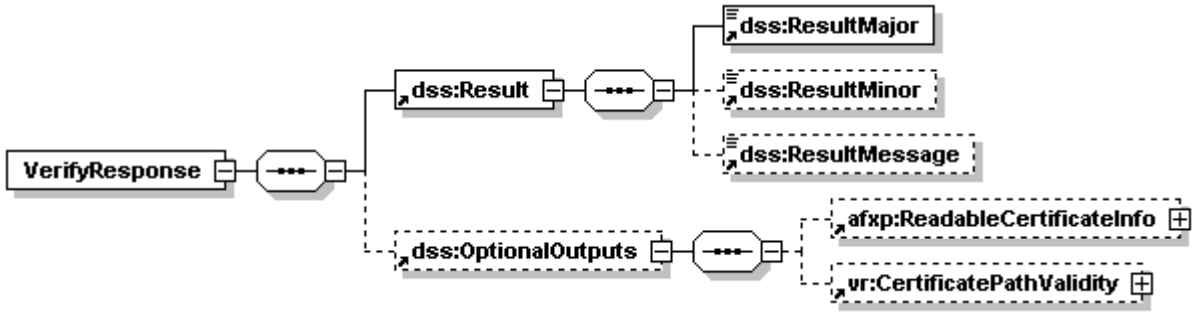
<table>
<tr><th colspan="3">ReportOptions</th></tr>
<tr><td>Diagrama</td><td colspan="2"> 
</td></tr>
<tr><td>Descripción</td><td colspan="2">Dentro del contexto de validación de certificado este componente detalla que información adicional debe incluirse en la respuesta.</td></tr>
<tr><td>Namespace</td><td colspan="2">urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#</td></tr>
<tr><td rowspan="2">Hijos</td><td>Nombre</td><td>Descripción</td></tr>
<tr><td>IncludeVerifier</td><td>Este elemento no se encuentra habilitado en la versión actual del perfil del sistema, aunque no se descarta su uso en versiones posteriores.

Permite especificar en formato booleano si se desea que la</td></tr>
</table>

ReportOptions		
		respuesta incluya la identidad del verificador.
	IncludeCurrentTime	Este elemento no se encuentra habilitado en la versión actual del perfil del sistema, aunque no se descarta su uso en versiones posteriores. Permite especificar en formato booleano si se desea obtener fecha y hora local del servidor, del momento en el que se ha realizado la verificación del certificado.
	IncludeCertificateValues	Permite especificar en formato booleano si se desea que la respuesta incluya los certificados validados. Valor por defecto “false”. En el caso de establecerse el valor a “true” la respuesta contendrá todos los certificados que forman la cadena de validación del certificado enviado, sin embargo no se incluirá el certificado enviado para reducir el tamaño de la respuesta.
	IncludeRevocationValues	Permite especificar en formato booleano si se desea que la respuesta incluya los elementos de consulta de estado de revocación CRL u OCSP utilizados en la validación de los certificados que forman la cadena validada.
	ReportDetailLevel	URI que especifica el nivel de detalle que se desea obtener en la respuesta del servicio. Para más información acerca de los valores que pueden ser incluidos en dicho elemento, consulte el anexo 0.

8.3.1.2 Mensajería XML de Respuesta

En la siguiente figura se representan los elementos que forman la respuesta a una petición de verificación de certificado.



Como observamos la respuesta es parecida a la de verificación de firma, en los siguientes apartados se detallarán cada uno de los componentes que la forma.

8.3.1.2.1 <dss:VerifyResponse>

Elemento raíz de una respuesta de verificación, este componente se describe en el apartado 8.2.1.2.1

8.3.1.2.2 <dss:Result>

Componente que recoge el resultado final del proceso de validación, este componente se define en el apartado 8.1.1.2.2

8.3.1.2.3 <dss:OptionalOutputs>

Este componente se encarga de recoger aquellos elementos adicionales de respuesta DSS, para respuestas de validación de certificado se recoge los elementos

- “afxp:ReadableCertificateInfo” si se ha solicitado en la petición mediante un elemento “afxp:ReturnReadableCertificateInfo”
- “vr:CertificatePathValidity” si se ha establecido el valor de “vr:ReportDetailLevel” a los valores “urn:oasis:names:tc:dss:1.0:reportdetail:noPathDetails” o ”urn:oasis:names:tc:dss:1.0:reportdetail:allDetails”.

Se puede consulta la descripción formal de este componente en el apartado 8.1.1.2.3

8.3.1.2.4 <afxp:ReadableCertificateInfo>

Este elemento incluye información detallada del certificado validado. Esta información será una lista de campos del tipo atributo/valor con el resultado de haber parseado el certificado según la configuración del sistema.

NOTA: En el caso de haberse verificado el estado de revocación del certificado mediante una TSL (el tipo no fue reconocido por la plataforma para la aplicación indicada), y se haya solicitado información del certificado, los campos devueltos son los siguientes (en el mismo u otro orden):

```
<afxp:ReadableCertificateInfo>
        <afxp:ReadableField>
                <afxp:FieldIdentity>certQualified</afxp:FieldIdentity>
                <afxp:FieldValue>[TSL: Indica si se considera cualificado]</afxp:FieldValue>
        </afxp:ReadableField>
        <afxp:ReadableField>
                <afxp:FieldIdentity>certClassification</afxp:FieldIdentity>
                <afxp:FieldValue>[TSL: Tipo de certificado]</afxp:FieldValue>
        </afxp:ReadableField>
        <afxp:ReadableField>
                <afxp:FieldIdentity>qscd</afxp:FieldIdentity>
                <afxp:FieldValue>[TSL: Si se almacena en dispositivo seguro cualificado]</
afxp:FieldValue>
        </afxp:ReadableField>
</afxp:ReadableCertificateInfo>
```

Se puede obtener más información sobre este componente en el apartado 8.2.1.2.16

8.3.1.2.5 <vr:CertificatePathValidity>

Este componente incluye información sobre la verificación de una cadena de certificación.

Dependiendo del valor establecido en el componente "*vr:ReportDetailLevel*" puede darse los casos expuestos en la siguiente tabla:

ReportDetailLevel*	CertificatePathValidity
noDetails	No se incluye en la respuesta componente “vr: CertificatePathValidity”
noPathDetails	Se incluye en la respuesta componente “vr: CertificatePathValidity” con un único elemento “vr:CertificateValidity” con la información del certificado final
allDetails	Se incluye en la respuesta componente “vr: CertificatePathValidity” con un único elemento “vr:CertificateValidity” por cada certificado que forma la cadena de certificación

* Los valores expuestos en la columna debe ir precedidos de la cadena “urn:oasis:names:tc:dss:1.0:reportdetail:”

Puede consultarse más información sobre este componente en el apartado 8.2.1.2.31

8.4 Servicios de Validaciones en Lotes

En este apartado se define los servicios de “Validaciones en Lotes” mediante interfaces DSS. Mediante estos servicios se puede solicitar la verificación de múltiples firmas o certificados digitales al servidor en una única petición. Estas peticiones serán procesadas de forma asíncrona por el servidor, el cual generará una respuesta del tipo “pendiente de procesado” tal y como se especifica en [DSS APAP]

La plataforma publica dos interfaces Web Services para peticiones de “Validaciones en Lotes”.

- ***DSSBatchVerifyCertificate.*** Servicio de Validación Masiva de Certificados. Mediante este servicio se puede solicitar la verificación asíncrona de un conjunto de certificados.

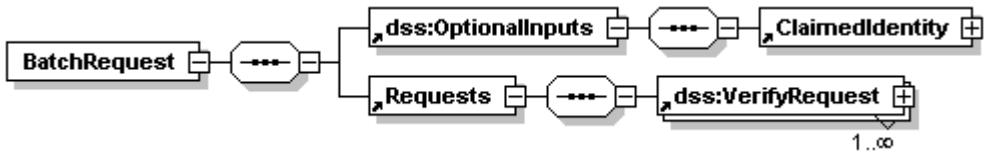
- ***DSSBatchVerifySignature.*** Servicio de Validación Masiva de Firmas. Mediante este servicio se puede solicitar la verificación asíncrona de un conjunto de firmas.

8.4.1 Validación de Certificados

En los siguientes apartados se detallarán los mensajes petición y respuesta para ambos servicios.

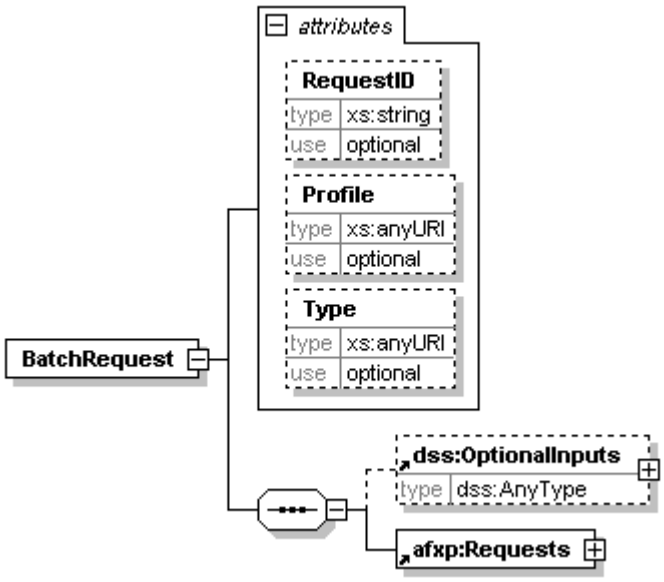
8.4.1.1 Mensajería XML de Petición

En la siguiente figura se puede observar la estructura de una petición de “Validación en Lote”



A continuación se desarrollarán los componentes expuestos.

8.4.1.1.1 <afxp:BatchRequest>

BatchRequest		
Diagrama		
Descripción	Componente raíz de una petición de “Validaciones en Lote” (certificados o firmas).	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	dss:OptionalInputs	Elemento que contiene los componentes adicionales de petición.
	afxp:Requests	Elemento encargado de recoger las peticiones individuales de verificación.
Atributos	Nombre	Descripción
	Profile	Identificador del perfil soportado por el servicio. Para peticiones de verificaciones en lotes de firmas o verificaciones en lotes de certificados el valor de este atributo debe ser **urn:afirma:dss:1.0:profile:XSS**, esta URI identifica al perfil XSS de @Firma.

BatchRequest		
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma. Si la aplicación cliente incluye este atributo, la respuesta generada por el servidor incluirá de igual manera un atributo con el mismo valor en el elemento *BatchResponse*.
	Type	Parámetro que permite identificar el tipo de petición en lote realizada, pudiendo tomar alguno de estos dos valores: Validaciones de Firmas en Lotes → urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifySignatureType Validaciones de Certificados en Lotes → urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifyCertificateType En el caso de no indicarse este atributo el servidor tratará la petición como una petición de Validaciones de Firmas en Lotes.

8.4.1.1.2 <dss:OptionalInputs>

Componente que recoge los elementos adicionales de petición. En este caso solamente contendrá un componente "*dss:ClaimedIdentity*" con el identificador de la aplicación solicitante.

Se puede consultar más información sobre este componente en el apartado 8.1.1.1.7

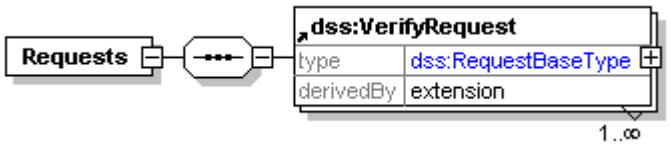
8.4.1.1.3 <dss:ClaimedIdentity>

Elemento que contiene el identificador de la aplicación que realiza la aplicación. Es necesario que se incluya este componente en la petición para autorizar la misma.

Las peticiones individuales (*dss:VerifyRequest*) no deben incluir este elemento ya que se identifica al solicitante con el componente *dss:ClaimedIdentity*" situado en "*dss:BatchRequest/dss:OptionalInputs*"

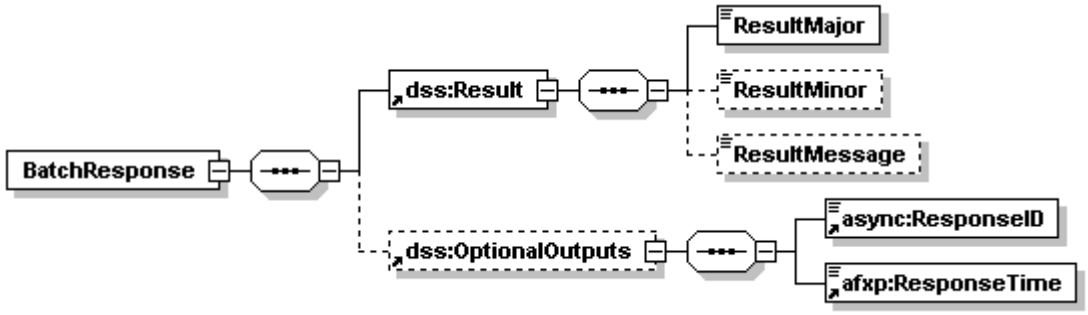
Se puede consultar la descripción formal de este componente en el apartado 0

8.4.1.1.4 <afxp:Requests>

Requests		
Diagrama		
Descripción	Componente que recoge el conjunto de peticiones individuales de validar firma o validar certificado.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	dss:VerifyRequest	Una petición de validaciones en lotes agrupa a un conjunto de peticiones de validación de firma (apartado 8.2.1.1) o validación de certificados (apartado 8.3.1.1) representadas por el elemento “dss:VerifyRequest”. Cada uno de los elementos “dss:VerifyRequest” deben tener establecido su atributo “RequestID” a un valor único en la petición con el fin de relacionar petición y respuesta, de no ser así el servidor devolverá un mensaje de petición no correcta. No es necesario incluir el componente “dss:ClaimedIdentity” en estas peticiones individuales.

8.4.2 Mensajería XML de Respuesta

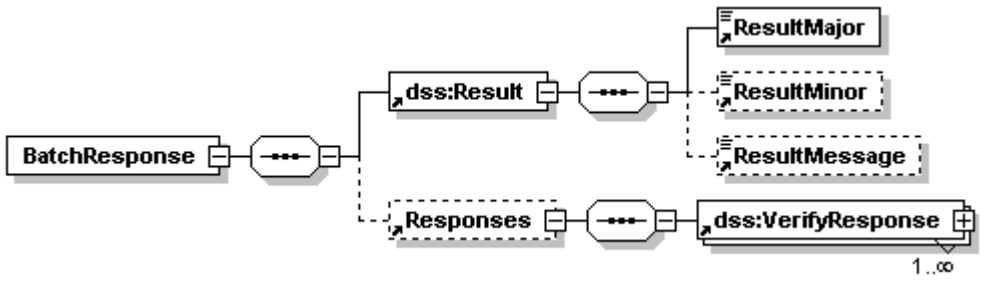
Ante una petición de “Validaciones en Lotes” la respuesta del servidor es del tipo “Pendiente de Procesado”, en el siguiente esquema podemos ver una representación de una respuesta de este tipo.



En estos casos el mensaje de respuesta, *afxp:BatchResponse*, esta compuesto por dos elementos diferenciados:

- *dss:Result*. Componente que recoge el resultado final del proceso. Al ser un proceso asíncrono el componente "*dss:Result*" tendrá el valor "**urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending"** en su componente "*dss:ResultMayor*" siguiendo las recomendaciones [DSS APAP]
- *dss:OptionalOutputs*. Elemento que añade información adicional a la respuesta. En este caso contendrá los elementos:
  - *async:ResponseID.* Componente que recoge el identificador de proceso asíncrono para su posterior consulta.
  - *afxp:ResponseTime.* Elemento que contiene una fecha estimada de finalización del proceso.

Una vez procesada la petición se genera un mensaje de respuesta con los componentes expuestos en la siguiente figura.

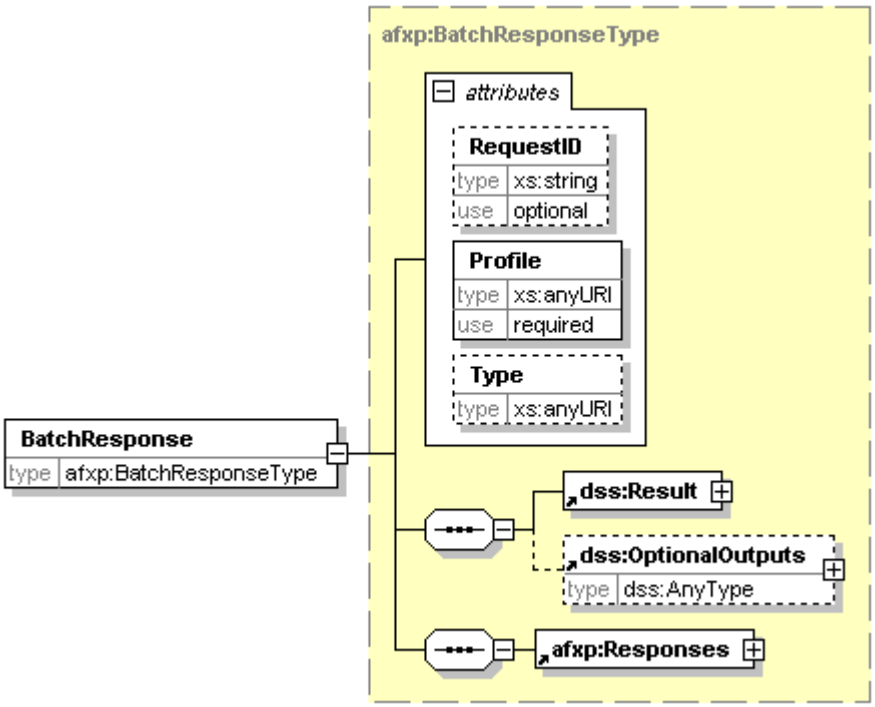


Una vez finalizado los procesos de validación (firmas o certificados) se genera una respuesta con dos componentes:

- *dss:Result*. Componente que recoge el resultado final del proceso.
- *afxp:Responses*. Elemento que recoge los resultados individuales

A continuación se desarrollarán los componentes expuestos.

8.4.2.1.1 <afxp:BatchResponse>

BatchResponse		
Diagrama		
Descripción	Componente raíz de una respuesta de “Validaciones en Lote” (certificados o firmas).	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	dss:Result	Componente que recoge el resultado del proceso. Este componente se detalla en el apartado 8.1.1.2.2
	dss:OptionalOutputs	Elemento que contiene los componentes adicionales de respuesta.
	afxp:Responses	Elemento encargado de recoger respuestas individuales de verificación.
Atributos	Nombre	Descripción

BatchResponse		
	Profile	Identificador del perfil soportado por el servicio. Para peticiones de verificaciones en lotes de firmas o verificaciones en lotes de certificados el valor de este atributo debe ser **urn:afirma:dss:1.0:profile:XSS**, esta URI identifica al perfil XSS de @Firma.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma. Si la aplicación cliente incluye este atributo en la petición, la respuesta generada por el servidor incluirá el mismo valor establecido.
	Type	Parámetro que permite identificar el tipo de petición en lote realizada, pudiendo tomar alguno de estos dos valores: Validaciones de Firmas en Lotes → urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifySignatureType Validaciones de Certificados en Lotes → urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifyCertificateType

8.4.2.1.2 <dss:Result>

Componente que recoge el resultado del procesado de la petición.

Si la petición esta pendiente de procesarse el componente "*dss:ResultMajor*" incluido en este elemento tendrá el valor "**urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending"**.

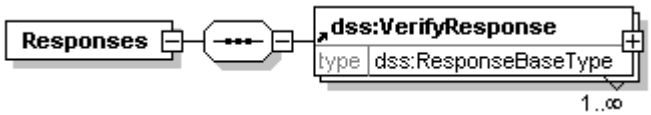
Se puede consultar más información de este componente en el apartado 8.1.1.2.2

8.4.2.1.3 <dss:OptionalOutputs>

Elemento que contiene los componentes adicionales de respuesta. La respuesta solamente contendrá este elemento sí la respuesta es de tipo "Pendiente de Procesado" en cuyo caso incluirá los elementos "*async:ResponseID*" y " *afxp:ResponseTime*".

Se puede consultar más información sobre este componente en el apartado 8.1.1.1.7

8.4.2.1.4 <afxp:Responses>

Responses		
Diagrama		
Descripción	Componente que recoge el conjunto de respuestas individuales de validar firma o validar certificado.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	dss:VerifyResponse	Respuesta de validación de firma (apartado 8.2.1.1.21) o validación de certificados (apartado 8.3.1.2). Cada uno de los elementos "dss:VerifyResponse" tendrá establecido su atributo "RequestID" al valor que tenía el componente "dss:VerifyRequest" asociado.

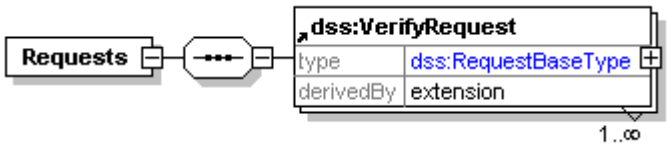
8.4.2.1.5 <dss:ClaimedIdentity>

Elemento que contiene el identificador de la aplicación que realiza la aplicación. Es necesario que se incluya este componente en la petición para autorizar la misma.

Las peticiones individuales (*dss:VerifyRequest*) no deben incluir este elemento ya que se identifica al solicitante con el componente *dss:ClaimedIdentity*" situado en "*dss:BatchRequest/dss:OptionalInputs*"

Se puede consultar la descripción formal de este componente en el apartado 0

8.4.2.1.6 <afxp:Requests>

Requests		
Diagrama		
Descripción	Componente que recoge el conjunto de peticiones individuales de validar firma o validar certificado.	
Namespace	urn:afirma:dss:1.0:profile:XSS:schema	
Hijos	Nombre	Descripción
	dss:VerifyRequest	Una petición de validaciones en lotes agrupa a un conjunto de peticiones de validación de firma (apartado 8.2.1) o validación de certificados (apartado 8.3) representadas por el elemento "dss:VerifyRequest". Cada uno de los elementos "dss:VerifyRequest" deben tener establecido su atributo "RequestID" a un valor único en la petición con el fin de relacionar petición y respuesta, de no ser así el servidor devolverá un mensaje de petición no correcta. No es necesario incluir el componente "dss:ClaimedIdentity" en estas peticiones individuales.

8.4.2.1.7 <async:ResponseID>

Elemento que contiene el "Identificador de Proceso Asíncrono" para obtener el resultado asociada a la petición mediante el servicio "DSSAsyncRequestStatus".

Puede obtenerse más información sbre este componente en el apartado 0

8.4.2.1.8 <afxp:ResponseTime>

Componente que recoge la fecha estimada a partir de la cual se podrá obtener la respuesta correspondiente a la petición realizada.

Puede obtenerse más información sbre este componente en el apartado 0

8.5 Servicio de Consulta de Peticiones Asíncronas

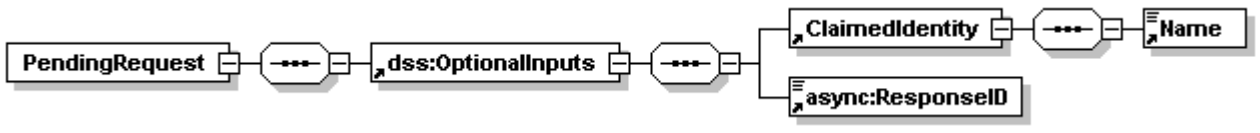
En las especificaciones [DSS APAP] se define el mecanismo para la realización de procesos de firma y verificación de forma asíncrona, siguiendo estas especificaciones @Firma adapta los servicios susceptibles de funcionar de forma asíncrona y publica el servicio "DSSAsyncRequestStatus" para consultar el estado de peticiones asíncrona.

8.5.1 Validación de Certificados

En los siguientes apartados analizaremos los mensajes de petición y respuesta que se utilizarán para interaccionar con este servicio.

8.5.1.1 Mensajería XML de Petición

En la siguiente figura se muestra la composición del mensaje de petición de consulta de procesos asíncronos.

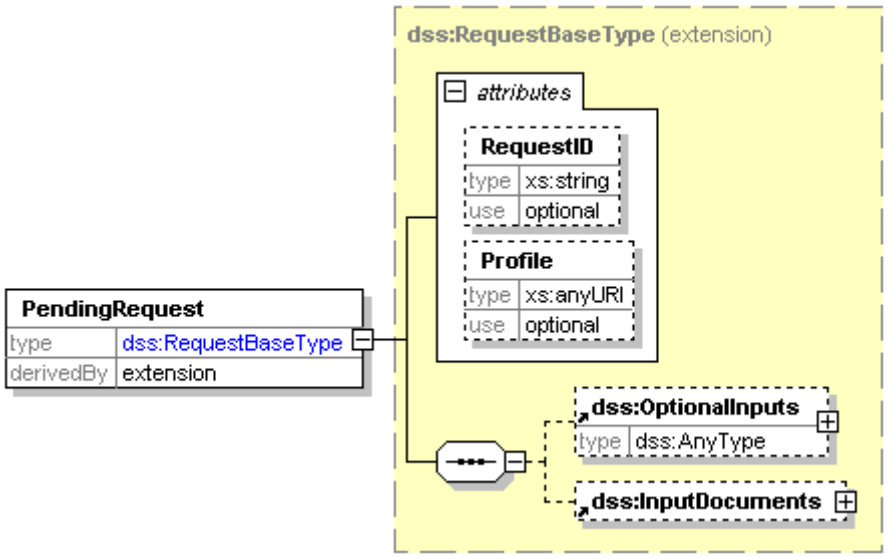


Como observamos en la figura anterior el mensaje debe incluir dentro del elemento "*dss:OptionalInputs*" los componentes:

- "*dss:ClaimedIdentity*" Con el identificador de la aplicación solicitante.
- "*async:ResponseID*" Con el identificador del proceso asíncrono a consultar

Independientemente del proceso asíncrono a consultar (firma, upgrade o validaciones en lote) la composición del mensaje de petición es la misma. A continuación analizaremos los componentes expuestos

8.5.1.1.1 <async:PendingRequest>

PendingRequest		
Diagrama		
Descripción	Componente raíz de una petición de consulta de proceso asíncrono.	
Namespace	urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:1.0	
Hijos	Nombre	Descripción
	dss:OptionalInputs	Elemento que contiene los componentes adicionales de petición.
	dss:InputDocuments	Elemento encargado de recoger documentos de entrada en una petición. Este elemento no esta soportado para peticiones de consultas asíncronas.

PendingRequest		
Atributos	Nombre	Descripción
	Profile	Identificador del perfil soportado por el servicio. No se debe incluir este atributo en la petición ya que esta información ya se incluyo en el mensaje de inicio del proceso asíncrono.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma. Si la aplicación cliente incluye este atributo en la petición, la respuesta generada por el servidor incluirá el mismo valor establecido.

8.5.1.1.2 <dss:OptionalInputs>

Componente que recoge los elementos adicionales de petición. En este caso solamente contendrá los componentes

- "*dss:ClaimedIdentity*" con el identificador de la aplicación solicitante.
- "*async:ResponseID*" con el identificador del proceso asíncrono a consultar

Se puede consultar más información sobre este componente en el apartado 8.1.1.1.7

8.5.1.1.3 <dss:ClaimedIdentity>

Elemento que contiene el identificador de la aplicación que realiza la aplicación. Es necesario que se incluya este componente en la petición para autorizar la misma.

Se puede consultar la descripción formal de este componente en el apartado 0

8.5.1.1.4 <async:ResponseID>

Elemento que contiene el "Identificador de Proceso Asíncrono" para obtener el resultado asociada a la petición mediante el servicio "DSSAsyncRequestStatus".

Puede obtenerse más información sbre este componente en el apartado 0

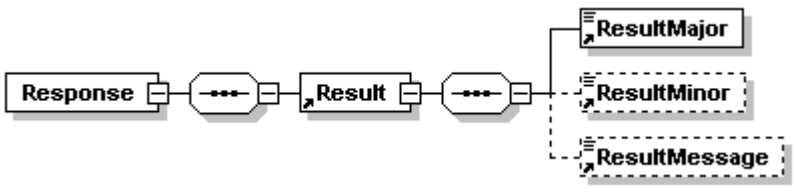
8.5.1.2 Mensajería XML de Respuesta

Se pueden generar dos tipos de respuesta ante peticiones de consulta de procesos asíncronos dependiendo de la validez de la petición.

- Respuesta de petición válida. Si la petición es válida y el proceso asíncrono consultado existe se devolverá una respuesta de proceso finalizado o pendiente de ejecutar acorde al servicio inicialmente invocado. En esta implementación se considera como servicios susceptibles de funcionar de forma asíncrona.
    - Firma Servidor Simple (descrito en el apartado 8.1.1)
    - Firma Servidor CoSign (descrito en el apartado 8.1.2)
    - Firma Servidor CounterSign (descrito en el apartado 8.1.3)
    - Upgrade de Firma (descrito en el apartado 8.2.2)
    - Validaciones en Lotes (descrito en el apartado 8.4)

Para conocer el contenido de la respuesta en estos casos se debe consultar los mensajes de respuesta de los anteriores servicios

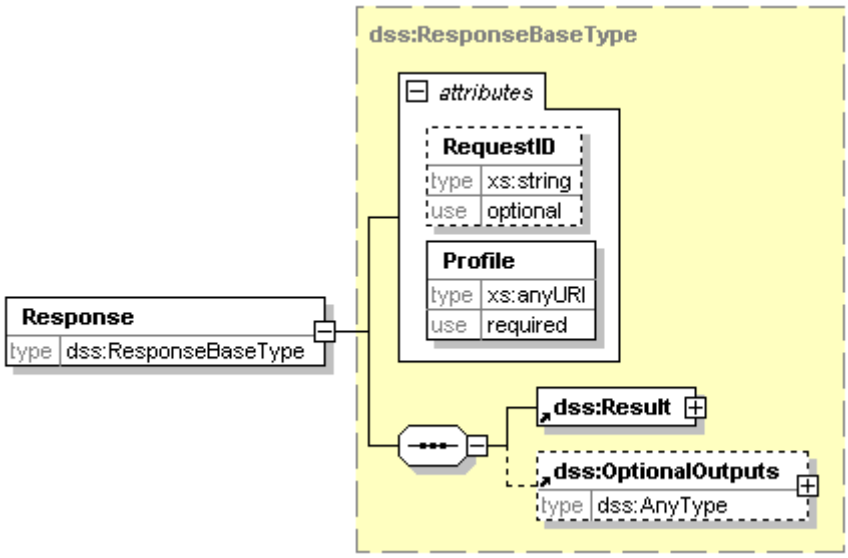
- Respuesta de petición no válida. Si la petición no es formalmente válida, no está autorizada, el identificador de procesos asíncrono no es válido o se produce otro tipo de error se devuelve al cliente una respuesta genérica como la representada en la figura.



Como observamos la respuesta solamente contiene un componente "*dss:Result*" detallando el error producido.

A continuación analizaremos los componentes expuestos

8.5.1.2.1 <dss:Response>

Response		
Diagrama		
Descripción	Componente raíz de una respuesta DSS generica.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	Nombre	Descripción
	dss:OptionalOuputs	Elemento que contiene los componentes adicionales de respuesta. En el contexto de consulta de peticiones asíncrona no se definen componentes adicionales de respuesta, por este motivo el servidor no incluirá este componente en la respuesta
	dss:Result	Componente que recoge el resultado del proceso.

Response		
		Este componente se detalla en el apartado 8.1.1.2.2
Atributos	Nombre	Descripción
	Profile	Identificador del perfil soportado por el servicio. Para respuesta de consulta de peticiones asíncronas el valor de este atributo es **urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing**.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma. Si la aplicación cliente incluye este atributo en la petición, la respuesta generada por el servidor incluirá el mismo valor establecido.

8.6 Servicio de Obtención de Firmas Registradas

El protocolo de recuperación de firma (Archive Retrieval Protocol) del perfil *Archive* de OASIS define los siguientes mensajes:

- ***arch:ArchiveRetrievalRequest***: petición de obtención de firma mediante identificador único.
- ***arch:ArchiveRetrievalResponse***: respuesta de obtención de firma mediante identificador único.

El contenido de estas interfaces se describe en el perfil *Signature Archive Profile* de OASIS.

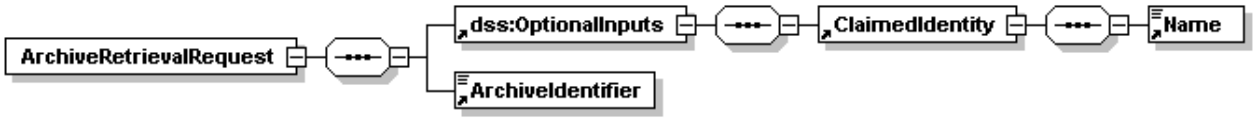
NOTA: Este servicio tan solo se encontrará disponible en la distribución federada.

En los siguientes apartados se describirán los mensajes de petición y respuesta que permiten realizar las anteriores operaciones.

8.6.1 Obtener Firma mediante Identificador de Transacción

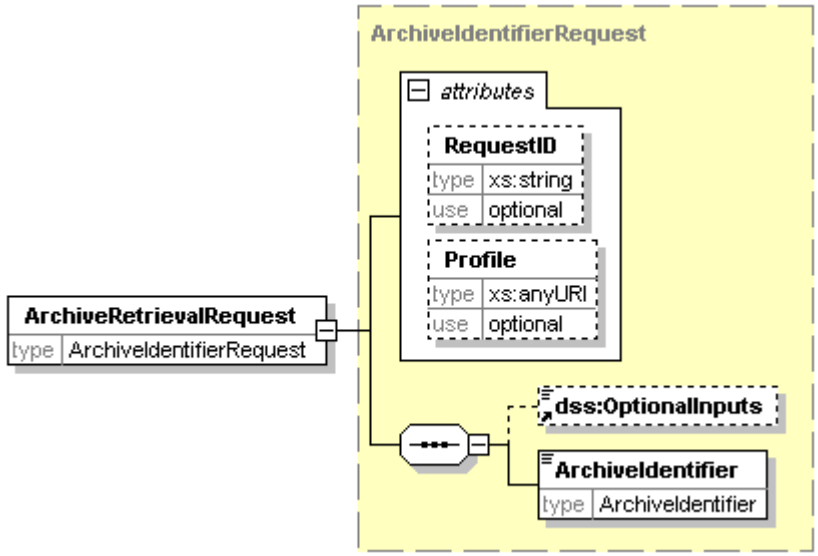
8.6.1.1 Mensajería XML de Petición

En el siguiente diagrama podemos observar los elementos que conforman una petición de obtención de una firma.



Como podemos observar la petición es simple, y únicamente requiere de la inclusión del elemento *dss:ClaimedIdentity* (ver apartado 0) y el identificador de registro de la firma a recuperar, especificado en *arch:ArchiveIdentifier* (ver apartado 0).

8.6.1.1.1 <arch:ArchiveRetrievalRequest>

ArchiveRetrievalRequest	
Diagrama	
Descripción	Elemento raíz de la petición de obtención de una firma registrada
Namespace	urn:oasis:names:tc:dss:1.0:profiles:archive
Hijos	• ArchiveIdentifier

ArchiveRetrievalRequest		
	• dss:OptionalInputs	
Atributos	Nombre	Descripción
	Profile	Identificador del perfil soportado por el servicio. Para respuestas de obtención de firmas, el valor de este atributo será ***urn:afirma:dss:1.0:profile:archive***, esta URI identifica al perfil *Archive* de @Firma.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma. Si la aplicación cliente incluye este atributo, la respuesta generada por el servidor incluirá de igual manera un atributo con el mismo valor en el elemento *ArchiveRetrievalResponse*.

8.6.1.1.2 <dss:OptionalInputs>

Componente que recoge los parámetros adicionales que deben incluirse en la petición. Para las peticiones de obtención de firma solamente es necesario incluir el componente *dss:ClaimedIdentity* .

Se puede obtener más información sobre la definición de este componente en el apartado 8.1.1.1.7.

8.6.1.1.3 <dss:ClaimedIdentity>

Componente que recoge el identificador de la aplicación que realiza la petición.

Se puede obtener más información sobre la definición de este componente en el apartado 0.

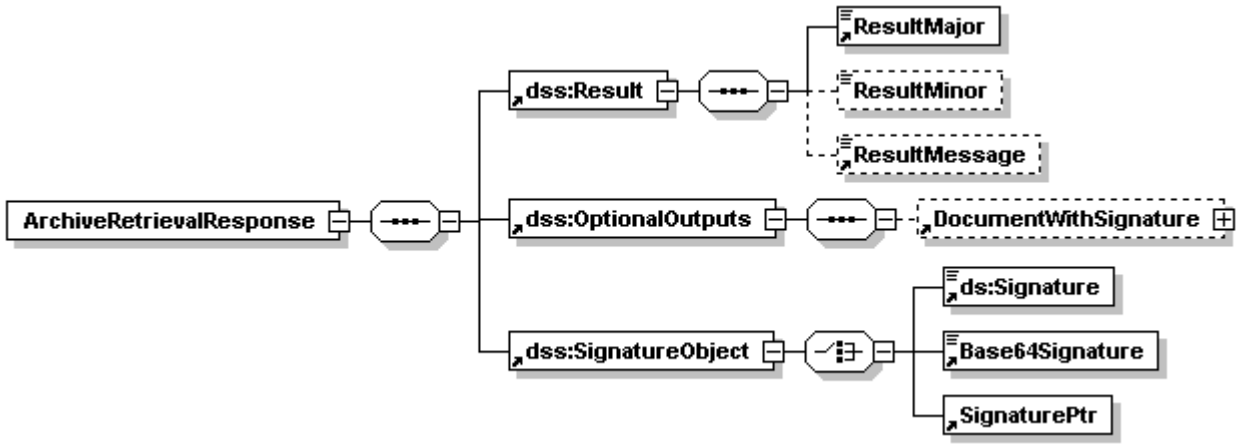
8.6.1.1.4 <arch:ArchiveIdentifier>

Componente que recoge el identificador de transacción de la firma a recuperar.

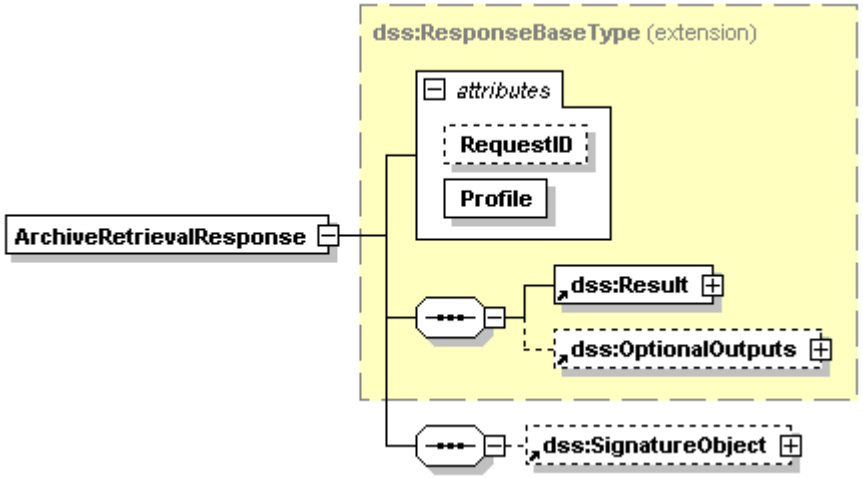
En el apartado 0 puede obtener información adicional sobre este elemento.

8.6.1.2 Mensajería XML de Respuesta

La respuesta a una petición de firma estara formada por los elementos expuestos en el siguiente esquema.



8.6.1.2.1 <arch:ArchiveRetrievalResponse>

ArchiveRetrievalResponse	
Diagrama	
Descripción	Elemento raíz de la respuesta a una petición de obtención de firma
Namespace	urn:oasis:names:tc:dss:1.0:profiles:archive
Hijos	dss:Result dss:OptionalOutput dss:SignatureObject

ArchiveRetrievalResponse		
Atributos	Nombre	Descripción
	Profile	Identificador del perfil soportado por el servicio. Para respuestas de obtención de firmas, el valor de este atributo será ***urn:afirma:dss:1.0:profile:archive***, esta URI identifica al perfil *Archive* de @Firma.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma. Si la aplicación cliente incluye este atributo, la respuesta generada por el servidor incluirá de igual manera un atributo con el mismo valor en el elemento *ArchiveRetrievalResponse*.

8.6.1.2.2 <dss:Result>

Una respuesta del servicio de obtención de firma contiene, al menos, el elemento *dss:Result* que detalla el resultado del proceso.

Puede obtener información detallada sobre este elemento en el apartado 8.1.1.2.2

8.6.1.2.3 <dss:OptionalOutputs>

Componente que contiene elementos adicionales a una respuesta DSS, para el caso de una respuesta de obtención de firma podrá contener el siguiente componente:

- *dss:DocumentWithSignature.* Si la firma recuperada es del tipo **XML Signature / XAdES** en modo **enveloped** o **detached**, es decir, documentos XML que *envuelven* a la firma electrónica, la firma actualizada será retornada en un elemento *dss:DocumentWithSignature.* En el apartado 8.1.1.2.11 puede obtener información adicional sobre este elemento.

Se puede obtener más información sobre el componente *dss:OptionalOutputs* en el apartado 8.1.1.2.3

8.6.1.2.4 <dss:SignatureObject>

Componente que contiene o referencia a la firma que se ha recuperado. Dependiendo de la naturaleza de la firma el contenido de este componente puede variar.

En caso de tratarse de una firma no XML (ASN.1, PDF u ODF), se incluirá en un elemento *dss:Base64Signature*. Para obtener más información sobre este componente consúltese el apartado 8.1.1.2.6

En el caso de firma XML **enveloping** se incluirá la firma sin codificar en un elemento *ds:Signature*

En el caso de firmas XML **enveloped** o **detached**, se incluirán un elemento *ds:SignaturePtr* el cual hará referencia al elemento dss:Base64XML que contendrá la firma. Puede obtener más información sobre el componente *ds:SignaturePtr* en el apartado 8.1.1.2.5

Puede obtener más información sobre el componente *dss:SignatureObject* en el apartado 8.1.1.2.4

A.1 Descripción de los Elementos utilizados en los Diagramas

A continuación se describen los distintos componentes utilizados para representar los XML de petición y respuesta.

- Elemento Simple Obligatorio.

El rectángulo representa un elemento y al ser un rectángulo de borde continuo indica que el elemento es requerido. El nombre de este elemento es "*dss:ResultMayor*" y el tipo es "*xs:anyURI*"

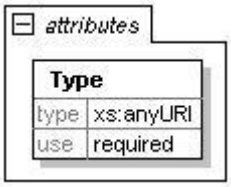
- Elemento Simple Opcional.

El rectángulo informa que se trata de un elemento y el borde discontinuo que el elemento es opcional. El nombre de este elemento es "*dss:ResultMinor*" y el tipo es "*xs:anyURI*"

- Múltiples Elementos.

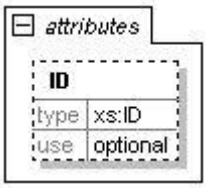
Dos rectángulos superpuestos indican varios elementos del mismo tipo. Si el elemento es requerido el borde será continuo, en caso contrario el sería discontinuo. En el parte inferior derecha se informa del rango de elementos permitidos (0.. ∞).

- Atributo Obligatorio.



Un rectángulo con la etiqueta "*attributes*" indica que el elemento que contiene es un atributo. Si el rectángulo que describe al atributo tiene los bordes continuos el atributo será requerido. El nombre de este atributo es "*Type*" y el tipo es "*xs:anyURI*"

- Atributo Opcional.

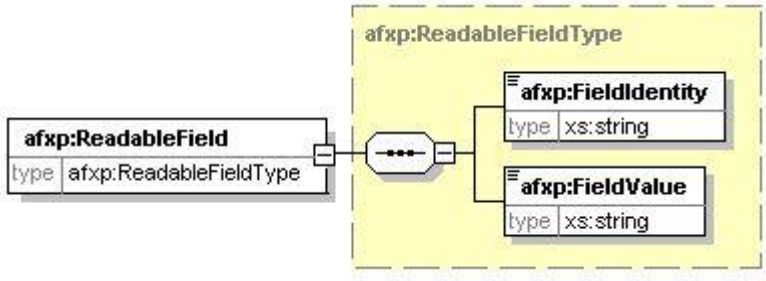


Un rectángulo con la etiqueta "*attributes*" indica que el elemento que contiene es un atributo. Si el rectángulo que describe al atributo tiene los bordes discontinuos el elemento será opcional. El nombre de este atributo es "*ID*" y el tipo es "*xs:ID*"

- Elementos de Composición.

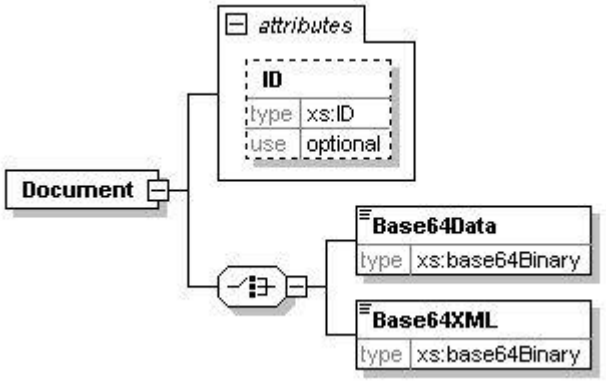
En este documento solamente se utilizan los elementos de composición "*sequence*" y "*choice*" los cuales tienen la representación que se muestra a continuación.

  - Sequence



El elemento "*afxp:ReadableField*" esta compuesto de la secuencia de elementos "*afxp:FieldIdentity*" y "*afxp:FieldValue*".

- Choice



En este caso el elemento "*Document*" esta compuesto del atributo "*ID*" y el elemento "*Base64Data*" o "*Base64XML*".

A.2 Schemas

En este apartado se detallarán los esquemas de los perfiles XSS y Archive de @Firma.

A.2.1 Schema del Perfil XSS de @Firma

El Schema que define los componentes del perfil XSS de @ Firma se pueden encontrar en las siguientes ubicaciones:

- Kit de integración (afirmaws.zip): xsd/dss/afirma-dss-1.0-profiles-XSS-schema.xsd
- En el entorno de Preproducción en la url:
- https://pre-afirma.redsara.es/afirmaws/xsd/dss/afirma-dss-1.0-profiles-XSS-schema.xsd

- En el entorno de Producción en la url:
- https://afirma.redsara.es/afirmaws/xsd/dss/afirma-dss-1.0-profiles-XSS-schema.xsd

A.2.2 Schema del Perfil Archive de @Firma

El Schema que define los los componentes del perfil Archive de @ Firma se pueden encontrar en las siguientes ubicaciones:

- Kit de integración (afirmaws.zip): xsd/dss/afirma-dss-1.0-profiles-archive-schema.xsd
- En el entorno de Preproducción en la url:
- https://pre-afirma.redsara.es/afirmaws/xsd/dss/afirma-dss-1.0-profiles-archive-schema.xsd
- En el entorno de Producción en la url:
- https://afirma.redsara.es/afirmaws/xsd/dss/afirma-dss-1.0-profiles-archive-schema.xsd

A.3 Identificadores

Muchos de los elementos DSS utilizan URI como valores para identificar formatos de firma, resultados del proceso, etc.

En este anexo se detallarán todas aquellas URI empleadas en la actual implementación.

A.3.1 Identificadores de Tipo de Firma

Las siguientes URI pueden ser usados como valor para el elemento *<dss:SignatureType>*.

Formato	Identificador
CMS	urn:ietf:rfc:3369
CMS (Con Sello de Tiempo)	urn:afirma:dss:1.0:profile:XSS:forms:CMSWithTST
XML Signature	urn:ietf:rfc:3275

CAdES	http://uri.etsi.org/01733/v1.7.3#
XAdES versión 1.3.2	http://uri.etsi.org/01903/v1.3.2#
XAdES versión 1.2.2	http://uri.etsi.org/01903/v1.2.2#
XAdES versión 1.1.1	http://uri.etsi.org/01903/v1.1.1#
ODF	urn:afirma:dss:1.0:profile:XSS:forms:ODF
PDF	urn:afirma:dss:1.0:profile:XSS:forms:PDF
PAdES	urn:afirma:dss:1.0:profile:XSS:forms:PAdES
CAdES Baseline	http://uri.etsi.org/103173/v2.2.1#
XAdES Baseline	http://uri.etsi.org/103171/v2.1.1#
PAdES Baseline	http://uri.etsi.org/103172/v2.1.1#
ASiC Baseline	http://uri.etsi.org/103174/v2.1.1#

A.3.2 Identificadores de Formato Avanzado

Las siguientes URI pueden ser usadas como valor para el elemento *<ades:SignatureForm>.*

Formato Avanzado	Identificador
BES	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES
EPES	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:EPES
T	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T
C	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-C
X	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X

X-1	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-1
X-2	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-2
X-L	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L
X-L-1	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L-1
X-L-2	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L-2
A	urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-A
B-Level	urn:afirma:dss:1.0:profile:XSS:AdES:forms:B-Level
T-Level	urn:afirma:dss:1.0:profile:XSS:AdES:forms:T-Level
LT-Level	urn:afirma:dss:1.0:profile:XSS:AdES:forms:LT-Level
LTA-Level	urn:afirma:dss:1.0:profile:XSS:AdES:forms:LTA-Level

A.3.3 Formatos soportados por el Sistema

En la siguiente tabla se muestra la correspondencia entre los formatos soportados por la plataforma y los valores que deben tomar los elementos *dss:SignatureType* y *ades:SignatureForm*

Formato	SignatureType	SignatureForm
PKCS#7 v1.5	*urn:ietf:rfc:2315*	
CMS	*urn:ietf:rfc:3369*	
CMS - T	*urn:afirma:dss:1.0:profile:XSS:forms:CMSWithTST*	
XML Signature	*urn:ietf:rfc:3275*	
CAdES	*http://uri.etsi.org/01733/v1.7.3#*	
CAdES-BES	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES**
CAdES-EPES	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:EPES**
CAdES-T	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T**
CAdES-C	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-C**

CAdES-X	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X**
CAdES-X1	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-1**
CAdES-X2	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-2**
CAdES-XL	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L**
CAdES-XL1	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L-1**
CAdES-XL2	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L-2**
CAdES-A	*http://uri.etsi.org/01733/v1.7.3#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-A**
XAdES	*http://uri.etsi.org/01903/v1.3.2#*	
XAdES-BES	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES**
XAdES-EPES	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:EPES**
XAdES-T	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T**
XAdES-C	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-C**
XAdES-X	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X**
XAdES-X1	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-1**
XAdES-X2	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-2**
XAdES-XL	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L**
XAdES-XL1	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L-1**
XAdES-XL2	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L-2**
XAdES-A	*http://uri.etsi.org/01903/v1.3.2#*	**urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-A**
ODF	*urn:afirma:dss:1.0:profile:XSS:forms:ODF*	
PDF	*urn:afirma:dss:1.0:profile:XSS:forms:PDF*	
PAdES Basic	*urn:afirma:dss:1.0:profile:XSS:forms:PAdES*	**urn:afirma:dss:1.0:profile:XSS:PAdES:1.2.1:forms:Basico**
PAdES-BES	*urn:afirma:dss:1.0:profile:XSS:forms:PAdES*	**urn:afirma:dss:1.0:profile:XSS:PAdES:1.1.2:forms:BES**
PAdES-EPES	*urn:afirma:dss:1.0:profile:XSS:forms:PAdES*	**urn:afirma:dss:1.0:profile:XSS:PAdES:1.1.2:forms:EPES**
PAdES-LTV	*urn:afirma:dss:1.0:profile:XSS:forms:PAdES*	**urn:afirma:dss:1.0:profile:XSS:PAdES:1.1.2:forms:LTV**
CAdES B-Level	*http://uri.etsi.org/103173/v2.2.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:B-Level**
CAdES T-Level	*http://uri.etsi.org/103173/v2.2.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:T-Level**

CAdES LT-Level	*http://uri.etsi.org/103173/v2.2.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:LT-Level**
CAdES LTA-Level	*http://uri.etsi.org/103173/v2.2.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:LTA-Level**
XAdES B-Level	*http://uri.etsi.org/103171/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:B-Level**
XAdES T-Level	*http://uri.etsi.org/103171/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:T-Level**
XAdES LT-Level	*http://uri.etsi.org/103171/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:LT-Level**
XAdES LTA-Level	*http://uri.etsi.org/103171/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:LTA-Level**
PAdES B-Level	*http://uri.etsi.org/103172/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:B-Level**
PAdES T-Level	*http://uri.etsi.org/103172/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:T-Level**
PAdES LT-Level	*http://uri.etsi.org/103172/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:LT-Level**
PAdES LTA-Level	*http://uri.etsi.org/103172/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:LTA-Level**
ASiC-S B-Level	*http://uri.etsi.org/103174/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:B-Level**
ASiC-S T-Level	*http://uri.etsi.org/103174/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:T-Level**
ASiC-S LT-Level	*http://uri.etsi.org/103174/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:LT-Level**
ASiC-S LTA-Level	*http://uri.etsi.org/103174/v2.1.1#*	**urn:afirma:dss:1.0:profile:XSS:AdES:forms:LTA-Level**

El formato PKCS#7 se encuentra obsoleto para Generación.

El formato CADES-XL solo se permite en Validación. En la generación y actualización de firmas la plataforma siempre generará CADES-XL1 cuando se le especifique CADES-XL.

El formato ASiC-S B-Level sólo se permite en Validación. Por su parte, los formatos ASiC-S T-Level, ASiC-S LT-Level y ASiC-S LTA-Level sólo se permiten en Actualización y Validación. Así pues, las firmas ASiC-S sólo se pueden validar o actualizar, y el proceso de actualización de una firma ASiC-S consistirá en actualizar la firma CAdES Baseline o XAdES Baseline que contenga.

A.3.4 Algoritmos de resumen

En la siguiente tabla se enumeran las distintas URI que identifican los algoritmos de hash soportados por la plataforma.

Algoritmo de Hash	Identificador
MD2	*urn:ietf:rfc:1319*
MD5	*http://www.w3.org/2001/04/xmldsig-more#md5*
SHA1	*http://www.w3.org/2000/09/xmldsig#sha1*
SHA256	*http://www.w3.org/2001/04/xmlenc#sha256*
SHA384	*http://www.w3.org/2001/04/xmldsig-more#sha384*
SHA512	*http://www.w3.org/2001/04/xmlenc#sha512*

Para el caso de las firmas en servidor, los algoritmos MD2 y MD5 no podrán utilizarse debido a que aportan un nivel de seguridad muy bajo. El resto de formatos puede combinarse con cualquier formato de firma.

A.3.5 Identificadores de resultado del proceso

A continuación se enumeran las diferentes URI utilizadas para determinar el resultado general de un proceso.

En las siguientes tablas se recogen los distintos resultados globales (ResultMajor) que puede arrojar una petición DSS.

ResultMajor
urn:oasis:names:tc:dss:1.0:resultmajor:Success
El proceso se ha realizado satisfactoriamente
urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError
La petición no es correcta
urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError
Se ha producido un error al realizar el proceso en el servidor
urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation
No se puede realizar la operación ya que falta información en la petición
urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature
La firma verificada es valida
urn:afirma:dss:1.0:profile:XSS:resultmajor:InvalidSignature
La firma verificada no es valida
urn:oasis:names:tc:dss:1.0:resultmajor:Warning
Durante la ejecución del proceso se ha detectado algún evento que debe advertirse al Cliente
urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmajor:Pending
La petición se encuentra pendiente de procesado. Ejecución asíncrona.

Los siguientes identificadores complementan a los anteriores para detallar el resultado del proceso (ResultMinor).

ResultMinor
urn:oasis:names:tc:dss:1.0:resultminor:KeyInfoNotProvided
La petición no incluye el alias del certificado servidor firmante
urn:oasis:names:tc:dss:1.0:resultminor:NotParseableXMLDocument
La petición o firma no es un XML válido
urn:oasis:names:tc:dss:1.0:resultminor:NotSupported
Alguno de los componentes que forma la petición no es soportado por el servidor
urn:oasis:names:tc:dss:1.0:resultminor:invalid:KeyLookupFailed
El alias del certificado servidor no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:UpdateSignatureTypeNotProvided
No se ha suministrado el formato al que se desea actualizar la firma
urn:afirma:dss:1.0:profile:XSS:resultminor:IncompleteUpgradeOperation
No se ha podido completar el proceso de actualización / generación de firma al formato indicado debido a algún error durante el proceso de inclusión/obtención de un sello de tiempo.
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTypeNotSupported
El valor establecido al elemento <dss:SignatureType> no es válido o no es soportado
urn:oasis:names:tc:dss:1.0:resultminor:invalid:IncorrectSignature
La firma enviada no es válida.

urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureFormNotSupported	
	El valor establecido al elemento <ades:SignatureForm> no es válido o no es soportado
urn:afirma:dss:1.0:profile:XSS:resultminor:HashAlgorithmNotSupported	
	El valor establecido al elemento <afxp:HashAlgorithm> no es válido o no es soportado
urn:afirma:dss:1.0:profile:XSS:resultminor:ClaimedIdentityNotProvided	
	No se ha incluido en la petición el elemento <dss:ClaimedIdentity>
urn:afirma:dss:1.0:profile:XSS:resultminor:UnauthorizedClaimedIdentity	
	El valor del elemento <dss:ClaimedIdentity> no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:InputDocumentNotSupported	
	Alguno de los elementos contenidos en el <dss:InputDocument> no es válido o no está soportado
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureArchiveIdentifierNotSupported	
	La operación no admite la utilización del componente <afxp:SignatureArchiveId>
urn:afirma:dss:1.0:profile:archive:resultminor:ArchiveIdentifierNotProvided	
El componente <arch:ArchiveIdentifier> no esta incluido en la petición	
urn:afirma:dss:1.0:profile:XSS:resultminor:IncorrectUpdateSignatureType	
	El atributo "Type" del elemento <dss:ReturnUpdatedSignature> no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:XMLSignatureModeNotSupported	
	El contenido del elemento <afxp:XMLSignatureMode> no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureNotProvided	

No se ha suministrado la firma a validar
urn:afirma:dss:1.0:profile:archive:resultminor:AdditionalSignatureInfoNotProvided
La petición de registro de firma no incluye el componente <afap:AdditionalSignatureInfo>
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureFormat:IncorrectFormat
El formato de la firma no es válido
urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyNotSupported
La política de firma no se encuentra soportada por el sistema
urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyDigestFailure
El hash de la política incluido en la firma no coincide con el hash real de la política de firma
urn:oasis:names:tc:dss-x:1.0:resultminor:error:SignaturePolicyIdentifierError
No se ha incluido identificador de la política de firma en la petición.
urn:afirma:dss:1.0:profile:XSS:resultminor:SignaturePolicy:IncompleteAttributes
La firma no incluye ciertos atributos requeridos por la política de firma
urn:afirma:dss:1.0:profile:XSS:resultminor:SignaturePolicy:InvalidAttributes
El contenido de algún atributo de firma no se ajusta a lo especificado por la política de firma
urn:afirma:dss:1.0:profile:XSS:resultminor:SignaturePolicy:InvalidDigestAlgorithms
Se ha utilizado un algoritmo de resumen no permitido por la política de firma.
urn:afirma:dss:1.0:profile:XSS:resultminor:SignaturePolicy:SignatureOutOfPolicyPeriod
La firma ha sido realizada fuera del periodo de validez de la política de firma

urn:afirma:dss:1.0:profile:XSS:resultminor:SignaturePolicy:InvalidSignatureAlgorithms
Se ha utilizado un algoritmo de firma no permitido por la política de firma.
urn:afirma:dss:1.0:profile:XSS:resultminor:SignaturePolicy:InvalidSignatureFormat
El formato de firma no está soportado por la política de firma
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:InvalidSignature
La verificación del valor de la firma no ha sido satisfactoria
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:InvalidReference
Alguna de las referencias de la firma no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:MismatchedSignedData
Los datos firmados no corresponden con los originalmente firmados
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:SignedDataNotProvided
No se han especificado los datos originalmente firmados para validar la firma explícita
urn:afirma:dss:1.0:profile:XSS:resultminor:SigningTime:InvalidPeriod
El atributo “SigningTime” es posterior al momento de validación
urn:afirma:dss:1.0:profile:XSS:resultminor:InvalidNotSignerCertificate
Se ha encontrado en la firma un certificado no válido distinto al firmante
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:InvalidSignature
La firma del certificado firmante no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:IncorrectIssuer

El emisor del certificado firmante no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:NotValidYet
El certificado firmante no es válido aun
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:Expired
El certificado firmante se encuentra caducado
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:Revoked
El certificado firmante se encuentra revocado
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:UnknownStatus
El estado del certificado firmante es desconocido
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:InvalidCertificateChain
La cadena de certificación del certificado firmante no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:NotSupported
El certificado firmante no se encuentra actualmente entre los certificados soportados por la plataforma
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:NotAllowed
El certificado firmante no está recogido en la política de certificación de la aplicación
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:NotAllowedBySignaturePolicy
El certificado firmante no está permitido por la política de firma
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:CertificatePolicyNotAllowed
La política del certificado firmante no está permitida por la política de firma

urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:InvalidCertificateKeyLength
La longitud de la clave del certificado firmante no cumple lo especificado en la política de firma
urn:afirma:dss:1.0:profile:XSS:resultminor:KeyInfo:MismatchedKeyInfo
La información del firmante no coincide con la incluida en el KeyInfo
urn:afirma:dss:1.0:profile:XSS:resultminor:KeyInfo:SigningCertificateNotIncluded
La firma no incluye el atributo “SigningCertificate”
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:InvalidSignature
La firma del Sello de Tiempo incluida en el atributo “SignatureTimeStamp” no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:MismatchedSignedData
Los datos firmados por el Sello de Tiempo del atributo “SignatureTimeStamp” no se corresponde con los incluidos en la firma
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:IncorrectFormat
El formato del Sello de Tiempo del atributo “SignatureTimeStamp” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:InvalidSignature
La firma del certificado firmante del “SignatureTimeStamp” no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:IncorrectIssuer
El emisor del certificado firmante del “SignatureTimeStamp” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:NotValidYet
El certificado firmante del “SignatureTimeStamp” todavía no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:Expired

El certificado firmante del “SignatureTimeStamp” se encuentra caducado
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:Revoked
El certificado firmante del “SignatureTimeStamp” se encuentra revocado
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:UnknownStatus
No se ha podido determinar el estado del certificado firmante del “SignatureTimeStamp”
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:InvalidCertificateChain
La cadena de certificación del certificado utilizado para la generación del atributo "SignatureTimeStamp" no es válida.
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:NotSupported
El certificado firmante del “SignatureTimeStamp” no se encuentra soportado por el Sistema
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:NotAllowed
El certificado firmante del “SignatureTimeStamp” no está recogido en la política de certificación de la aplicación
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:IdKpTimestampingExtensionNotFound
El certificado firmante del “SignatureTimeStamp” no posee la extensión crítica “id-kp-timestamping”
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:Repeated
El sello de tiempo está emitido por la misma TSA que otro sello de tiempo de la misma firma.
urn:afirma:dss:1.0:profile:XSS:resultminor: CertificateReferences:IncompletedReferences
Faltan referencias de certificados utilizados en la firma
urn:afirma:dss:1.0:profile:XSS:resultminor: CertificateReferences:InvalidFormat

El formato de las referencias no se ajustan a lo especificado en el estándar de firma
urn:afirma:dss:1.0:profile:XSS:resultminor: CertificateReferences:InvalidReferences
El formato de las referencias no se ajustan a lo especificado en el estándar de firma
urn:afirma:dss:1.0:profile:XSS:resultminor: SigAndRefsTimeStamp:InvalidSignature
La firma del Sello de Tiempo incluida en el atributo “SigAndRefsTimeStamp” no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:MismatchedSignedData
Los datos firmados por el Sello de Tiempo del atributo “SigAndRefsTimeStamp” no se corresponde con los incluidos en la firma
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:IncorrectFormat
El formato del Sello de Tiempo del atributo “SigAndRefsTimeStamp” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:InvalidSignature
La firma del certificado firmante del “SigAndRefsTimeStamp” no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:IncorrectIssuer
El emisor del certificado firmante del “SigAndRefsTimeStamp” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:NotValidYet
El certificado firmante del “SigAndRefsTimeStamp” todavía no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:Expired
El certificado firmante del “SigAndRefsTimeStamp” se encuentra caducado
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:Revoked
El certificado firmante del “SigAndRefsTimeStamp” se encuentra revocado

urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:UnknownStatus
No se ha podido determinar el estado del certificado firmante del “SigAndRefsTimeStamp”
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:InvalidCertificateChain
La cadena de certificación del certificado utilizado para la generación del atributo "SigAndRefTimeStamp" no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:NotSupported
El certificado firmante del “SigAndRefsTimeStamp” no se encuentra soportado por el Sistema
urn:afirma:dss:1.0:profile:XSS:resultminor:SigAndRefsTimeStamp:Certificate:NotAllowed
El certificado firmante del “SigAndRefsTimeStamp” no está recogido en la política de certificación de la aplicación
urn:afirma:dss:1.0:profile:XSS:resultminor: SigAndRefsTimeStamp:Certificate: IdKpTimestampingExtensionNotFound
El certificado firmante del “SigAndRefsTimeStamp” no posee la extensión crítica “id-kp-timestamping”
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:InvalidSignature
La firma del Sello de Tiempo incluida en el atributo “RefsOnlyTimeStamp” no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:MismatchedSignedData
Los datos firmados por el Sello de Tiempo del atributo “RefsOnlyTimeStamp” no se corresponde con los incluidos en la firma
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:IncorrectFormat
El formato del Sello de Tiempo del atributo “RefsOnlyTimeStamp” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:InvalidSignature

La firma del certificado firmante del “RefsOnlyTimeStamp” no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:IncorrectIssuer
El emisor del certificado firmante del “RefsOnlyTimeStamp” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:NotValidYet
El certificado firmante del “RefsOnlyTimeStamp” todavía no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:Expired
El certificado firmante del “RefsOnlyTimeStamp” se encuentra caducado
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:Revoked
El certificado firmante del “RefsOnlyTimeStamp” se encuentra revocado
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:UnknownStatus
No se ha podido determinar el estado del certificado firmante del “RefsOnlyTimeStamp”
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:InvalidCertificateChain
La cadena de certificación del certificado utilizado para la generación del atributo "RefsOnlyTimeStamp" no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:NotSupported
El certificado firmante del “RefsOnlyTimeStamp” no se encuentra soportado por el Sistema
urn:afirma:dss:1.0:profile:XSS:resultminor:RefsOnlyTimeStamp:Certificate:NotAllowed
El certificado firmante del “RefsOnlyTimeStamp” no está recogido en la política de certificación de la aplicación
urn:afirma:dss:1.0:profile:XSS:resultminor: RefsOnlyTimeStamp:Certificate: IdKpTimestampingExtensionNotFound

El certificado firmante del “RefsOnlyTimeStamp” no posee la extensión crítica “id-kp-timestamping”
urn:afirma:dss:1.0:profile:XSS:resultminor:CertAndRevValues:InvalidFormat
El formato de los atributos “RevocationValue” y/o “CertificateValue” no se ajustan a las especificaciones del formato de firma
urn:afirma:dss:1.0:profile:XSS:resultminor:CertAndRevValues:MissingRequiredReferences
Se ha detectado atributo “RevocationValue” y/o “CertificateValue” sin referencia asociada
urn:afirma:dss:1.0:profile:XSS:resultminor:CertAndRevValues:InvalidValues
El valor de los atributos “RevocationValue” y/o “CertificateValue” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:InvalidSignature
La firma del Sello de Tiempo incluida en el atributo “ArchiveTimeStamp” no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:MismatchedSignedData
Los datos firmados por el Sello de Tiempo del atributo “ArchiveTimeStamp” no se corresponde con los incluidos en la firma
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:IncorrectFormat
El formato del Sello de Tiempo del atributo “ArchiveTimeStamp” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:InvalidSignature
La firma del certificado firmante del “ArchiveTimeStamp” no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:IncorrectIssuer
El emisor del certificado firmante del “ArchiveTimeStamp” no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:NotValidYet

El certificado firmante del “ArchiveTimeStamp” todavía no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:Expired
El certificado firmante del “ArchiveTimeStamp” se encuentra caducado
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:Revoked
El certificado firmante del “ArchiveTimeStamp” se encuentra revocado
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:UnknownStatus
No se ha podido determinar el estado del certificado firmante del “ArchiveTimeStamp”
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:InvalidCertificateChain
La cadena de certificación del certificado utilizado para la generación del atributo "ArchiveTimeStamp" no es válida.
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:NotSupported
El certificado firmante del “ArchiveTimeStamp” no se encuentra soportado por el Sistema
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:Certificate:NotAllowed
El certificado firmante del “ArchiveTimeStamp” no está recogido en la política de certificación de la aplicación
urn:afirma:dss:1.0:profile:XSS:resultminor: ArchiveTimeStamp:Certificate: IdKpTimestampingExtensionNotFound
El certificado firmante del “ArchiveTimeStamp” no posee la extensión crítica “id-kp-timestamping”
urn:afirma:dss:1.0:profile:XSS:resultminor:InvalidBatchType
El tipo de petición en Lote especificada no es válida
urn:oasis:names:tc:dss:1.0:profile:archive:resultminor:ArchiveIdentifierNotFound

El identificador suministrado no ha sido encontrado en el sistema de custodia
urn:afirma:dss:1.0:profile:archive:resultminor:InvalidArchiveIdentifierType
El valor del componente afap:ArchiveIdentifierType no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:TargetSignerNotFound
El firmante objetivo no se ha encontrado en la firma
urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultminor:ResponseIdUnknown
El identificador de proceso asíncrono no es válido
urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:valid:certificate:Definitive
El certificado es válido, incluyendo su estado de revocación.
urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:valid:certificate:Temporal
El certificado es válido pero no se tiene constancia de su estado de revocación.
urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:unknown:certificate:BadCertificateFormat
El formato del certificado no es válido
urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:unknown:certificate:BadCertificateSignature
La firma del certificado no es válida
urn:oasis:names:tc:dss:1.0:profiles:XSS :resultminor:invalid:certificate:OnHold
El certificado está suspendido
urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:invalid:certificate:Revoked
El certificado se encuentra revocado

urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:invalid:certificate:Expired
El certificado se encuentra caducado
urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:invalid:certificate:NotYetValid
El certificado no es válido aun
urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:unknown:certificate:PathValidationFails
La validación de la cadena de certificación no es satisfactoria
urn:afirma:dss:1.0:profile:XSS:resultminor:X509CertificateNotProvided
La petición no incluye el certificado a validar
urn:afirma:dss:1.0:profile:XSS:resultminor:Certificate:NotAllowed
El certificado no está soportado por la política de la aplicación
urn:afirma:dss:1.0:profile:XSS:resultminor:Certificate:NotSupported
El certificado no está soportado por el sistema
urn:afirma:dss:1.0:profile:XSS:resultminor:Certificate:IncorrectIssuer
El emisor del certificado no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:Certificate:InvalidExtension
El certificado incluye extensiones no válida
urn:oasis:names:tc:dss:1.0:resultminor:GeneralError
Se ha producido un error no especificado por ningún identificador
urn:afirma:dss:1.0:profile:XSS:resultminor:PAdESInvalidContentsKey

El diccionario de firma posee una entrada Contents incorrecta.
urn:afirma:dss:1.0:profile:XSS:resultminor:PAdESInvalidMandatoryAttributes
La firma no cumple con la validación de los atributos obligatorios para una firma PAdES mejorada
urn:afirma:dss:1.0:profile:XSS:resultminor:PAdESIncompleteMandatoryAttributes
La firma no posee todos los atributos obligatorios para una firma PAdES mejorada
urn:afirma:dss:1.0:profile:XSS:resultminor:PAdESInvalidOptionalAttributes
La firma no cumple con la validación de los atributos opcionales para una firma PAdES mejorada
urn:afirma:dss:1.0:profile:XSS:resultminor:PAdESInvalidCertificateChain
La firma no cumple con la validación de la cadena de certificación
urn:afirma:dss:1.0:profile:XSS:resultminor:PAdESInvalidInnerDocumentTimeStamp
El documento PDF posee un diccionario de firma de tipo Document Time-stamp interno incorrecto
urn:afirma:dss:1.0:profile:XSS:resultminor:PAdESInvalidLatestDocumentTimeStamp
El diccionario de firma de tipo Document Time-stamp más reciente no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:InvalidXAdESReference
Alguna de las referencias de la una firma XADES no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:InvalidSignature
La firma del certificado firmante del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:IncorrectIssuer
El emisor del certificado firmante del sello de tiempo contenido en el diccionario de firma de tipo

Document Time-stamp más reciente no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:NotValidYet
El certificado firmante del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente todavía no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:Expired
El certificado del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente se encuentra caducado
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:Revoked
El certificado del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente se encuentra revocado
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:UnknownStatus
No se ha podido determinar el estado del certificado firmante del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:InvalidCertificateChain
La cadena de certificación del certificado utilizado para la generación del sello de tiempo contenido en el diccionario de tipo Document Time-stamp no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:NotSupported
El certificado firmante del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente no se encuentra soportado por el Sistema
urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate:NotAllowed
El certificado firmante del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente no está recogido en la política de certificación de la aplicación

urn:afirma:dss:1.0:profile:XSS:resultminor: LatestDocumentTimeStampDictionary:Certificate: IdKpTimestampingExtensionNotFound
El certificado firmante del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente no posee la extensión crítica “id-kp-timestamping”
urn:afirma:dss:1.0:profile:XSS:resultminor:PDFInvalidCertificationLevel
El documento PDF posee un diccionario de firma que ha sido añadido después de haber definido un diccionario de firma anterior como “Certified”.
urn:afirma:dss:1.0:profile:XSS:resultminor:ASiCStructure:MismatchedSignedData
El fichero firmado contenido dentro del fichero ZIP de la firma ASiC-S no coincide con los datos firmados por la firma CAdES Baseline o XAdES Baseline contenida dentro del fichero ZIP.
urn:afirma:dss:1.0:profile:XSS:resultminor:ASiCStructure:InvalidStructure
La estructura del fichero ZIP de la firma ASiC-S no es correcta.
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureTimeStamp:Certificate:InvalidInnerTimestampCertificate
El certificado firmante del sello de tiempo contenido dentro de un atributo signature-time-stamp que no es el más reciente de la firma, o de un elemento xades:SignatureTimeStamp que no es el más reciente de la firma, no es correcto.
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:InvalidATSHashIndex
La firma CAdES LTA-Level posee un atributo no firmado ats-hash-index incorrecto contenido dentro del atributo archive-time-stamp-v3 más reciente.
urn:afirma:dss:1.0:profile:XSS:resultminor:ArchiveTimeStamp:WithoutATSHashIndex
La firma CAdES LTA-Level posee un atributo archive-time-stamp-v3 que no contiene como atributo no firmado ats-hash-index.
urn:afirma:dss:1.0:profile:XSS:resultminor:CertAndRevValues:WithoutRevocationValues

La firma AdES LT-Level no incluye ningún valor de revocación dentro de los elementos SignedData.crls.crl ni SignedData.crls.other (en el caso de CAdES), o dentro del elemento xades:RevocationValues (en el caso de XAdES).
urn:afirma:dss:1.0:profile:XSS:resultminor:CertAndRevValues:IncompleteCertificationValues
La firma CAdES LT-Level no incluye ningún certificado dentro del elemento SignedData.certificates como un certificado de la cadena de certificación necesaria para validar la firma del certificado firmante del sello de tiempo contenido dentro de un atributo signature-time-stamp.
urn:afirma:dss:1.0:profile:XSS:resultminor:CertAndRevValues:WithoutSignatureTimeStamp
La firma CAdES LT-Level no incluye ningún sello de tiempo dentro de un atributo signature-time-stamp.
urn:afirma:dss:1.0:profile:XSS:resultminor:UnnecessaryUpgradeOperation
En la petición de actualización de firma se ha indicado como firmante objetivo uno que pertenece a una cadena de firmantes que ya está protegida por un sello de archivo. El hecho de realizar dicha actualización implicaría la invalidación del sello de archivo.

A.3.6 Identificadores de nivel de detalle en respuestas de verificación

En este anexo se indicarán los valores que puede tomar el elemento *vr:ReportDetailLevel* según las recomendaciones del perfil VR de OASIS.

Dependiendo de si la petición de verificación es de firma o certificado el valor de este componente afectará a la respuesta generada de forma distinta.

En la siguiente tabla se recogen los identificadores utilizados en una petición de verificación de firma.

vr:ReportDetailLevel
urn:oasis:names:tc:dss:1.0:reportdetail:noDetails
Por cada firma verificada solamente se devolverá el resultado final del proceso

urn:oasis:names:tc:dss:1.0:reportdetail:noPathDetails
Por cada firma verificada se retornará junto al resultado final otra información adicional (información sobre atributos firmados y no firmados, detalles sobre el proceso de verificación, etc.) Respecto de la validación de del certificado firmante sólo se devolverá el resultado final.
urn:oasis:names:tc:dss:1.0:reportdetail:allDetails
Por cada firma verificada toda la información sobre la firma y certificado firmante es devuelta. Esta es la opción por defecto, en caso de no especificar ningún modo.

En el caso de verificación de certificado las URI´s utilizadas coinciden con las expuestas en la anterior tabla, sin embargo el significado varía sustancialmente, como podemos observar en la siguiente tabla:

vr:ReportDetailLevel
urn:oasis:names:tc:dss:1.0:reportdetail:noDetails
La respuesta no incluirá el componente “vr:CertificatePathValidity” con detalles extras de validación.
urn:oasis:names:tc:dss:1.0:reportdetail:noPathDetails
La respuesta incluirá un componente “vr:CertificateValidity” dentro del elemento “vr:CertificatePathValidity” con información de validación del certificado final.
urn:oasis:names:tc:dss:1.0:reportdetail:allDetails
La respuesta incluirá un componente “vr:CertificateValidity” por cada certificado que forma la cadena de certificación dentro del elemento “vr:CertificatePathValidity”.

A.3.7 Identificadores de tareas de validación

En este anexo se detalla las URI´s utilizadas para identificar las distintas tareas y resultados que forman el proceso de validación de una firma electrónica

El proceso de validación de una firma electrónica se puede dividir en un conjunto de subprocesos que determinarán el estado de la firma, el formato de la firma determinará que tareas deben ejecutarse. En la siguiente En la siguiente tabla se puede observar que tareas de validación se realizarían para los distintos formatos de firma.

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA ASN.1													
	CMS/PKCS7	CMS-T	CAdES-BES	CAdES-EPES	CAdES-T	CAdES-C	CAdES-X1	CAdES-X2	CAdES-XL	CAdES-A	CAdES B-Level	CAdES T-Level	CAdES LT-Level	CAdES LTA-Level
Validación del "Core" de la Firma	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validación del Certificado Firmante	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validación del "KeyInfo"	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validación del "SigningTime"	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validación del "Core" del Sello de Tiempo sobre la Firma		✓			✓	✓	✓	✓	✓	✓		✓	✓	✓
Validación del Certificado del Sello de Tiempo sobre la Firma		✓			✓	✓	✓	✓	✓	✓		✓	✓	✓
Validación de los Atributos de Firma en base a la Política de Firma				✓	?	?	?	?	?	?	?	?	?	?

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA ASN.1													
	CMS/PKCS7	CMS-T	CAdES-BES	CAdES-EPES	CAdES-T	CAdES-C	CAdES-X1	CAdES-X2	CAdES-XL	CAdES-A	CAdES B-Level	CAdES T-Level	CAdES LT-Level	CAdES LTA-Level
Validación de la Referencia de los Certificados						✓	✓	✓	✓	✓				
Validación del "Core" del Sello de Tiempo AdES-X1							✓		?	?				
Validación del Certificado del Sello de tiempo AdES-X1							✓		?	?				
Validación del "Core" del Sello de Tiempo AdES-X2								✓	?	?				
Validación del Certificado del Sello de tiempo AdES-X2								✓	?	?				
Validación de las Evidencias del Estado de Revocación y Cadena de Certificación									✓	✓			✓	✓

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA ASN.1													
	CMS/PKCS7	CMS-T	CAdES-BES	CAdES-EPES	CAdES-T	CAdES-C	CAdES-X1	CAdES-X2	CAdES-XL	CAdES-A	CAdES B-Level	CAdES T-Level	CAdES LT-Level	CAdES LTA-Level
Validación del "Core" del Sello de Tiempo Archivado										✓				✓
Validación del Certificado del Sello de Tiempo Archivado										✓				✓

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA XML														
	XMLDSig	OOXML	XAdES-BES	XAdES-EPES	XAdES-T	XAdES-C	XAdES-X1	XAdES-X2	XAdES-XL	XAdES-A	XAdES B-Level	XAdES T-Level	XAdES LT-Level	XAdES LTA-Level	ODF
Validación del "Core" de la Firma	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validación del Certificado Firmante	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validación del "KeyInfo"	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA XML														
	XMLDSig	OOXML	XAdES-BES	XAdES-EPES	XAdES-T	XAdES-C	XAdES-X1	XAdES-X2	XAdES-XL	XAdES-A	XAdES B-Level	XAdES T-Level	XAdES LT-Level	XAdES LTA-Level	ODF
Validación del "SigningTime"			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Validación del "Core" del Sello de Tiempo sobre la Firma					✓	✓	✓	✓	✓	✓		✓	✓	✓	
Validación del Certificado del Sello de Tiempo sobre la Firma					✓	✓	✓	✓	✓	✓		✓	✓	✓	
Validación de los Atributos de Firma en base a la Política de Firma				✓	?	?	?	?	?	?	?	?	?	?	
Validación de los Algoritmos de Firma y Resumen en base a la Política de Firma				✓	?	?	?	?	?	?	?	?	?	?	
Validación de la Referencia de los Certificados						✓	✓	✓	✓	✓					
Validación del "Core" del Sello de Tiempo AdES-X1							✓		?	?					
Validación del Certificado del Sello de tiempo AdES-X1							✓		?	?					
Validación del "Core" del Sello de Tiempo AdES-X2								✓	?	?					

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA XML													
	XMLDSig	OOXML	XAdES-BES	XAdES-EPES	XAdES-T	XAdES-C	XAdES-X1	XAdES-X2	XAdES-XL	XAdES-A	XAdES B-Level	XAdES T-Level	XAdES LT-Level	XAdES LTA-Level	ODF
Validación del Certificado del Sello de tiempo AdES-X2								✓	?	?					
Validación de las Evidencias del Estado de Revocación y Cadena de Certificación									✓	✓			✓	✓	
Validación del "Core" del Sello de Tiempo Archivado										✓				✓	
Validación del Certificado del Sello de Tiempo Archivado										✓				✓	

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA PDF								
	PDF	PAdES Basic	PAdES-BES	PAdES-EPES	PAdES-LTV	PAdES B-Level	PAdES T-Level	PAdES LT-Level	PAdES LTA-Level
Validación del "Core" de la Firma	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validación del Certificado Firmante	✓	✓	✓	✓	✓	✓	✓	✓	✓

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA PDF								
	PDF	PAdES Basic	PAdES-BES	PAdES-EPES	PAdES-LTV	PAdES B-Level	PAdES T-Level	PAdES LT-Level	PAdES LTA-Level
Validación del "KeyInfo"		✓	✓	✓	?	✓	✓	✓	✓
Validación del "SigningTime"		✓			?				
Validación de los Atributos de Firma en base a la Política de Firma				✓	?	?	?	?	?
Validación del "Core" del Sello de Tiempo sobre la Firma		?	?	?	?	?	?	?	?
Validación del Certificado del Sello de Tiempo sobre la Firma		?	?	?	?	?	?	?	?
Validación del Nivel de Certificación de un Documento PDF	✓	✓	✓	✓	✓	✓	✓	✓	✓
Validación de la Entrada Contents del Diccionario de Firma		✓	✓	✓	?	✓	✓	✓	✓
Validación de los Atributos Opcionales para PAdES		✓	✓	✓	?	✓	✓	✓	✓
Validación de los Atributos Obligatorios para PAdES			✓	✓	?	✓	✓	✓	✓
Validación del Diccionario de Firma Más Reciente de Tipo Document Time-stamp					✓				✓
Validación del Certificado Firmante del Diccionario de Firma Más Reciente de Tipo Document Time-stamp					✓				✓
Validación de los Diccionarios de Firma Internos de Tipo Document Time-stamp					?				?

TAREAS DE VALIDACIÓN	FORMATOS DE FIRMA ASiC			
	ASiC-S B-Level	ASiC-S T-Level	ASiC-S LT-Level	ASiC-S LTA-Level
Validación de la Estructura de la Firma ASiC-S	✓	✓	✓	✓
Validación del “Core” de la Firma	✓	✓	✓	✓
Validación del Certificado Firmante	✓	✓	✓	✓
Validación del “KeyInfo”	✓	✓	✓	✓
Validación del “SigningTime”	✓	✓	✓	✓
Validación del “Core” del Sello de Tiempo sobre la Firma		✓	✓	✓
Validación del Certificado del Sello de Tiempo sobre la Firma		✓	✓	✓
Validación de los Atributos de Firma en base a la Política de Firma	?	?	?	?
Validación de los Algoritmos de Firma y Resumen en base a la Política de Firma	?	?	?	?
Validación de las Evidencias del Estado de Revocación y Cadena de Certificación			✓	✓
Validación del “Core” del Sello de Tiempo Archivado				✓
Validación del Certificado del Sello de Tiempo Archivado				✓

En la siguiente tabla se representa las URI's que permiten identificar las tareas expuestas anteriormente.

En la columna "Type" se representan los identificadores de las tareas de validación, estos valores se corresponden con los que puede tener el atributo "Type" de los elementos "*dss:ValidDetail*", "*dss:InvalidDetail*" o "*dss:IndeterminateDetail*":

Tarea	Type*	Descripción
Validación del "Core" de la Firma	*SignatureCore*	Proceso de validación de la firma realizada con la clave pública y validación de los datos firmados
Validación del Certificado Firmante	*SignerCertificateValidation*	Proceso de validación del certificado firmante y la cadena de certificación del mismo
Validación del "KeyInfo"	*KeyInfoValidation*	Validación de la información sobre la clave publica del firmante incluida en la firma
Validación del "SigningTime"	*SigningTime*	Validación del atributo firmado "SigningTime"
Validación del "Core" del Sello de Tiempo sobre la Firma	*SignatureTimeStamp*	Validación del atributo "SignatureTimeStamp" (Sello de tiempo sobre la firma).
Validación del Certificado del Sello de Tiempo sobre la Firma	*SignatureTimeStampCertificate*	Validación del certificado de la TSA utilizado para generar el sello de tiempo del atributo "SignatureTimeStamp"
Validación de los Atributos de Firma en base a la Política de Firma	*MandatoryPolicyAttributes*	Validación del resumen de la política contenido en la firma y de los atributos de firma en base a la politica

Tarea	Type*	Descripción
Validación de los Algoritmos de Firma y Resumen en base a la Política de Firma	*PolicyAlgorithms*	Proceso de validación de los algoritmos de firma y resumen utilizados en la generación de la misma
Validación de la Referencia de los Certificados	*CompleteCertificateRefs*	Proceso de validación de las referencias de los certificados contenidos en la firma
Validación del "Core" del Sello de Tiempo AdES-X1	*SigAndRefsTimeStamp*	Proceso de validación del "Core" del Sello de Tiempo sobre la estructura AdES-C
Validación del Certificado del Sello de Tiempo AdES-X1	*SigAndRefsTimeStampCertificate*	Validación del certificado de la TSA utilizado para la generación del sellado de tiempo sobre la estructura AdES-C
Validación del "Core" del Sello de Tiempo AdES-X2	*RefsOnlyTimeStamp*	Tarea de validación del Sello de Tiempo sobre las referencias de certificados y evidencias del estado de revocación
Validación del Certificado del Sello de Tiempo AdES-X2	*RefsOnlyTimeStampCertificate*	Tarea de validación del certificado de la TSA utilizado en la generación del Sello de Tiempo sobre las referencias de certificados y evidencias del estado de revocación
Validación de las Evidencias del Estado de Revocación y Cadena de Certificación	*CompleteRevAndCertValues*	Tarea de validación de las evidencias del estado de revocación y cadena de certificación contenidas en la firma

Tarea	Type*	Descripción
Validación del "Core" del Sello de Tiempo de Archivado.	*ArchiveTimeStamp*	Validación del "Core" del Sello de Tiempo de Archivado.
Validación del Certificado del Sello de Tiempo de Archivado.	*ArchiveTimeStampCertificate*	Validación del certificado utilizado para la generación del Sello de Tiempo de archivado.
Validación de la Entrada Contents del Diccionario de Firma.	*PAdESContentsKey*	Validación de la entrada Contents del diccionario de firma de una firma PAdES.
Validación de los Atributos Obligatorios para PAdES.	*PAdESMandatoryAttributes*	Validación del conjunto de atributos obligatorios que debe cumplir una firma PAdES.
Validación de los Atributos Opcionales para PAdES.	*PAdESOptionalAttributes*	Validación del conjunto de atributos opcionales que debe cumplir una firma PAdES.
Validación de los Diccionarios de Firma Internos de Tipo Document Time-stamp.	*PAdESInnerDocTimeStampDictionaries*	Validación del conjunto de diccionarios de firma internos (aquellos que no son el más reciente) de tipo Document Time-stamp contenidos en un documento PDF.

Tarea	Type*	Descripción
Validación del Diccionario de Firma Más Reciente de Tipo Document Time-stamp.	*PAdESLatestDocTimeStamp*	Validación del diccionario de firma más reciente de tipo Document Time-stamp contenido en un documento PDF.
Validación del Certificado Firmante del Diccionario de Firma Más Reciente de Tipo Document Time-stamp.	*PAdESLatestDocTimeStampCertificate*	Validación del certificado firmante de la firma perteneciente al sello de tiempo inluido en el diccionario de firma más reciente de tipo Document Time-stamp contenido en un documento PDF.
Validación del Nivel de Certificación de un Documento PDF	*PDFCertificationLevel*	Validación de que no exista ningún diccionario de firma añadido al documento PDF después de que se haya añadido un diccionario de firma "Certified".
Validación de la Estructura de la Firma ASiC-S	*ASiCSignatureStructure*	Validación de que la estructura y contenido del fichero ZIP que constituye la firma ASiC-S.

***** Los valores expuestos en la columna debe ir precedidos de la cadena "urn:afirma:dss:1.0:profile:XSS:detail:"

Durante la ejecución de la tarea se puede obtener un resultado no satisfactorio, en la siguiente tabla se representa los errores identificados en este perfil para cada una de las tareas anteriormente expuestas.

En la columna "Code" se representas los identificadores de resultado para la tarea en cuestión, estos valores se corresponden con los que pueden incluirse en los elementos "*dss:Code*" de los componentes "*dss:InvalidDetail*" o "*dss:IndeterminateDetail*":

Tarea	Code*	Descripción
Validación del "Core" de la Firma	*SignatureCore:code:InvalidSignature*	Firma no válida
	SignatureCore:code:InvalidReference	Alguna de las referencias incluidas en la firma no es válida
	SignatureCore:code:MismatchedSignedData	Los datos pasados en la petición no se corresponden con los firmados
	SignatureCore:code:SignedDataNotProvided	No se han especificado los datos originalmente firmados para validar la firma explícita
	SignatureCore:code:InvalidReferenceType	Alguna de las referencias incluidas en la firma no tiene un tipo válido
	code:GeneralError	Error no categorizado.
Validación del Certificado Firmante	*Certificate:code:NotSupported*	Certificado no soportado
	Certificate:code:NotAllowed	El certificado no esta entre los habilitados para la aplicación
	Certificate:code:InvalidSignature	La firma del certificado no es válida
	Certificate:code:IncorrectIssuer	El emisor de certificado no es válido
	Certificate:code:NotValidYet	El certificado no es válido aun
	Certificate:code:Expired	El certificado está caducado

	Certificate:code:Revoked	El certificado está revocado
	Certificate:code:UnknownStatus	No se ha podido conocer su estado de revocación
	Certificate:code:InvalidChain	La cadena de certificación no es válida
	SignerCertificateValidation:code:InvalidNotSignerCertificate	La firma contiene un certificado (no firmante) no válido. Este error se puede presentar en firmas XML.
	Certificate:code:CertificatePolicyNotSupported	El certificado no esta soportado por la política de firma. Este error sólo se puede producir en firmas AdES-EPES o AdES con política de firma
	Certificate:code:CertificateNotSupportedBySignaturePolicy	La politica del certificado no está soportada por la política de firma. Este error sólo se puede producir en firmas AdES-EPES o AdES con política de firma
	Certificate:code:InvalidCertificateKeyLength	La longitud de clave del certificado firmante no se ajusta a lo especificado por la política de firma. Este error sólo se puede producir en firmas AdES-EPES o AdES con política de firma
	code:GeneralError	Error no categorizado.

Validación del "KeyInfo"	*KeyInfoValidation:code:MismatchedKeyInfo*	La información del firmante no se corresponde con la real
	KeyInfoValidation:code:SigningCertificateNotIncluded	La firma no incluye el atributo SigningCertificate
	code:GeneralError	Error no categorizado
Validación del "SigningTime"	*SigningTime:code:InvalidPeriod*	El instante recogido en el SigningTime es posterior al momento de validación
	code:GeneralError	Error no categorizado
Validación del "Core" del Sello de Tiempo sobre la Firma	*SignatureTimeStamp:code:InvalidSignature*	La firma del TST no es válida
	SignatureTimeStamp:code:MismatchedSignedData	Los datos firmados por la TSA no se corresponden con los de la firma
	SignatureTimeStamp:code:IncorrectFormat	El formato del sello de tiempo no es válido
	SignatureTimeStamp:code:RepeatedTSA	Existe un sello de tiempo emitido por la misma TSA que otro sello de tiempo de la misma firma.
	code:GeneralError	Error no categorizado
Validación del Certificado del Sello de Tiempo sobre la Firma	*Certificate:code:NotSupported*	Certificado no soportado
	Certificate:code:NotAllowed	El certificado no esta entre los habilitados para la aplicación
	Certificate:code:InvalidSignature	La firma del certificado no es válida

	Certificate:code:IncorrectIssuer	El emisor de certificado no es válido
	Certificate:code:NotValidYet	El certificado no es válido aun
	Certificate:code:Expired	El certificado está caducado
	Certificate:code:Revoked	El certificado está revocado
	Certificate:code:UnknownStatus	No se ha podido conocer su estado de revocación
	Certificate:code:InvalidChain	La cadena de certificación no es válida
	Certificate:code:IdKpTimestampingExtensionNotFound	El certificado no contiene la extensión crítica "id-kp-timestamping"
	SignatureTimeStampCertificate:code:InvalidInnerCertificate	El certificado firmante de un sello de tiempo, que no es el más reciente, contenido en un atributo signature-time-stamp (caso de CAdES Baseline), o contenido en un elemento xades:SignatureTimeStamp (caso de XAdES Baseline), no es correcto.
	code:GeneralError	Error no categorizado
Validación de los Atributos de Firma en base a la Política de Firma	*MandatoryPolicyAttributes:code:IncompleteAttributes*	Los atributos incluidos en la firma no se corresponden con los especificados en la política. Falta algún atributo.

	MandatoryPolicyAttributes:code:InvalidAttributes	El valor de los atributos incluidos en la firma no se corresponde con el valor especificado en la política de firma
	MandatoryPolicyAttributes:code:SignatureOutOfPolicyPeriod	La firma fue realizada fuera del periodo de validez de la política de firma
	MandatoryPolicyAttributes:code:InvalidDigest	El resumen de la política de firma no se corresponde con el valor real del mismo
	PolicyAlgorithms:code:InvalidSignatureFormat	El formato de la firma no se ajusta a la política
	MandatoryPolicyAttributes:code:SignaturePolicyNotSupported	La política de firma utilizada no está soportada por el sistema
	code:GeneralError	Error no categorizado
Validación de los Algoritmos de Firma y Resumen en base a la Política de Firma	*PolicyAlgorithms:code:InvalidDigestAlgorithms*	Se ha utilizado algoritmo de resumen no contemplado por la política
	PolicyAlgorithms:code:InvalidSignatureAlgorithms	Se ha utilizado algoritmo de firma no contemplado por la política
	code:GeneralError	Error no categorizado
Validación de las Referencia de los Certificados	*CompleteCertificateRefs:code:InvalidReferences*	Las referencias contenidas son inválidas o no se corresponden con los valores obtenidos

	CompleteCertificateRefs:code:IncompletedReferences	No se encuentran todas las referencias a certificados implicados en la firma en una firma avanzada
	CompleteCertificateRefs:code:InvalidFormat	La firma no incorpora alguno de los atributos necesarios para la validación AdES-C
	code:GeneralError	Error no categorizado.
Validación del "Core" del Sello de Tiempo AdES-X1	*SigAndRefsTimeStamp:code:InvalidSignature*	La firma del TST no es válida
	SigAndRefsTimeStamp:code:MismatchedSignedData	Los datos firmados por la TSA no se corresponden con los de la firma
	SigAndRefsTimeStamp:code:InvalidFormat	El formato del sello de tiempo no es válido
	SigAndRefsTimeStamp:code:MissingRequiredValidationData	La firma no incorpora alguno de los atributos necesarios para la validación AdES-X1
	code:GeneralError	Error no categorizado
Validación del Certificado del Sello de Tiempo AdES-X1	*Certificate:code:NotSupported*	Certificado no soportado
	Certificate:code:NotAllowed	El certificado no esta entre los habilitados para la aplicación
	Certificate:code:InvalidSignature	La firma del certificado no es válida
	Certificate:code:IncorrectIssuer	El emisor de certificado no es válido

	Certificate:code:NotValidYet	El certificado no es válido aun
	Certificate:code:Expired	El certificado está caducado
	Certificate:code:UnknownStatus	No se ha podido conocer su estado de revocación
	Certificate:code:InvalidChain	La cadena de certificación no es válida
	Certificate:code:IdKpTimestampingExtensionNotFound	El certificado no contiene la extensión crítica "id-kp-timestamping"
	code:GeneralError	Error no categorizado.
Validación del "Core" del Sello de Tiempo AdES-X2	*RefsOnlyTimeStamp:code:InvalidSignature*	La firma del TST no es válida
	RefsOnlyTimeStamp:code:InvalidFormat	El formato del sello de tiempo no es válido
	RefsOnlyTimeStamp:code:MismatchedSignedData	Los datos firmados por la TSA no se corresponden con los de la firma
	RefsOnlyTimeStamp:code:MissingRequiredValidationData	La firma no incorpora alguno de los atributos necesarios para la validación AdES-X2
	code:GeneralError	Error no categorizado
Validación del Certificado del Sello de Tiempo AdES-X2	*Certificate:code:NotSupported*	Certificado no soportado
	Certificate:code:NotAllowed	El certificado no esta entre los habilitados para la aplicación
	Certificate:code:InvalidSignature	La firma del certificado no es

		válida
	Certificate:code:IncorrectIssuer	El emisor de certificado no es válido
	Certificate:code:NotValidYet	El certificado no es válido aun
	Certificate:code:Expired	El certificado está caducado
	Certificate:code:UnknownStatus	No se ha podido conocer su estado de revocación
	Certificate:code:InvalidChain	La cadena de certificación no es válida
	Certificate:code:IdKpTimestampingExtensionNotFound	El certificado no contiene la extensión crítica "id-kp-timestamping"
	code:GeneralError	Error no categorizado
Validación de las evidencias del estado de revocación y cadena de certificación	*CompleteRevAndCertValues:code:InvalidValues*	Las referencias contenidas son inválidas o no se corresponden con los valores obtenidos
	CompleteRevAndCertValues:code:MissingRequiredReferences	No se encuentran todas los referencias a certificados o evidencia del estado de revocación implicados en la generación de una firma avanzada
	CompleteRevAndCertValues:code:InvalidFormat	La firma no incorpora alguno de los atributos necesarios para la validación -XL
	CompleteRevAndCertValues:code:WithoutRevocationV	La firma no incluye ningún

	alues	valor de revocación dentro de los elementos SignedData.crls.crl y SignedData.crls.other (caso de CAdES Baseline) o dentro del elemento xades:RevocationValues (caso de XAdES Baseline).
	CompleteRevAndCertValues:code:IncompleteCertificationValues	La firma CAdES LT-Level no incluye un certificado dentro del elemento SignedData.certificates como un certificado de la cadena de certificación necesario para validar el certificado firmante del sello de tiempo contenido en un atributo signature-time-stamp.
	CompleteRevAndCertValues:code:WithoutSignatureTimeStamps	La firma CAdES LT-Level no incluye ningún sello de tiempo dentro del atributo signature-time-stamp.
	code:GeneralError	Error no categorizado
Validación del "Core" del Sello de Tiempo de Archivado	*ArchiveTimeStamp:code:InvalidSignature*	La firma del TST no es válida
	ArchiveTimeStamp:code:InvalidFormat	El formato del sello de tiempo no es válido
	ArchiveTimeStamp:code:MismatchedSignedData	Los datos firmados por la TSA no se corresponden con los de la firma
	ArchiveTimeStamp:code:InvalidATSHashIndexAttribute	La firma CAdES LTA-Level

		posee un atributo no firmado ats-hash-index no correcto contenido dentro del atributo archive-time-stamp-v3 más reciente.
	ArchiveTimeStamp:code:WithoutATSHashIndexAttribute	La firma CAdES LTA-Level posee un atributo archive-time-stamp-v3 que no contiene un atributo no firmado ats-hash-index.
	code:GeneralError	Error no categorizado
Validación del Certificado del Sello de Tiempo de Archivado.	*Certificate:code:NotSupported*	Certificado no soportado
	Certificate:code:NotAllowed	El certificado no esta entre los habilitados para la aplicación
	Certificate:code:InvalidSignature	La firma del certificado no es válida
	Certificate:code:IncorrectIssuer	El emisor de certificado no es válido
	Certificate:code:NotValidYet	El certificado no es válido aun
	Certificate:code:Expired	El certificado está caducado
	Certificate:code:UnknownStatus	No se ha podido conocer su estado de revocación
	Certificate:code:InvalidChain	La cadena de certificación no es válida
	Certificate:code:IdKpTimestampingExtensionNotFound	El certificado no contiene la extensión crítica "id-kp-timestamping"

	ArchiveTimeStampCertificate:code:InvalidInnerCertificate	El certificado firmante de un sello de tiempo, que no es el más reciente, contenido en un atributo archive-time-stamp-v3 (caso de CAdES Baseline), o contenido en un elemento xades:ArchiveTimeStamp o xadesv141:ArchiveTimeStamp (caso de XAdES Baseline), no es correcto.
	code:GeneralError	Error no categorizado
Validación de la Entrada Contents del Diccionario de Firma.	*PAdESContentsKey:code:InvalidContentsKey*	Entrada Contents incorrecta
	code:GeneralError	Error no categorizado
Validación de los Atributos Obligatorios para PAdES.	*PAdESMandatoryAttributes:code:InvalidAttributes*	Atributos obligatorios incorrectos
	PAdESMandatoryAttributes:code:IncompleteAttributes	Atributos obligatorios incompletos
	code:GeneralError	Error no categorizado
Validación de los Atributos Opcionales para PAdES.	*PAdESOptionalAttributes:code:InvalidAttributes*	Atributos opcionales incorrectos
	code:GeneralError	Error no categorizado
Validación de los Diccionarios de Firma Internos de Tipo Document Time-stamp.	*PAdESInnerDocTimeStampDictionaries:code:InvalidContentsKey*	Entrada Contents incorrecta
	PAdESInnerDocTimeStampDictionaries:code:InvalidDictionaryStructure	Estructura del diccionario de firma de tipo Document Time-

		stamp incorrecta
	PAdESInnerDocTimeStampDictionaries:code:InvalidSigningTimeTST	Fecha de generación del sello de tiempo superior a la fecha de validación del mismo
	PAdESInnerDocTimeStampDictionaries:code:InvalidCertificateChain	Cadena de certificación no válida
	code:GeneralError	Error no categorizado
Validación del Diccionario de Firma Más Reciente de Tipo Document Time-stamp.	*PAdESLatestDocTimeStamp:code:InvalidContentsKey*	Entrada Contents incorrecta
	PAdESLatestDocTimeStamp:code:InvalidSigningTimeTST	Fecha de generación del sello de tiempo superior a la fecha de validación del mismo
	PAdESLatestDocTimeStamp:code:InvalidSignatureTST	La firma del TST no es válida
	PAdESLatestDocTimeStamp:code:InvalidDictionaryStructure	Estructura del diccionario de firma de tipo Document Time-stamp incorrecta
	code:GeneralError	Error no categorizado
Validación del Certificado Firmante del Diccionario de Firma Más Reciente de Tipo Document Time-stamp.	*Certificate:code:NotSupported*	Certificado no soportado
	Certificate:code:NotAllowed	El certificado no esta entre los habilitados para la aplicación
	Certificate:code:InvalidSignature	La firma del certificado no es válida
	Certificate:code:IncorrectIssuer	El emisor de certificado no es válido
	Certificate:code:NotValidYet	El certificado no es válido aún

	Certificate:code:Expired	El certificado está caducado
	Certificate:code:Revoked	El certificado está revocado
	Certificate:code:UnknownStatus	No se ha podido conocer su estado de revocación
	Certificate:code:InvalidChain	La cadena de certificación no es válida
	Certificate:code:IdKpTimestampingExtensionNotFound	El certificado no contiene la extensión crítica "id-kp-timestamping"
	code:GeneralError	Error no categorizado
Validación del Nivel de Certificación de un Documento PDF	*PDFCertificationLevel:InvalidStatus*	Un diccionario de sello de tiempo ha sido añadido después de añadir un diccionario de sello de tiempo definido como "Certified"
	code:GeneralError	Error no categorizado
Validación de la Estructura de la Firma ASiC-S	*ASiCSignatureStructure:code:MismatchedSignedData*	El fichero firmado contenido dentro del fichero ZIP de la firma ASiC-S no coincide con los datos firmados por la firma CAdES Baseline o XAdES Baseline contenida dentro del fichero ZIP.
	ASiCSignatureStructure:code:InvalidStructure	La estructura del fichero ZIP de la firma ASiC-S no es correcta.
	code:GeneralError	Error no categorizado

* Los valores expuestos en la columna debe ir precedidos de la cadena "urn:afirma:dss:1.0:profile:XSS:detail:"

A.3.8 Identificadores del componente "*vr:FormatOk*"

En la siguiente tabla se representa los valores admitidos por el componente "*vr:FormatOK*" para verificación del formato una firma electrónica.

Type*	Code*	Descripción
SignatureFormat	SignatureFormat:code:ValidFormat	El formato de la firma es válido
SignatureFormat	SignatureFormat:code:IncorrectFormat	El formato de la firma no es correcto

* Los valores expuestos en la columna debe ir precedidos de la cadena "urn:afirma:dss:1.0:profile:XSS:detail:"

A.3.9 Identificadores del componente *"vr:SigMathOK"*

En este anexo se recoge los valores que puede tomar el elemento "*vr:SigMathOK*" en una respuesta de verificación de firma.

Este componente informa sobre el resultado de realizar la verificación de una firma mediante su correspondiente clave pública, dependiendo de la naturaleza del componente verificado (firma electrónica, sello de tiempo, certificado, CRL o respuesta OCSP) su contenido puede variar susceptiblemente.

En la siguiente tabla se recogen los valores admitidos para la verificación de una firma electrónica o sello de tiempo.

Type*	Code*	Descripción
SignatureCore	SignatureCore:code:ValidSignature	La clave pública valida la firma realizada
SignatureCore	SignatureCore:code:InvalidSignature	La firma realizada no es valida

* Los valores expuestos en la columna debe ir precedidos de la cadena "urn:afirma:dss:1.0:profile:XSS:detail:"

En la tabla mostrada a continuación se detallan los valores admitidos para la verificación de la firma realizada sobre un certificado.

Type*	Code*	Descripción
Certificate	Certificate:code:ValidSignature	La firma del certificado es correcta
Certificate	Certificate:code:InvalidSignature	La firma del certificado no es válida
Certificate	Certificate:code:UnknownStatusSignature	No se ha podido determinar la validez de la firma del certificado

* Los valores expuestos en la columna debe ir precedidos de la cadena "urn:afirma:dss:1.0:profile:XSS:detail:"

Para la verificación de evidencias de revocación (CRL u OCSP) los valores admitidos se recogen en la siguiente tabla:

Type*	Code*	Descripción
RevocationStatusEvidence	RevocationStatusEvidence:code:ValidSignature	La firma de la CRL u OCSP es válida
RevocationStatusEvidence	RevocationStatusEvidence:code:InvalidSignature	La firma de la CRL u OCSP no es válida

* Los valores expuestos en la columna debe ir precedidos de la cadena "urn:afirma:dss:1.0:profile:XSS:detail:"

A.3.10 Identificadores del componente "*vr:PathValiditySummary*"

En la siguiente tabla se representa los valores admitidos por el componente "*vr:PathValiditySummary*" para informar sobre el resultado de verificación de un certificado.

Type*	Code*	Descripción
Certificate	*Certificate:code:Valid*	El certificado es válido
Certificate	*Certificate:code:NotSupported*	El certificado no se encuentra soportado por el sistema
Certificate	*Certificate:code:NotAllowed*	El certificado no se encuentra entre los certificados permitidos para la aplicación
Certificate	*Certificate:code:InvalidSignature*	La firma del certificado no es válida
Certificate	*Certificate:code:IncorrectIssuer*	El emisor del certificado no es válido.
Certificate	*Certificate:code:Expired*	El certificado se encuentra caducado
Certificate	*Certificate:code:NotValidYet*	El certificado no es válido aun.
Certificate	*Certificate:code:InvalidExtension*	El certificado contiene extensiones inválidas
Certificate	*Certificate:code:Revoked*	El certificado se encuentra revocado
Certificate	*Certificate:code:UnknownStatus*	No se ha podido determinar el estado de revocación del certificado

Type*	Code*	Descripción
Certificate	*Certificate:code: IdKpTimestampingExtensionNotFound*	El certificado no posee la extensión crítica "id-kp-timestamping"
ArchiveTimeStampCertificate	*ArchiveTimeStampCertificate:code: InvalidInnerCertificate*	El certificado firmante de un sello de tiempo, que no es el más reciente, contenido en un atributo archive-time-stamp-v3 (caso de CAdES Baseline), o contenido en un elemento xades:ArchiveTimeStamp o xadesv141:ArchiveTimeStamp (caso de XAdES Baseline), no es correcto.
SignatureTimeStampCertificate	*SignatureTimeStampCertificate:code: InvalidInnerCertificate*	El certificado firmante de un sello de tiempo, que no es el más reciente, contenido en un atributo signature-time-stamp (caso de CAdES Baseline), o contenido en un elemento xades:SignatureTimeStamp (caso de XAdES Baseline), no es correcto.

***** Los valores expuestos en la columna debe ir precedidos de la cadena "urn:afirma:dss:1.0:profile:XSS:detail:"

A.4 Ejemplos de Peticiones y Respuesta

A continuación se detallan distintos ejemplos de peticiones y respuestas DSS a los servicios detallados en el presente documento.

A.4.1 Ejemplos de Firma Delegada Simple

Ejemplo 1. Firma sobre un documento incluido en la petición.

En la siguiente figura se muestra un ejemplo de petición de firma de servidor, en la cual el documento a firmar no es XML y la firma que se desea realizar es CAdES-T implícita.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:InputDocuments>

                <dss:Document>
        <dss:Base64Data><![CDATA[IyBSdXRh....]]></dss:Base64Data>

                </dss:Document>

        </dss:InputDocuments>

        <dss:OptionalInputs>

                <dss:ClaimedIdentity>

                        <dss:Name>tester</dss:Name>

                </dss:ClaimedIdentity>
```

```
                    <dss:KeySelector>
                        <ds:KeyInfo>
                            <ds:KeyName>servidor</ds:KeyName>
                        </ds:KeyInfo>
                    </dss:KeySelector>
                    <afxp:ReferenceId>id_referencia</afxp:ReferenceId>
                    <dss:SignatureType>http://uri.etsi.org/01733/v1.7.3#</dss:SignatureType>
                    <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-
T</ades:SignatureForm>

            <afxp:HashAlgorithm>http://www.w3.org/2001/04/xmlenc#sha256</afxp:HashAlgorith
m>
                    <afxp:AdditionalDocumentInfo>

            <afxp:DocumentName>configuration.properties</afxp:DocumentName>
                        <afxp:DocumentType>properties</afxp:DocumentType>
                    </afxp:AdditionalDocumentInfo>
                    <dss:IncludeEContent/>
            </dss:OptionalInputs>
</dss:SignRequest>
```

El mensaje de respuesta sería el siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:Result>


        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                <dss:ResultMessage xml:lang="es">Proceso de generación de firma en servidor
realizado correctamente.</dss:ResultMessage>

        </dss:Result>

        <dss:OptionalOutputs>

                <dss:SignatureType>http://uri.etsi.org/01733/v1.7.3#</dss:SignatureType>

                <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-
T</ades:SignatureForm>

                <xss:ArchiveInfo>

                        <arch:ArchiveIdentifier>1228746420437004</arch:ArchiveIdentifier>

                </xss:ArchiveInfo>

        </dss:OptionalOutputs>

        <dss:SignatureObject>

                <dss:Base64Signature
Type="http://uri.etsi.org/01733/v1.7.3#"><![CDATA[MIIQjQ....]]></dss:Base64Signature>
```

```
            </dss:SignatureObject>

</dss:SignResponse>
```

Ejemplo 2. Firma sobre un documento custodiado en @firma

En el siguiente ejemplo se muestra una petición de firma de servidor en la cual el documento ya se encuentra registrado.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:InputDocuments>

                        <dss:Other>

                                    <afxp:DocumentArchiveId>62</afxp:DocumentArchiveId>

                        </dss:Other>

            </dss:InputDocuments>

            <dss:OptionalInputs>

                        <dss:ClaimedIdentity>

                                    <dss:Name>tester</dss:Name>

                        </dss:ClaimedIdentity>

                        <dss:KeySelector>
```

```
                    <ds:KeyInfo>
                        <ds:KeyName>servidor</ds:KeyName>
                    </ds:KeyInfo>
                </dss:KeySelector>
                <afxp:ReferenceId>id_referencia</afxp:ReferenceId>
                <dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>

        <afxp:HashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</afxp:HashAlgorithm>

        <afxp:XMLSignatureMode>urn:afirma:dss:1.0:profile:XSS:XMLSignatureMode:Enveloped
Mode</afxp:XMLSignatureMode>
        </dss:OptionalInputs>
</dss:SignRequest>
```

La respuesta al anterior mensaje sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"    xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
        <dss:Result>
```

```
                    <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                    <dss:ResultMessage xml:lang="es">Proceso de generación de firma en servidor realizado correctamente.</dss:ResultMessage>

            </dss:Result>

            <dss:OptionalOutputs>

                    <dss:DocumentWithSignature>

                            <dss:Document ID="BCCIHEHIJFABF2">

                                    <dss:Base64XML><![CDATA[PD94b....]]></dss:Base64XML>

                            </dss:Document>

                    </dss:DocumentWithSignature>

                    <dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>


            <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES</ades:SignatureForm>

                    <xss:ArchiveInfo>

                            <arch:ArchiveIdentifier>1228746420437011</arch:ArchiveIdentifier>

                    </xss:ArchiveInfo>

            </dss:OptionalOutputs>

            <dss:SignatureObject>

                    <dss:SignaturePtr WhichDocument="BCCIHEHIJFABF2"/>

            </dss:SignatureObject>
```

```
</dss:SignResponse>
```

Ejemplo 3. Firma sobre un documento alojado en un gestor documental.

La siguiente petición corresponde a una petición de firma servidor sobre un documento localizado en un gestor documental.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest Profile="urn:afirma:dss:1.0:profile:XSS" xmlns:cmism="http://docs.oasis-open.org/ns/cmis/messaging/200908/" xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

        <dss:InputDocuments>

                <dss:Other>

                        <cmism:getContentStream>


        <cmism:repositoryId>ALFRESCO_NODO_210</cmism:repositoryId>

                                <cmism:objectId>6a644199-4890-11df-aed4-cb0bb0fce2df</cmism:objectId>

                        </cmism:getContentStream>

                </dss:Other>

        </dss:InputDocuments>

        <dss:OptionalInputs>

                <dss:ClaimedIdentity>

                        <dss:Name>appPrueba</dss:Name>
```

```
                    </dss:ClaimedIdentity>

                    <dss:KeySelector>

                            <ds:KeyInfo>

                                    <ds:KeyName>firmante</ds:KeyName>

                            </ds:KeyInfo>

                    </dss:KeySelector>


            <dss:SignatureType>urn:afirma:dss:1.0:profile:XSS:forms:PDF</dss:SignatureType>

            </dss:OptionalInputs>

</dss:SignRequest>
```

En caso de producirse el proceso de firma satisfactoriamente el mensaje de respuesta será similar al seguidamente expuesto:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                   Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>


            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                    <dss:ResultMessage xml:lang="es">Proceso de generación de firma en servidor
realizado correctamente.</dss:ResultMessage>
```

```
            </dss:Result>
            <dss:OptionalOutputs>

            <dss:SignatureType>urn:afirma:dss:1.0:profile:XSS:forms:PDF</dss:SignatureType>
                        <xss:ArchiveInfo>
                                    <arch:ArchiveIdentifier>1271661821575105</arch:ArchiveIdentifier>
                        </xss:ArchiveInfo>
            </dss:OptionalOutputs>
            <dss:SignatureObject>
                        <dss:Base64Signature
Type="urn:afirma:dss:1.0:profile:XSS:forms:PDF"><![CDATA[JVBE.....]]></dss:Base64Signature>
            </dss:SignatureObject>
</dss:SignResponse>
```

Ejemplo 4. Firma en base a una política con resultado de tipo “Warning”

En la siguiente figura se muestra una petición de firma de servidor en formato XADES-A, se ha solicitado que se haga en base a una política de firma y se ignore un posible periodo de gracia.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest Profile="urn:afirma:dss:1.0:profile:XSS" xmlns:sigpol="urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#" xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema" xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema">
```

```
<dss:InputDocuments>
<dss:Document>
<dss:Base64XML><![CDATA[PD94bWw…]]></dss:Base64XML>
</dss:Document>
</dss:InputDocuments>
<dss:OptionalInputs>
<dss:ClaimedIdentity>
<dss:Name>tester</dss:Name>
</dss:ClaimedIdentity>
<dss:KeySelector>
<ds:KeyInfo>
<ds:KeyName>servidor</ds:KeyName>
</ds:KeyInfo>
</dss:KeySelector>
<afxp:ReferenceId>firmaServidorDSS</afxp:ReferenceId>
<dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>
<ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-A</ades:SignatureForm>

<afxp:HashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</afxp:HashAlgorithm>

<sigpol:GenerateUnderSignaturePolicy>.....
```

```
            <sigpol:SignaturePolicyIdentifier>http://www.map.es/documentacion/Politica_firma/Version1_0/</sigpol:SignaturePolicyIdentifier>

                    </sigpol:GenerateUnderSignaturePolicy>

                    <afxp:IgnoreGracePeriod/>

            </dss:OptionalInputs>

</dss:SignRequest>
```

Por ejemplo, si ante la petición anterior no tuviéramos conexión a una TSA (Autoridad de Sellado de Tiempo) se generaría un mensaje de respuesta como el siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                   Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>


            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Warning</dss:ResultMajor>


            <dss:ResultMinor>urn:afirma:dss:1.0:profile:XSS:resultminor:IncompleteUpgradeOperation</dss:ResultMinor>

                    <dss:ResultMessage xml:lang="es">No se ha podido realizar la firma en el formato [XADES-A]. El formato de la  firma es [XADES-BES] </dss:ResultMessage>
```

```
            </dss:Result>
            <dss:OptionalOutputs>
                        <dss:DocumentWithSignature>
                                    <dss:Document ID="BCFFEDJHEBEGG1">
                                                <dss:Base64XML><![CDATA[PD94b…]]></dss:Base64XML>
                                    </dss:Document>
                        </dss:DocumentWithSignature>
                        <dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>

            <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES</ades:Signat
ureForm>
                        <xss:ArchiveInfo>
                                    <arch:ArchiveIdentifier>1255433385383018</arch:ArchiveIdentifier>
                        </xss:ArchiveInfo>
            </dss:OptionalOutputs>
            <dss:SignatureObject>
                        <dss:SignaturePtr WhichDocument="BCFFEDJHEBEGG1"/>
            </dss:SignatureObject>
</dss:SignResponse>
```

Ejemplo 5. Firma sobre el hash de un documento

En la siguiente figura se muestra una petición de firma de servidor en formato XADES-BES a partir del hash calculado de un documento XML.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema" xmlns:cmism="http://docs.oasis-
open.org/ns/cmis/messaging/200908/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:sigpol="urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS" Profile="urn:afirma:dss:1.0:profile:XSS">

        <dss:InputDocuments>

                <dss:DocumentHash>

                        <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>


        <ds:DigestValue>SUj06ZPnC/tafBzIL19EDtmcq21V92InORdqHgv0p+A=</ds:DigestValue>

                </dss:DocumentHash>

        </dss:InputDocuments>

        <dss:OptionalInputs>

                <dss:ClaimedIdentity>

                        <dss:Name>appAfirma</dss:Name>

                </dss:ClaimedIdentity>

                <dss:KeySelector>

                        <ds:KeyInfo>
```

```
                                    <ds:KeyName>juan_lopez_vela</ds:KeyName>
                                </ds:KeyInfo>
                            </dss:KeySelector>
                            <dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>

        <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES</ades:SignatureForm>

        <afxp:HashAlgorithm>http://www.w3.org/2001/04/xmlenc#sha256</afxp:HashAlgorithm>
        </dss:OptionalInputs>
</dss:SignRequest>
```

En caso de producirse el proceso de firma satisfactoriamente el mensaje de respuesta será similar al seguidamente expuesto:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema# xsd/dss/oasis-dss-
profiles-AdES-schema-v1.0-os.xsd urn:oasis:names:tc:dss:1.0:core:schema http://docs.oasis-
open.org/dss/v1.0/oasis-dss-core-schema-v1.0-os.xsd urn:oasis:names:tc:dss:1.0:profiles:archive
xsd/dss/oasis-dss-1.0-profiles-archive-schema.xsd urn:oasis:names:tc:dss:1.0:profiles:XSS xsd/dss/oasis-
```

```
dss-1.0-profiles-XSS-schema-wd02.xsd">
        <dss:Result>
            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            <dss:ResultMessage xml:lang="es">Proceso de generación de firma en servidor realizado correctamente.</dss:ResultMessage>
        </dss:Result>
        <dss:OptionalOutputs>
            <dss:DocumentWithSignature>
                <dss:Document ID="BEFABIBIJFFBB7">
                    <dss:Base64XML>
                        <![CDATA[PD9...]]>
                    </dss:Base64XML>
                </dss:Document>
            </dss:DocumentWithSignature>
            <dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>

        <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES</ades:SignatureForm>
            <xss:ArchiveInfo>
                <arch:ArchiveIdentifier>145018068908887024</arch:ArchiveIdentifier>
            </xss:ArchiveInfo>
```

```
        </dss:OptionalOutputs>

        <dss:SignatureObject>

                <dss:SignaturePtr WhichDocument="BEFABIBIJFFBB7"/>

        </dss:SignatureObject>

</dss:SignResponse>
```

A.4.2 Ejemplos de Firma Delegada CoSign

En los siguientes ejemplos podemos ver una serie de peticiones y respuestas de firma de servidor en paralelo. Para que una petición de firma sea CoSign es necesario incluir el componente "xss:ParallelSignature".

Ejemplo 6. Firma CoSign sobre una firma registrada en @firma

La siguiente petición corresponde a una petición de firma CoSign sobre una firma registrada en la plataforma

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:InputDocuments>

                <dss:Other>
```

```
            <afxp:DocumentArchiveId>1228746420437004</afxp:DocumentArchiveId>
                    </dss:Other>
            </dss:InputDocuments>
            <dss:OptionalInputs>
                    <dss:ClaimedIdentity>
                            <dss:Name>tester</dss:Name>
                    </dss:ClaimedIdentity>
                    <dss:KeySelector>
                            <ds:KeyInfo>
                                    <ds:KeyName>servidor2</ds:KeyName>
                            </ds:KeyInfo>
                    </dss:KeySelector>
                    <afxp:ReferenceId>ref_cosign</afxp:ReferenceId>

            <afxp:HashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</afxp:HashAlgorithm
>
                    <xss:ParallelSignature/>
            </dss:OptionalInputs>
</dss:SignRequest>
```

El mesaje de salida sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:Result>


        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                <dss:ResultMessage xml:lang="es">Proceso de generación de firma coSign en
servidor realizado correctamente.</dss:ResultMessage>

        </dss:Result>

        <dss:OptionalOutputs>

                <dss:SignatureType>http://uri.etsi.org/01733/v1.7.3#</dss:SignatureType>

                <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-
T</ades:SignatureForm>

                <xss:ArchiveInfo>

                        <arch:ArchiveIdentifier>1228746420437015</arch:ArchiveIdentifier>

                </xss:ArchiveInfo>

        </dss:OptionalOutputs>

        <dss:SignatureObject>

                <dss:Base64Signature
Type="http://uri.etsi.org/01733/v1.7.3#"><![CDATA[MIIew....]]></dss:Base64Signature>
```

```
            </dss:SignatureObject>

</dss:SignResponse>
```

Ejemplo 7. Firma CoSign sobre una firma registrada en un gestor documental externo

El siguiente ejemplo muetra una petición de firma CoSign sobre una firma alojada en un gestor documental.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"          xmlns:cmism="http://docs.oasis-
open.org/ns/cmis/messaging/200908/">

            <dss:InputDocuments>

                        <dss:Other>

                                    <cmism:getContentStream>


            <cmism:repositoryId>ALFRESCO_NODO_210</cmism:repositoryId>

                                                <cmism:objectId>6a644199-4890-11df-aed4-
cb0bb0fce2df</cmism:objectId>

                                    </cmism:getContentStream>

                        </dss:Other>

                        <dss:Other>

                                    <dss:SignatureObject>
```

```
                                    <dss:Other>
                                        <cmism:getContentStream>
            <cmism:repositoryId>ALFRESCO_NODO_210</cmism:repositoryId>
                                            <cmism:objectId>e5695b3c-495c-11df-
aed4-cb0bb0fce2df</cmism:objectId>
                                        </cmism:getContentStream>
                                    </dss:Other>
                                </dss:SignatureObject>
                            </dss:Other>
                        </dss:InputDocuments>
                        <dss:OptionalInputs>
                            <xss:ParallelSignature/>
                            <dss:ClaimedIdentity>
                                <dss:Name>appPrueba</dss:Name>
                            </dss:ClaimedIdentity>
                            <dss:KeySelector>
                                <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                    <ds:KeyName>firmante_firma_5_5</ds:KeyName>
                                </ds:KeyInfo>
                            </dss:KeySelector>
```

```
        </dss:OptionalInputs>

</dss:SignRequest>
```

Si el proceso a finalizado satisfactoriamente la respuesta sería similar a la siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:Result>


        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                <dss:ResultMessage xml:lang="es">Proceso de generación de firma coSign en
servidor realizado correctamente.</dss:ResultMessage>

        </dss:Result>

        <dss:OptionalOutputs>

                <dss:DocumentWithSignature>

                        <dss:Document ID="BCHBGGBJDCGDE3">

                                <dss:Base64XML><![CDATA[PD94b....]]></dss:Base64XML>

                        </dss:Document>

                </dss:DocumentWithSignature>
```

```
                    <dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>

                    <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L-
1</ades:SignatureForm>

                    <xss:ArchiveInfo>

                            <arch:ArchiveIdentifier>1271661821575017</arch:ArchiveIdentifier>

                    </xss:ArchiveInfo>

            </dss:OptionalOutputs>

            <dss:SignatureObject>

                    <dss:SignaturePtr WhichDocument="BCHBGGBJDCGDE3"/>

            </dss:SignatureObject>

</dss:SignResponse>
```

Ejemplo 8. Firma CoSign sobre una firma enviada en la petición

La siguiente petición corresponde a una petición de firma CoSign sobre una firma enviada en la petición

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema" xmlns:cmism="http://docs.oasis-
open.org/ns/cmis/messaging/200908/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:sigpol="urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS" Profile="urn:afirma:dss:1.0:profile:XSS">
```

```
            <dss:InputDocuments>
                        <dss:Document>
                                    <dss:Base64XML>PHNl...</dss:Base64XML>
                        </dss:Document>
                        <dss:Document ID="2942.4909403902448">
                                    <dss:Base64XML>PD94bWwg...</dss:Base64XML>
                        </dss:Document>
                        <dss:Other>
                                    <dss:SignatureObject>
                                                <dss:SignaturePtr
WhichDocument="2942.4909403902448"/>
                                    </dss:SignatureObject>
                        </dss:Other>
            </dss:InputDocuments>
            <dss:OptionalInputs>
                        <dss:ClaimedIdentity>
                                    <dss:Name>appAfirma</dss:Name>
                        </dss:ClaimedIdentity>
                        <dss:KeySelector>
                                    <ds:KeyInfo>
```

```
                                    <ds:KeyName>juan_lopez_vela</ds:KeyName>

                                </ds:KeyInfo>

                            </dss:KeySelector>


                <afxp:HashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</afxp:HashAlgorithm
>

                            <xss:ParallelSignature/>

                </dss:OptionalInputs>

</dss:SignRequest>
```

El mesaje de salida sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"    xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"    xsi:schemaLocation="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#    xsd/dss/oasis-dss-
profiles-AdES-schema-v1.0-os.xsd    urn:oasis:names:tc:dss:1.0:core:schema    http://docs.oasis-
open.org/dss/v1.0/oasis-dss-core-schema-v1.0-os.xsd    urn:oasis:names:tc:dss:1.0:profiles:archive
xsd/dss/oasis-dss-1.0-profiles-archive-schema.xsd    urn:oasis:names:tc:dss:1.0:profiles:XSS    xsd/dss/oasis-
dss-1.0-profiles-XSS-schema-wd02.xsd">

                <dss:Result>

                            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                            <dss:ResultMessage    xml:lang="es">Proceso    de    generación    de    firma    coSign    en
```

```
servidor realizado correctamente.</dss:ResultMessage>
            </dss:Result>
            <dss:OptionalOutputs>
                  <dss:DocumentWithSignature>
                        <dss:Document ID="BEFABIDEJJEIF9">
                              <dss:Base64XML><![CDATA[PD94bW..]]></dss:Base64XML>
                        </dss:Document>
                  </dss:DocumentWithSignature>
                  <dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>

            <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES</ades:SignatureFor
m>
                  <xss:ArchiveInfo>
                        <arch:ArchiveIdentifier>145018068908887028</arch:ArchiveIdentifier>
                  </xss:ArchiveInfo>
            </dss:OptionalOutputs>
            <dss:SignatureObject>
                  <dss:SignaturePtr WhichDocument="BEFABIDEJJEIF9"/>
            </dss:SignatureObject>
</dss:SignResponse>
```

A.4.3 Ejemplos de Firma Delegada CounterSign

Los siguientes XML corresponden a peticiones y respuestas de firma de servidor CounterSign, en estos casos es necesario incluir en la petición el componente “xss:CounterSignature” para indicar que la petición es counterSign.

Ejemplo 9. Firma CounterSign sobre una firma registrada en @firma

El siguiente XML muetra una petición de firma CounterSign en el que la firma origin se encuentra registrada en @firma

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:InputDocuments>

                <dss:Other>

                        <afxp:DocumentArchiveId                    ID="CounterSignature-
1228770422390">1228769383421004</afxp:DocumentArchiveId>

                </dss:Other>

        </dss:InputDocuments>

        <dss:OptionalInputs>

                <dss:ClaimedIdentity>

                        <dss:Name>tester</dss:Name>
```

```
                    </dss:ClaimedIdentity>

                    <dss:KeySelector>

                        <ds:KeyInfo>

                            <ds:KeyName>servidor2</ds:KeyName>

                        </ds:KeyInfo>

                    </dss:KeySelector>

                    <afxp:ReferenceId>ref_countersign</afxp:ReferenceId>

                    <afxp:HashAlgorithm>http://www.w3.org/2001/04/xmldsig-
more#sha384</afxp:HashAlgorithm>

                    <xss:CounterSignature WhichDocument="CounterSignature-1228770422390"/>

                    <afxp:TargetSigner><![CDATA[MIID...]]></afxp:TargetSigner>

            </dss:OptionalInputs>

</dss:SignRequest>
```

El mesaje de salida sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                   Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>
```

```
        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            <dss:ResultMessage xml:lang="es">Proceso de generación de firma counterSign en servidor realizado correctamente.</dss:ResultMessage>
        </dss:Result>
        <dss:OptionalOutputs>
            <dss:UpdatedSignature>
                <dss:SignatureObject>
                    <dss:Base64Signature Type="urn:afirma:dss:1.0:profile:XSS:forms:CMSWithTST"><![CDATA[MIIS…]]></dss:Base64Signature>
                </dss:SignatureObject>
            </dss:UpdatedSignature>

        <dss:SignatureType>urn:afirma:dss:1.0:profile:XSS:forms:CMSWithTST</dss:SignatureType>
            <xss:ArchiveInfo>
                <arch:ArchiveIdentifier>1228769383421009</arch:ArchiveIdentifier>
            </xss:ArchiveInfo>
        </dss:OptionalOutputs>
</dss:SignResponse>
```

Ejemplo 10. Firma CounterSign sobre una firma registrada en un gestor documental

El siguiente XML corresponde a una petición de firma CounterSign de una firma alojada en un gestor documental externo.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

        <dss:InputDocuments xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

                <dss:Other xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

                        <dss:SignatureObject
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

                                <dss:Other
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

                                        <cmism:getContentStream
xmlns:cmism="http://docs.oasis-open.org/ns/cmis/messaging/200908/">


        <cmism:repositoryId>ALFRESCO_NODO_210</cmism:repositoryId>

                                                <cmism:objectId>5cf7d9fd-495c-11df-aed4-
cb0bb0fce2df</cmism:objectId>

                                        </cmism:getContentStream>

                                </dss:Other>

                        </dss:SignatureObject>

                </dss:Other>

        </dss:InputDocuments>

        <dss:OptionalInputs xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">
```

```
                    <xss:CounterSignature    WhichDocument="CounterSignature-1271752801076"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"/>

                    <dss:ClaimedIdentity xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

                        <dss:Name
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">appPrueba</dss:Name>

                    </dss:ClaimedIdentity>

                    <dss:KeySelector xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

                            <ds:KeyName>firmante_firma_5_5</ds:KeyName>

                        </ds:KeyInfo>

                    </dss:KeySelector>

            </dss:OptionalInputs>

</dss:SignRequest>
```

El mensaje de respuesta sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                                Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>
```

```
<dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
<dss:ResultMessage xml:lang="es">Proceso de generación de firma counterSign en servidor realizado correctamente.</dss:ResultMessage>
</dss:Result>
<dss:OptionalOutputs>
<dss:DocumentWithSignature>
<dss:Document ID="BCHBHFCIAAEDE7">
<dss:Base64XML><![CDATA[PD94...]]></dss:Base64XML>
</dss:Document>
</dss:DocumentWithSignature>
<dss:UpdatedSignature>
<dss:SignatureObject>
<dss:SignaturePtr WhichDocument="BCHBHFCIAAEDE7"/>
</dss:SignatureObject>
</dss:UpdatedSignature>
<dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>
<ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-1</ades:SignatureForm>
<xss:ArchiveInfo>
<arch:ArchiveIdentifier>1271752446816038</arch:ArchiveIdentifier>
```

```
                </xss:ArchiveInfo>

        </dss:OptionalOutputs>

</dss:SignResponse>
```

Ejemplo 11. Firma CounterSign sobre una firma enviada en la petición

La siguiente petición corresponde a una petición de firma CoSign sobre una firma enviada en la petición

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema" xmlns:cmism="http://docs.oasis-
open.org/ns/cmis/messaging/200908/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:sigpol="urn:oasis:names:tc:dss-x:1.0:profiles:SignaturePolicy:schema#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS" Profile="urn:afirma:dss:1.0:profile:XSS">

        <dss:InputDocuments>

                <dss:Document ID="1095.673480506959">

                        <dss:Base64XML>PD94b...</dss:Base64XML>

                </dss:Document>

                <dss:Other>

                        <dss:SignatureObject>

                                <dss:SignaturePtr WhichDocument="1095.673480506959"/>

                        </dss:SignatureObject>
```

```
                </dss:Other>
        </dss:InputDocuments>
        <dss:OptionalInputs>
                <dss:ClaimedIdentity>
                        <dss:Name>appAfirma</dss:Name>
                </dss:ClaimedIdentity>
                <dss:KeySelector>
                        <ds:KeyInfo>
                                <ds:KeyName>juan_lopez_vela</ds:KeyName>
                        </ds:KeyInfo>
                </dss:KeySelector>

        <afxp:HashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</afxp:HashAlgorithm
>
                <xss:CounterSignature/>
        </dss:OptionalInputs>
</dss:SignRequest>
```

El mesaje de salida sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:SignResponse                                        Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
```

```
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema# xsd/dss/oasis-dss-profiles-AdES-schema-v1.0-os.xsd urn:oasis:names:tc:dss:1.0:core:schema http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-schema-v1.0-os.xsd urn:oasis:names:tc:dss:1.0:profiles:archive xsd/dss/oasis-dss-1.0-profiles-archive-schema.xsd urn:oasis:names:tc:dss:1.0:profiles:XSS xsd/dss/oasis-dss-1.0-profiles-XSS-schema-wd02.xsd">

        <dss:Result>

            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

            <dss:ResultMessage xml:lang="es">Proceso de generación de firma counterSign en servidor realizado correctamente.</dss:ResultMessage>

        </dss:Result>

        <dss:OptionalOutputs>

            <dss:DocumentWithSignature>

                <dss:Document ID="BEFABIDJDEHFG11">

                    <dss:Base64XML><![CDATA[PD94b...]]></dss:Base64XML>

                </dss:Document>

            </dss:DocumentWithSignature>

            <dss:UpdatedSignature>

                <dss:SignatureObject>

                    <dss:SignaturePtr WhichDocument="BEFABIDJDEHFG11"/>

                </dss:SignatureObject>
```

```
                    </dss:UpdatedSignature>

                    <dss:SignatureType>http://uri.etsi.org/01903/v1.3.2#</dss:SignatureType>


            <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:BES</ades:SignatureFor
m>

                    <xss:ArchiveInfo>

                            <arch:ArchiveIdentifier>145018068908887033</arch:ArchiveIdentifier>

                    </xss:ArchiveInfo>

            </dss:OptionalOutputs>

</dss:SignResponse>
```

A.4.4 Ejemplos de Validar Firma

Ejemplo 12. Validación de una firma incluida en la petición

En la siguiente figura se representa un mensaje de petición de validar firma, donde la firma a verificar es una firma XAdES enveloping. En el ejemplo se solicita además de toda la información contenida en la firma el resultado del mapeo del certificado

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyRequest                                  Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:OptionalInputs>

                    <dss:ClaimedIdentity>
```

```
                    <dss:Name>tester</dss:Name>

                </dss:ClaimedIdentity>

                <afxp:ReturnReadableCertificateInfo
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"/>

                <afxp:AdditionalReportOption                                xmlns:afxp="
urn:afirma:dss:1.0:profile:XSS:schema ">

                    <afxp:IncludeProperties>

                        <afxp:IncludeProperty
Type="urn:afirma:dss:1.0:profile:XSS:SignatureProperty:SignatureTimeStamp"/>

                    </afxp:IncludeProperties>

                </afxp:AdditionalReportOption>

                <vr:ReturnVerificationReport
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#">

                    <vr:ReportOptions>


        <vr:IncludeCertificateValues>true</vr:IncludeCertificateValues>


        <vr:ReportDetailLevel>urn:oasis:names:tc:dss:1.0:reportdetail:allDetails</vr:ReportDeta
ilLevel>

                    </vr:ReportOptions>

                </vr:ReturnVerificationReport>

        </dss:OptionalInputs>

        <dss:SignatureObject>
```

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Id="Signature-BCCIHHBBHIIBC2">

<ds:SignedInfo Id="SignedInfo-BCCIHHBBHIIBC2">

<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

<ds:Reference Id="SignedProperties-Reference-
BCCIHHBBHIIBC2" Type="http://uri.etsi.org/01903#SignedProperties" URI="#SignedProperties-
BCCIHHBBHIIBC2">

<ds:Transforms>

<ds:Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

</ds:Transforms>

<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>


<ds:DigestValue>XwNoACjR0HDFvQc3eayNLx+/Nkc=</ds:DigestValue>

</ds:Reference>

<ds:Reference Id="SignedDataObject-Reference-
BCCIHHBBHIIBC2" URI="#SignedDataObject-BCCIHHBBHIIBC2">

<ds:Transforms>

<ds:Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
```

```
                                    </ds:Transforms>

                                    <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

            <ds:DigestValue>NPFO9RXeP63F4CYxl35bzs+YD7k=</ds:DigestValue>

                                </ds:Reference>

                                <ds:Reference URI="#keyInfo-BCCIHHBBHIIBC2">

                                    <ds:Transforms>

                                        <ds:Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>

                                    </ds:Transforms>

                                    <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

            <ds:DigestValue>6JGkjD9s7joEShGETdfppykmcyY=</ds:DigestValue>

                                </ds:Reference>

                            </ds:SignedInfo>

                            <ds:SignatureValue                          Id="SignatureValue-
BCCIHHBBHIIBC2">Dmz79MbFkUuTEHjhXAupyPZq2Bw/v5lI85Ye/e46TqRziFPRZm9LiUuzLngDpOYVV
DOfwwE1aB1irYUFcS5IDNqm+ZuF5AYCkI9BBErRtVKxu/SGMJmgVStxDmFjWdkmG3bxChhFYlX1xh7e
K2d81FQXOYW5LIZBVctCPaGYejo=</ds:SignatureValue>

                            <ds:KeyInfo                          Id="keyInfo-BCCIHHBBHIIBC2"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

                                <ds:KeyValue>
```

```
<ds:RSAKeyValue>

<ds:Modulus>4SNeWUCLebrwiGBo+nKZV8lkDEGrzUbn1CCx8IVGBpRc88S9PBoxzxqgEM
D6ZXnwkTyf81fR5nWF/tJ3OVfIMS7OcbXKRQ/zJPz8e0oYFgpd8EvSBgmwaK6wSz7tWPZgqYEIiHz0hv6
fFUXgheFQpyWoVT5nnmerQF6bTqepJ70=</ds:Modulus>

<ds:Exponent>AQAB</ds:Exponent>

</ds:RSAKeyValue>

</ds:KeyValue>

<ds:X509Data>

<ds:X509Certificate>MIIDfDCCAuWgAwIBAgIBBTANBgkqhkiG9w0BAQsFADCBzTELMAkG
A1UEBhMCRVMxEDAOBgNVBAgTB1NFVklMTEExEDAOBgNVBAcTB1NFVklMTEExIjAgBgNVBAoTGVR
FTFZFTlQgSU5URVJBQ1RJVkEuIFMuQS4xMjAwBgNVBAsTKURFUEFSVEFNRU5UTyBERSBBRE1JTklTVF
JBQ0lPTkVTIFBVQkxJQ0FTMR0wGwYDVQQDFBRDQSBERVNBUlJPTExPIEBGSVJNQTEjMCEGCSqGSIb3
DQEJARYUamEucm9tYW5AdGVsdmVudC5jb20wHhcNMDgxMDMwMDczOTQ0WhcNMDkwODI2M
DczOTQ0WjCBozELMAkGA1UEBhMCRVMxEDAOBgNVBAgTB1NFVklMTEExEDAOBgNVBAcTB1NFVkl
MTEExHDAaBgNVBAoTE1RFTFZFTlQgSU5URVJBQ1RJVkExDzANBgNVBAsWBkBGSVJNQTEcMBoGA1
UEAxMTU0VSVklET1IgREVTQVJST0xMTzEjMCEGCSqGSIb3DQEJARYUamEucm9tYW5AdGVsdmVudC
5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOEjXllAi3m68IhgaPpymVfJZAxBq81G59Qgsf
CFRgaUXPPEvTwaMc8aoBDA+mV58JE8n/NX0eZ1hf7SdzlXyDEuznG1ykUP8yT8/HtKGBYKXfBL0gYJsGi
usEs+7Vj2YKmBCIh89Ib+nxVF4IXhUKclqFU+Z55nq0Bem06nqSe9AgMBAAGjgZMwgZAwDAYDVR0TA
QH/BAIwADAdBgNVHQ4EFgQUPNaziL0lD1vsX3aKkKzFcB9D7aowCwYDVR0PBAQDAgEGMDQGCWC
GSAGG+EIBCAQnFiVodHRwOlxcdGVsdmVudC5kZXNhcnJvbGxvLmNvbXBvbmVudGVzMB4GCWCGSA
GG+EIBDQQRFg94Y2EgY2VydGlmaWNhdGUwDQYJKoZIhvcNAQELBQADgYEAX6xji6Fn2luHuLTDo4fH
WYFYXkdQ0/mLuGYy9uLC9hEHqptrRjkoQbZm31fXfETPukUnX5WKnjLNEEOV6/Bm3oU6B60Ea75/JTc
eFVu1F5akguPZMfsj8wNZ5P5mSj9xPcKcITl6j3wJe+DqcUOLKO7rPU1TE59JEtlJTxHSGqw=</ds:X509C
ertificate>

<ds:X509IssuerSerial>
```

<ds:X509IssuerName>EMAIL=dss@telvent.com,CN=CA DESARROLLO @FIRMA,OU=DEPARTAMENTO DE ADMINISTRACIONES PUBLICAS,O=TELVENT INTERACTIVA. S.A.,L=SEVILLA,ST=SEVILLA,C=ES</ds:X509IssuerName>

<ds:X509SerialNumber>5</ds:X509SerialNumber>

</ds:X509IssuerSerial>

</ds:X509Data>

</ds:KeyInfo>

<ds:Object>

<xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#Signature-BCCIHHBBHIIBC2">

<xades:SignedProperties Id="SignedProperties-BCCIHHBBHIIBC2">

<xades:SignedSignatureProperties>

..... <xades:SigningTime>2008-12-08T22:19:38+01:00</xades:SigningTime>

..... <xades:SigningCertificate>

.....

<xades:Cert>

.....

<xades:CertDigest>

.....

<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

```
                                                                    .....
                    <ds:DigestValue>NVv4+1B+U7mymhHuyajmE3KVmso=</ds:DigestValue>

                                                                    .....
            </xades:CertDigest>

                                                                    .....
            <xades:IssuerSerial>

                                                                    .....
                    <ds:X509IssuerName>EMAIL=dss@telvent.com,CN=CA DESARROLLO
@FIRMA,OU=DEPARTAMENTO DE ADMINISTRACIONES PUBLICAS,O=TELVENT INTERACTIVA.
S.A.,L=SEVILLA,ST=SEVILLA,C=ES</ds:X509IssuerName>

                                                                    .....
                    <ds:X509SerialNumber>5</ds:X509SerialNumber>

                                                                    .....
            </xades:IssuerSerial>

                                                                    .....
            </xades:Cert>

                                                                .....</xades:SigningCertificate>

                                                            </xades:SignedSignatureProperties>

                                                    </xades:SignedProperties>

                                                    <UnsignedProperties
xmlns="http://uri.etsi.org/01903/v1.3.2#">

                                                            <UnsignedSignatureProperties
xmlns="http://uri.etsi.org/01903/v1.3.2#">

                                                            ..... <SignatureTimeStamp
Id="SignatureTimeStamp" xmlns="http://uri.etsi.org/01903/v1.3.2#">
```

.....

<CanonicalizationMethod xmlns="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

.....

<EncapsulatedTimeStamp Encoding="http://uri.etsi.org/01903/v1.2.2#DER" xmlns="http://uri.etsi.org/01903/v1.3.2#">MIIH4gYJKoZIhvcNAQcCoIIH0zCCB88CAQMxCzAJBgUrDgMCGgUAMGkGCyqGSIb3DQEJEAEEoFoEWDBWAgEBBgkrBoENolwKAgEwITAJBgUrDgMCGgUABBTovFmy92T1yFRNKTGeakY2TYvciAIHBF2PKpwUVxgPMjAwODEyMDgyMTE5MzhaMAkCAQqAAQGBAQGgggRtMIIEaTCCA9KgAwIBAgIBBzANBgkqhkiG9w0BAQUFADCBzTELMAkGA1UEBhMCRVMxEDAOBgNVBAgTB1NFVklMTEExEDAOBgNVBAcTB1NFVklMTEExIjAgBgNVBAoTGVRFTFZFTlQgSU5URVJBQ1RJVkEuIFMuQS4xMjAwBgNVBAsTKURFUEFSVEFNRU5UTyBERSBBRE1JTklTVFJBQ0lPTkVTIFBVQkxJQ0FTMR0wGwYDVQQDFBRDQSBERVNBUlJPTExPIEBGSVJNQTEjMCEGCSqGSIb3DQEJARYUamEucm9tYW5AdGVsdmVudC5jb20wHhcNMDgxMDMwMDc0MjA5WhcNMDkwODI2MDc0MjA5WjCBnjELMAkGA1UEBhMCRVMxEDAOBgNVBAgTB1NFVklMTEExEDAOBgNVBAcTB1NFVklMTEExHDAaBgNVBAoTE1RFTFZFTlQgSU5URVJBQ1RJVkExDzANBgNVBAsWBkBGSVJNQTEXMBUGA1UEAxMOVFNBIERFU0FSUk9MTE8xIzAhBgkqhkiG9w0BCQEWFGphLnJvbWFuQHRlbHZlbnQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKOAxab+GntD32ZS/ShtCskTIox9Sk4Idg9nVFHNIR3QMIRfgJ5w8UNUGmmhxWho3Iq8zFpuISrad/kVEUGQDork2np6vQKpb3k5VAiEBoeeMAT0AU9Qls74YTkwynQgLRoNYM4R97LA2zOUypJwYbCB8kJKs17JlW3OxhDD51zQIDAQABo4IBhDCCAYAwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQUAUB4vcgfavtOPF7TFZztYk8xL1cwgfoGA1UdIwSB8jCB74AUOlMeQGl0pg0dQenIve7/H+fs2cWhgdOkgdAwgc0xCzAJBgNVBAYTAkVTMRAwDgYDVQQIEwdTRVZJTExBMRAwDgYDVQQHEwdTRVZJTExBMSIwIAYDVQQKExlURUxWRU5UIElOVEVSQUNUSVZBLiBTLkEuMTIwMAYDVQQLEylERVBBUlRBTUVOVE8gREUgQURNSU5JU1RSQUNJT05FUyBQVUJMSUNBUzEdMBsGA1UEAxQUQ0EgREVTQVJST0xMTyBARklSTUExIzAhBgkqhkiG9w0BCQEWFGphLnJvbWFuQHRlbHZlbnQuY29tggEBMDQGCWCGSAGG+EIBCAQnFiVodHRwOlxcdGVsdmVudC5kZXNhcnJvbGxvLmNvbXBvbmVudGVzMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2VydGlmaWNhdGUwDQYJKoZIhvcNAQEFBQADgYEALEBiOlAK6I1oTQMXbyBWKQF2AedI8m8kRpUwEFTFbUUCci0D1lZ6BlxV3VT7+j8s2f2BmHpsFa/fhI4qPSjpYoeis050w2i59eZ/wXAdyKlhWnpMdK/wp2JmhxwLx/DTW2j9kHDHRax/IzmM9UvxlG7nvqULPp4N5fZmkD6miiwxggLfMIIC2wIBATCB0zCBzTELMAkGA1UEBhMCRVMxEDAOBgNVBAgTB1NFVklMTEExEDAOBgNVBAcTB1NFVklMTEExIjAgBgNVBAoTGVRFTFZFTlQgSU5URVJBQ1RJVkEuIFMuQS4xMjAwBgNVBAsTKURFUEFSVEFNRU5UTyBERSBBRE1JTklTVFJBQ0lPTkVTIFBVQkxJQ0FTMR0wGwYDVQQDFBRDQSBERVNBUlJPTExPIEBGSVJNQTEjMCEGCSqGSIb3DQEJARYUamEucm9tYW5AdGVsdmVudC5jb20CAQcwCQYFKw4DAhoFAKCCAW

EwGgYJKoZIhvcNAQkDMQ0GCyqGSIb3DQEJEAEEMCMGCSqGSIb3DQEJBDEWBBQaQkFlXVT7h5Iqu4
pB93U+GEOW/zCCARwGCyqGSIb3DQEJEAIMMYIBCzCCAQcwgfUwgfIEFKQ2zjJuqdE4LPs+MDeVnEH
NIRrjMIHZMIHTpIHQMIHNMQswCQYDVQQGEwJFUzEQMA4GA1UECBMHU0VWSUxMQTEQMA4GA
1UEBxMHU0VWSUxMQTEiMCAGA1UEChMZVEVMVkVOVCBJTlRFUkFDVElWQS4gUy5BLjEyMDAGA1
UECxMpREVQQVJUQU1FTlRPIERFIEFETUlOSVNUUkFDSU9ORVMgUFVCTElDQVMxHTAbBgNVBAMU
FENBIERFU0FSUk9MTE8gQEZJUk1BMSMwIQYJKoZIhvcNAQkBFhRqYS5yb21hbkB0ZWx2ZW50LmNv
bQIBBzANMAsGCSsGgQ2iXAoCATANBgkqhkiG9w0BAQEFAASBgLTwbgrZxhGFJxBFkZbHX96FKcmeIt
Wrpw88iy3OpXJidg1MvIIZzFZEaNLWsGVARv32QqmrV0uc2TwfL2whnezqf4I87yDwvUzf3XzBsKiTG39
wJe5qWi11DBHMm7G6X9BJGdLydrTv1OGrHiAV7vIi5VS6j03IrY9juxai+QoW

.....

</SignatureTimeStamp>

</UnsignedSignatureProperties>

</UnsignedProperties>

</xades:QualifyingProperties>

</ds:Object>

<ds:Object Id="SignedDataObject-BCCIHHBBHIIBC2">

IyBSdXRhIGNvbXBsZXRhIChvIHJlbGF0aXZhIHJlc3BlY3RvIGEgbGEgbG9jYWxpemFjafNuIGRl

bCBmaWNoZXJvIC5iYXQgZGUgZWplY3VjafNuKSBhbCBkaXJlY3RvcmlvIHRlbXBvcmFsIGRlbCBD

bGllbnRlIFdTDQpkaXIudGVtcG9yYWwucGF0aD0uLi8uLi90ZW1wLw0KDQojIEFsbWFjZW5hciBw

ZXRpY2lvbg0KYWxtYWNlbmFyLnBldGljaW9uID0gZmFsc2UNCg0KIyBBbG1hY2VuYXIgcmVzcHVl

c3RhDQphbG1hY2VuYXIucmVzcHVlc3RhID0gZmFsc2UNCg0KIyBQYXRy824gdXRpbGl6YWRvIHBh

cmEgZXNjcmliaXIgbGEgZmVjaGEgZW4gbG9zIG5vbWJyZXMgZGUgbG9zIGZpY2hlcm9zDQojIF1

ZSBhbG1hY2VuYW4gbGEgcGV0aWNp824gbyByZXNwdWVzdGEgcmVhbGl6YWRhcy4NCmZvcm1hdG

8u

```
ZmVjaGEgPSB5eXl5LU1NLWRkX0hILW1tLXNzLVNTU18NCg0K</ds:Object>

                    </ds:Signature>

            </dss:SignatureObject>

</dss:VerifyRequest>
```

El mesaje resultante es:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyResponse                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"   xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

            <dss:Result>


            <dss:ResultMajor>urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature</dss:ResultMaj
or>

                    <dss:ResultMessage xml:lang="es">La firma es valida</dss:ResultMessage>

            </dss:Result>

            <dss:OptionalOutputs>

                    <vr:VerificationReport>

                            <vr:IndividualSignatureReport>

                                    <vr:SignatureIdentifier>
```

```
                                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

        <ds:DigestValue><![CDATA[Xg/fkQ1qvUlptIZK0OboNB2cjeE=]]></ds:DigestValue>
                                        </vr:SignatureIdentifier>
                                        <dss:Result>

        <dss:ResultMajor>urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature</dss:ResultMaj
or>
                                        <dss:ResultMessage xml:lang="es">La firma es
valida</dss:ResultMessage>
                                        </dss:Result>
                                        <vr:Details>
                                                <afxp:ReadableCertificateInfo>
                                                        <afxp:ReadableField>

        <afxp:FieldIdentity>idPolitica</afxp:FieldIdentity>
                                                        <afxp:FieldValue>PRUEBA</afxp:FieldValue>
                                                        </afxp:ReadableField>
                                                        <afxp:ReadableField>

        <afxp:FieldIdentity>NombreYApellidos</afxp:FieldIdentity>
                                                <afxp:FieldValue>SERVIDOR
```

```
DESARROLLO</afxp:FieldValue>
                                                    </afxp:ReadableField>
                                                    <afxp:ReadableField>
                                                    <afxp:FieldIdentity>tipo</afxp:FieldIdentity>
                                                    <afxp:FieldValue>Certificado de
persona</afxp:FieldValue>
                                                    </afxp:ReadableField>
                                                    <afxp:ReadableField>

            <afxp:FieldIdentity>versionPolitica</afxp:FieldIdentity>
                                                     <afxp:FieldValue>4</afxp:FieldValue>
                                                    </afxp:ReadableField>
                                                </afxp:ReadableCertificateInfo>
                                                <vr:DetailedReport>
                                                    <vr:FormatOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:SignatureFormat">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:SignatureFormat:code:ValidFormat</dss:Co
de>
                                                    </vr:FormatOK>
                                                    <vr:Properties>
                                                     .....<vr:UnsignedProperties>
```

```
                                                                    .....
            <vr:UnsignedSignatureProperties>

                                                                    .....
            <vr:SignatureTimeStamp>

                                                                    .....
                  <vr:FormatOK Type="urn:afirma:dss:1.0:profile:XSS:detail:SignatureFormat">

                                                                    .....

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:SignatureFormat:code:ValidFormat</dss:Co
de>

                                                                    .....
                  </vr:FormatOK>

                                                                    .....
                  <vr:TimeStampContent>

                                                                    .....
                        <vr:SerialNumber>1228769383421015</vr:SerialNumber>

                                                                    .....
                        <vr:CreationTime>2008-12-08T21:19:38.000Z</vr:CreationTime>

                                                                    .....
                  </vr:TimeStampContent>

                                                                    .....
                  <vr:MessageHashAlg
Type="urn:afirma:dss:1.0:profile:XSS:detail:MessageHashAlg">

                                                                    .....
                        <dss:Code>http://www.w3.org/2000/09/xmldsig#sha1</dss:Code>

                                                                    .....
```

```
                    </vr:MessageHashAlg>

                                                                    .....

                    <vr:SignatureOK>

                                                                    .....

                            <vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:SignatureCore">

                                                                    .....

          <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:SignatureCore:code:ValidSignature</dss:Co
de>

                                                                    .....

                            </vr:SigMathOK>

                                                                    .....

                    </vr:SignatureOK>

                                                                    .....

                    <vr:CertificatePathValidity>

                                                                    .....

                            <vr:PathValiditySummary
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

                                                                    .....

          <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:Valid</dss:Code>

                                                                    .....

                            </vr:PathValiditySummary>

                                                                    .....

                            <vr:CertificateIdentifier>
```

```
                                                                    .....
                                        <ds:X509IssuerName>EMAIL=dss@telvent.com,CN=CA
DESARROLLO @FIRMA,OU=DEPARTAMENTO DE ADMINISTRACIONES PUBLICAS,O=TELVENT
INTERACTIVA. S.A.,L=SEVILLA,ST=SEVILLA,C=ES</ds:X509IssuerName>

                                                                    .....
                                        <ds:X509SerialNumber>7</ds:X509SerialNumber>

                                                                    .....
                                    </vr:CertificateIdentifier>

                                                                    .....
                                    <vr:PathValidityDetail>

                                                                    .....
                                        <vr:CertificateValidity>

                                                                    .....
                                            <vr:CertificateIdentifier>

                                                                    .....

                    <ds:X509IssuerName>EMAIL=dss@telvent.com,CN=CA DESARROLLO
@FIRMA,OU=DEPARTAMENTO DE ADMINISTRACIONES PUBLICAS,O=TELVENT INTERACTIVA.
S.A.,L=SEVILLA,ST=SEVILLA,C=ES</ds:X509IssuerName>

                                                                    .....

                    <ds:X509SerialNumber>7</ds:X509SerialNumber>

                                                                    .....
                                            </vr:CertificateIdentifier>

                                                                    .....
                                            <vr:Subject>EMAIL=dss@telvent.com,CN=TSA
DESARROLLO,OU=@FIRMA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=SEVILLA,C=ES</vr:Subject>
```

```
                                                    .....

            <vr:CertificateValue><![CDATA[MIIEa....]]></vr:CertificateValue>

                                                    .....
                                                <vr:SignatureOK>

                                                    .....
                                                    <vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

                                                    .....

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidSignature</dss:Code>

                                                    .....
                                                    </vr:SigMathOK>

                                                    .....
                                                </vr:SignatureOK>

                                                    .....
                                                <vr:ExtensionsOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

                                                    .....

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidExtension</dss:Code>

                                                    .....
                                                </vr:ExtensionsOK>

                                                    .....
                                                <vr:ValidityPeriodOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

                                                    .....
```

```
            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidPeriod</dss:Code>

                                                                    .....
                                                            </vr:ValidityPeriodOK>

                                                                    .....
                                                    </vr:CertificateValidity>

                                                                    .....
                                                    <vr:TrustOrigin
Type="urn:oasis:names:tc:dss:1.0:trustorigin:certDataBase"/>

                                                                    .....
                                            </vr:PathValidityDetail>

                                                                    .....
                                    </vr:CertificatePathValidity>

                                                                    .....
            </vr:SignatureTimeStamp>

                                                                    .....
            </vr:UnsignedSignatureProperties>

                                                                    ..... </vr:UnsignedProperties>

                                                                  </vr:Properties>

                                                                  <vr:SignatureOK>

                                                                  .....<vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:SignatureCore">

                                                                    .....
            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:SignatureCore:code:ValidSignature</dss:Co
de>
```

```
                                                    ..... </vr:SigMathOK>
                                                </vr:SignatureOK>
                                                <vr:CertificatePathValidity>
                                                .....<vr:PathValiditySummary
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">
                                                .....
            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:Valid</dss:Code>
                                                ..... </vr:PathValiditySummary>
                                                ..... <vr:CertificateIdentifier>
                                                .....
            <ds:X509IssuerName>EMAIL=dss@telvent.com,CN=CA DESARROLLO
@FIRMA,OU=DEPARTAMENTO DE ADMINISTRACIONES PUBLICAS,O=TELVENT INTERACTIVA.
S.A.,L=SEVILLA,ST=SEVILLA,C=ES</ds:X509IssuerName>
                                                .....
            <ds:X509SerialNumber>5</ds:X509SerialNumber>
                                                .....</vr:CertificateIdentifier>
                                                .....<vr:PathValidityDetail>
                                                .....
            <vr:CertificateValidity>
                                                .....
            <vr:CertificateIdentifier>
                                                .....
                <ds:X509IssuerName>EMAIL=dss@telvent.com,CN=CA DESARROLLO
@FIRMA,OU=DEPARTAMENTO DE ADMINISTRACIONES PUBLICAS,O=TELVENT INTERACTIVA.
```

```
S.A.,L=SEVILLA,ST=SEVILLA,C=ES</ds:X509IssuerName>

                                                                    .....
                    <ds:X509SerialNumber>5</ds:X509SerialNumber>

                                                                    .....
            </vr:CertificateIdentifier>

                                                                    .....
            <vr:Subject>EMAIL=dss@telvent.com,CN=SERVIDOR
DESARROLLO,OU=@FIRMA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=SEVILLA,C=ES</vr:Subject>

                                                                    .....
            <vr:CertificateValue><![CDATA[MIID....]]></vr:CertificateValue>

                                                                    .....
            <vr:SignatureOK>

                                                                    .....
                    <vr:SigMathOK Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

                                                                    .....

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidSignature</dss:Code>

                                                                    .....
                    </vr:SigMathOK>

                                                                    .....
            </vr:SignatureOK>

                                                                    .....
            <vr:ExtensionsOK Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

                                                                    .....

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidExtension</dss:Code>
```

```
                                                                    .....
            </vr:ExtensionsOK>

                                                                    .....
            <vr:ValidityPeriodOK Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

                                                                    .....

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidPeriod</dss:Code>

                                                                    .....
            </vr:ValidityPeriodOK>

                                                                    .....
            </vr:CertificateValidity>

                                                                    .....
            <vr:TrustOrigin Type="urn:oasis:names:tc:dss:1.0:trustorigin:certDataBase"/>

                                                                ..... </vr:PathValidityDetail>

                                                            </vr:CertificatePathValidity>

                                                    </vr:DetailedReport>

                                            </vr:Details>

                                    </vr:IndividualSignatureReport>

                            </vr:VerificationReport>

            </dss:OptionalOutputs>

</dss:VerifyResponse>
```

Ejemplo 13. Validación de una firma electrónica registrada en un gestor documental

En la siguiente figura se muestra una petición de validación de firma en la cual la firma a validar y el documento firmado están registrados en un gestor documental externo.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyRequest Profile="urn:afirma:dss:1.0:profile:XSS" RequestID="BCHBHGCFFFIID1" xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

        <dss:InputDocuments>

            <dss:Other>

                <cmism:getContentStream xmlns:cmism="http://docs.oasis-open.org/ns/cmis/messaging/200908/">


        <cmism:repositoryId>ALFRESCO_NODO_210</cmism:repositoryId>

                    <cmism:objectId>9fc51b00-f3ad-11de-a59b-d593cdd6d7fd</cmism:objectId>

                </cmism:getContentStream>

            </dss:Other>

        </dss:InputDocuments>

        <dss:OptionalInputs>

            <dss:ClaimedIdentity>

                <dss:Name>appPrueba</dss:Name>

            </dss:ClaimedIdentity>
```

```
            </dss:OptionalInputs>

            <dss:SignatureObject>

                <dss:Other>

                    <cmism:getContentStream xmlns:cmism="http://docs.oasis-
open.org/ns/cmis/messaging/200908/">


            <cmism:repositoryId>ALFRESCO_NODO_210</cmism:repositoryId>

                        <cmism:objectId>dde4c59b-4b92-11df-aed4-
cb0bb0fce2df</cmism:objectId>

                    </cmism:getContentStream>

                </dss:Other>

            </dss:SignatureObject>

</dss:VerifyRequest>
```

Si la firma es válida el mensaje de respuesta sería como el siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyResponse Profile="urn:afirma:dss:1.0:profile:XSS" RequestID="BCHBHGCFFFIID1"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>


            <dss:ResultMajor>urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature</dss:ResultMaj
or>
```

```
                    <dss:ResultMessage xml:lang="es">La firma es valida</dss:ResultMessage>

            </dss:Result>

</dss:VerifyResponse>
```

A.4.5 Ejemplos de Upgrade de Firma

Ejemplo 14. Upgrade de Firma sobre una firma registrada en @firma

La siguiente petición corresponde a una petición de actualización de firma donde la firma ya se encontraba registrada en la plataforma.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:OptionalInputs>

                    <dss:ClaimedIdentity>

                            <dss:Name>tester</dss:Name>

                    </dss:ClaimedIdentity>

                    <afxp:TargetSigner><![CDATA[MIIDf....]]></afxp:TargetSigner>

                    <dss:ReturnUpdatedSignature
```

```
Type="urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T"/>

        <afxp:UpdatedSignatureMode>urn:afirma:dss:1.0:profile:XSS:upgrade:NoCertificateVali
dation</afxp:UpdatedSignatureMode>

        </dss:OptionalInputs>

        <dss:SignatureObject>

                <dss:Other>

                        <afxp:SignatureArchiveId
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema">1228319769910004</afxp:SignatureArchiveId>

                </dss:Other>

        </dss:SignatureObject>

</dss:VerifyRequest>
```

En este caso el mensaje de respuesta sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyResponse                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:Result>


        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                <dss:ResultMessage xml:lang="es">Proceso de actualización de firma realizado
correctamente.</dss:ResultMessage>
```

```
        </dss:Result>
        <dss:OptionalOutputs>
            <dss:DocumentWithSignature>
                <dss:Document ID="BCCIDCBJAGFJA0">
                    <dss:Base64XML><![CDATA[PD94b.....]]></dss:Base64XML>
                </dss:Document>
            </dss:DocumentWithSignature>
            <dss:UpdatedSignature>
                <dss:SignatureObject>
                    <dss:SignaturePtr WhichDocument="BCCIDCBJAGFJA0"/>
                </dss:SignatureObject>
            </dss:UpdatedSignature>
        </dss:OptionalOutputs>
</dss:VerifyResponse>
```

Ejemplo 15. Upgrade de Firma sobre una firma incluida en la petición

En el siguiente ejemplo se muestra una petición de actualización donde se incluye la firma a actualizar en lugar de su identificador de transacción.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
            <dss:InputDocuments>
                  <dss:Document ID="1228322297948">
                        <dss:Base64XML><![CDATA[PD94bWw……]]></dss:Base64XML>
                  </dss:Document>
            </dss:InputDocuments>
            <dss:OptionalInputs>
                  <dss:ClaimedIdentity>
                        <dss:Name>tester</dss:Name>
                  </dss:ClaimedIdentity>
                  <afxp:TargetSigner><![CDATA[MIIDfD…..]]></afxp:TargetSigner>
                  <dss:ReturnUpdatedSignature
Type="urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T"/>

            <afxp:UpdatedSignatureMode>urn:afirma:dss:1.0:profile:XSS:upgrade:NoCertificateVali
dation</afxp:UpdatedSignatureMode>
            </dss:OptionalInputs>
            <dss:SignatureObject>
                  <dss:SignaturePtr WhichDocument="1228322297948"/>
            </dss:SignatureObject>
</dss:VerifyRequest>
```

En este caso el mensaje de respuesta es:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyResponse                                    Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xss="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:Result>


        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                <dss:ResultMessage xml:lang="es">Proceso de actualización de firma realizado
correctamente.</dss:ResultMessage>

        </dss:Result>

        <dss:OptionalOutputs>

                <dss:DocumentWithSignature>

                        <dss:Document ID="BCCIDCCFGABFG0">


        <dss:Base64XML><![CDATA[PD94bWwg....]]></dss:Base64XML>

                        </dss:Document>

                </dss:DocumentWithSignature>

                <dss:UpdatedSignature>

                        <dss:SignatureObject>

                                <dss:SignaturePtr WhichDocument="BCCIDCCFGABFG0"/>

                        </dss:SignatureObject>
```

```
                    </dss:UpdatedSignature>

                    <xss:ArchiveInfo>

                            <arch:ArchiveIdentifier>1228322535998004</arch:ArchiveIdentifier>

                    </xss:ArchiveInfo>

            </dss:OptionalOutputs>

</dss:VerifyResponse>
```

Ejemplo 16. Upgrade de Firma sobre una firma registrada en un gestor documental

El siguiente ejemplo muestra una petición de actualización de firma en un gestor documental

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyRequest                                  Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

            <dss:OptionalInputs>

                    <dss:ClaimedIdentity>

                            <dss:Name>appPrueba</dss:Name>

                    </dss:ClaimedIdentity>

                    <dss:ReturnUpdatedSignature
Type="urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T"/>

            </dss:OptionalInputs>

            <dss:SignatureObject>

                    <dss:Other>
```

```
                    <cmism:getContentStream xmlns:cmism="http://docs.oasis-
open.org/ns/cmis/messaging/200908/">

            <cmism:repositoryId>ALFRESCO_NODO_210</cmism:repositoryId>

                        <cmism:objectId>2f2879a0-492a-11df-aed4-
cb0bb0fce2df</cmism:objectId>

                    </cmism:getContentStream>

                </dss:Other>

            </dss:SignatureObject>

</dss:VerifyRequest>
```

La respuesta asociada sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyResponse Profile="urn:afirma:dss:1.0:profile:XSS"
xmlns:ades="urn:oasis:names:tc:dss:1.0:profiles:AdES:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>

            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                <dss:ResultMessage xml:lang="es">Proceso de actualización de firma realizado
correctamente.</dss:ResultMessage>

            </dss:Result>
```

```
            <dss:OptionalOutputs>
                        <dss:UpdatedSignature>
                                    <dss:SignatureObject>
                                                <dss:Base64Signature
Type="http://uri.etsi.org/01733/v1.7.3#"><![CDATA[MIIM0Q....]]></dss:Base64Signature>
                                    </dss:SignatureObject>
                        </dss:UpdatedSignature>
                        <dss:SignatureType>http://uri.etsi.org/01733/v1.7.3#</dss:SignatureType>
                        <ades:SignatureForm>urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-
T</ades:SignatureForm>
            </dss:OptionalOutputs>
</dss:VerifyResponse>
```

A.4.6 Ejemplos de Validación de Certificados

Ejemplo 17. Validación de un certificado incluido en una petición

En la siguiente figura se observa una petición de validación de certificado, en ella se ha solicitado que se incluya los certificados y evidencia de revocación utilizados. Se debe incluir información sobre toda la cadena de certificación (allDetails) y se ha solicitado que se devuelva el "parseo" del certificado (ReturnReadableCertificateInfo)

```
<?xml version="1.0" encoding="UTF-8"?>
<dss:VerifyRequest Profile="urn:afirma:dss:1.0:profile:XSS" RequestID="BCFFEEAFJHAGE0"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
```

```
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

        <dss:OptionalInputs>

            <dss:ClaimedIdentity>

                <dss:Name>tester</dss:Name>

            </dss:ClaimedIdentity>

            <afxp:ReturnReadableCertificateInfo/>

            <vr:ReturnVerificationReport>

                <vr:CheckOptions>

                    <vr:CheckCertificateStatus>true</vr:CheckCertificateStatus>

                </vr:CheckOptions>

                <vr:ReportOptions>

                    <vr:IncludeCertificateValues>true</vr:IncludeCertificateValues>

                    <vr:IncludeRevocationValues>true</vr:IncludeRevocationValues>


        <vr:ReportDetailLevel>urn:oasis:names:tc:dss:1.0:reportdetail:allDetails</vr:ReportDetailLev
el>

                </vr:ReportOptions>

            </vr:ReturnVerificationReport>

        </dss:OptionalInputs>

        <dss:SignatureObject>
```

```
                    <dss:Other>
                        <ds:X509Data>
                            <ds:X509Certificate><![CDATA[MIIDP….]]></ds:X509Certificate>
                        </ds:X509Data>
                    </dss:Other>
                </dss:SignatureObject>
</dss:VerifyRequest>
```

La respuesta que obtendríamos podría ser como la representada en la siguiente figura:

```
<?xml version="1.0" encoding="UTF-8"?>
<dss:VerifyResponse Profile="urn:afirma:dss:1.0:profile:XSS" RequestID="BCFFEEAFJHAGE0"
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                <dss:Result>

                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                <dss:ResultMinor>urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:valid:certificate:De
finitive</dss:ResultMinor>
                    <dss:ResultMessage xml:lang="es">El certificado es válido</dss:ResultMessage>
```

```
            </dss:Result>
            <dss:OptionalOutputs>
                  <afxp:ReadableCertificateInfo>
                        <afxp:ReadableField>
                              <afxp:FieldIdentity>Subject</afxp:FieldIdentity>

            <afxp:FieldValue>EMAIL=felipe.barrera@telvent.com,CN=Felipe      Barrera,OU=TELVENT
INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</afxp:FieldValue>
                        </afxp:ReadableField>
                        <afxp:ReadableField>
                              <afxp:FieldIdentity>idPolitica</afxp:FieldIdentity>
                              <afxp:FieldValue>DEFAULT</afxp:FieldValue>
                        </afxp:ReadableField>
                        <afxp:ReadableField>
                              <afxp:FieldIdentity>versionPolitica</afxp:FieldIdentity>
                              <afxp:FieldValue>1</afxp:FieldValue>
                        </afxp:ReadableField>
                  </afxp:ReadableCertificateInfo>
                  <vr:CertificatePathValidity>
                        <vr:PathValiditySummary
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">
```

```
<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:Valid</dss:Code>

</vr:PathValiditySummary>

<vr:CertificateIdentifier>

<ds:X509IssuerName>EMAIL=desarrollo@telvent.com,CN=PERSONA_ENTIDAD,OU=TELVENT INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</ds:X509IssuerName>

<ds:X509SerialNumber>6</ds:X509SerialNumber>

</vr:CertificateIdentifier>

<vr:PathValidityDetail>

<vr:CertificateValidity>

<vr:CertificateIdentifier>

<ds:X509IssuerName>EMAIL=desarrollo@telvent.com,CN=PERSONA_ENTIDAD,OU=TELVENT INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</ds:X509IssuerName>

<ds:X509SerialNumber>6</ds:X509SerialNumber>

</vr:CertificateIdentifier>

<vr:Subject>EMAIL=felipe.barrera@telvent.com,CN=Felipe Barrera,OU=TELVENT INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</vr:Subject>

<vr:SignatureOK>

<vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">
```

```
            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidSignature</dss:Cod
e>
                                                    </vr:SigMathOK>
                                                </vr:SignatureOK>
                                                <vr:ExtensionsOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidExtension</dss:Cod
e>
                                                </vr:ExtensionsOK>
                                                <vr:ValidityPeriodOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidPeriod</dss:Code>
                                                </vr:ValidityPeriodOK>
                                                <vr:CertificateStatus>
                                                    <vr:CertStatusOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidStatus</dss:Code>
                                                    </vr:CertStatusOK>
                                                    <vr:RevocationEvidence>
                                                    .....<vr:CRLValidity>
                                                    .....
```

```
<vr:CRLIdentifier>

                                                                    .....

<xades:Issuer>1.2.840.113549.1.9.1=#16146a612e726f6d616e4074656c76656e742e636f
6d,CN=PERSONA_ENTIDAD,OU=TELVENT                                    INTERACTIVA,O=TELVENT
INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</xades:Issuer>

                                                                    .....

<xades:IssueTime>2009-10-06T15:22:53.000Z</xades:IssueTime>

                                                                    .....

</vr:CRLIdentifier>

                                                                    .....

<vr:SignatureOK>

                                                                    .....

<vr:SigMathOK Type="urn:afirma:dss:1.0:profile:XSS:detail:RevocationStatusEvidence">

                                                                    .....

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:RevocationStatusEvidence:code:ValidSign
ature</dss:Code>

                                                                    .....

</vr:SigMathOK>

                                                                    .....

</vr:SignatureOK>

                                                                    .....

<vr:CRLValue><![CDATA[MIIBj....]]></vr:CRLValue>

                                                                    ..... </vr:CRLValidity>

                                                                  </vr:RevocationEvidence>
```

```
                                        </vr:CertificateStatus>

                                    </vr:CertificateValidity>

                                    <vr:CertificateValidity>

                                        <vr:CertificateIdentifier>

            <ds:X509IssuerName>EMAIL=desarrollo@telvent.com,CN=DESARROLLO,O=TELVENT
INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</ds:X509IssuerName>

            <ds:X509SerialNumber>3</ds:X509SerialNumber>

                                        </vr:CertificateIdentifier>

            <vr:Subject>EMAIL=desarrollo@telvent.com,CN=PERSONA_ENTIDAD,OU=TELVENT
INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</vr:Subject>

            <vr:CertificateValue><![CDATA[MIIDID....]]></vr:CertificateValue>

                                        <vr:SignatureOK>

                                            <vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidSignature</dss:Cod
e>

                                            </vr:SigMathOK>

                                        </vr:SignatureOK>

                                        <vr:ExtensionsOK
```

```
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidExtension</dss:Cod
e>
                                                </vr:ExtensionsOK>
                                                <vr:ValidityPeriodOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidPeriod</dss:Code>
                                                </vr:ValidityPeriodOK>
                                                <vr:CertificateStatus>
                                                        <vr:CertStatusOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidStatus</dss:Code>
                                                        </vr:CertStatusOK>
                                                        <vr:RevocationEvidence>
                                                        ..... <vr:CRLValidity>
                                                        .....
            <vr:CRLIdentifier>
                                                        .....
            <xades:Issuer>1.2.840.113549.1.9.1=#16146a612e726f6d616e4074656c76656e742e636f
6d,CN=DESARROLLO,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</xades:Issuer>
                                                        .....
```

```
<xades:IssueTime>2009-10-06T15:15:18.000Z</xades:IssueTime>

                                                    .....
</vr:CRLIdentifier>

                                                    .....
<vr:SignatureOK>

                                                    .....
<vr:SigMathOK Type="urn:afirma:dss:1.0:profile:XSS:detail:RevocationStatusEvidence">

                                                    .....

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:RevocationStatusEvidence:code:ValidSign
ature</dss:Code>

                                                    .....
</vr:SigMathOK>

                                                    .....
</vr:SignatureOK>

                                                    .....
<CRLValue><![CDATA[MIIB....]]></CRLValue>

                                                    ..... </vr:CRLValidity>

                                                  </vr:RevocationEvidence>

                                            </vr:CertificateStatus>

                                    </vr:CertificateValidity>

                                    <vr:CertificateValidity>

                                            <vr:CertificateIdentifier>
```

```
<ds:X509IssuerName>EMAIL=desarrollo@telvent.com,CN=DESARROLLO,O=TELVENT
INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</ds:X509IssuerName>

<ds:X509SerialNumber>1</ds:X509SerialNumber>
                                        </vr:CertificateIdentifier>

<vr:Subject>EMAIL=desarrollo@telvent.com,CN=DESARROLLO,O=TELVENT
INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</vr:Subject>

<vr:CertificateValue><![CDATA[MIICzz...]]></vr:CertificateValue>
                                        <vr:SignatureOK>
                                            <vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidSignature</dss:Cod
e>
                                            </vr:SigMathOK>
                                        </vr:SignatureOK>
                                        <vr:ExtensionsOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidExtension</dss:Cod
e>
                                        </vr:ExtensionsOK>
                                        <vr:ValidityPeriodOK
```

```
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidPeriod</dss:Code>

                                        </vr:ValidityPeriodOK>

                                    </vr:CertificateValidity>

                                    <vr:TrustOrigin
Type="urn:oasis:names:tc:dss:1.0:trustorigin:certDataBase"/>

                                </vr:PathValidityDetail>

                        </vr:CertificatePathValidity>

            </dss:OptionalOutputs>

</dss:VerifyResponse>
```

Ejemplo 18. Validación de un certificado registrado en un gestor documental

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyRequest        Profile="urn:afirma:dss:1.0:profile:XSS"        RequestID="BCHCCJAHDFGEB13"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

            <dss:OptionalInputs>

                        <dss:ClaimedIdentity>

                                <dss:Name>appPrueba</dss:Name>

                        </dss:ClaimedIdentity>

                        <vr:ReturnVerificationReport
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#">
```

```
                        <vr:CheckOptions
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#">
                                <vr:CheckCertificateStatus>true</vr:CheckCertificateStatus>
                        </vr:CheckOptions>
                        <vr:ReportOptions
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#">
                                <vr:IncludeCertificateValues>false</vr:IncludeCertificateValues>

        <vr:IncludeRevocationValues>false</vr:IncludeRevocationValues>

        <vr:ReportDetailLevel>urn:oasis:names:tc:dss:1.0:reportdetail:allDetails</vr:ReportDetailLev
el>
                        </vr:ReportOptions>
                </vr:ReturnVerificationReport>
        </dss:OptionalInputs>
        <dss:SignatureObject>
                <dss:Other>
                        <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                <cmism:getContentStream      xmlns:cmism="http://docs.oasis-
open.org/ns/cmis/messaging/200908/">

        <cmism:repositoryId>ALFRESCO_NODO_210</cmism:repositoryId>
                                        <cmism:objectId>9e9363de-5135-11df-aed4-
```

```
cb0bb0fce2df</cmism:objectId>
                                        </cmism:getContentStream>
                                    </ds:X509Data>
                                </dss:Other>
                            </dss:SignatureObject>
</dss:VerifyRequest>
```

El mensaje de respuesta sería similar al siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:VerifyResponse Profile="urn:afirma:dss:1.0:profile:XSS" RequestID="BCHCCJAHDFGEB13"
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>


            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>


            <dss:ResultMinor>urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:valid:certificate:D
efinitive</dss:ResultMinor>

                        <dss:ResultMessage xml:lang="es">El certificado es
```

válido</dss:ResultMessage>

</dss:Result>

<dss:OptionalOutputs>

<vr:CertificatePathValidity>

<vr:PathValiditySummary
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:Valid</dss:Code>

</vr:PathValiditySummary>

<vr:CertificateIdentifier>

<ds:X509IssuerName>EMAIL=ja.roman@telvent.com,CN=PERSONA_ENTIDAD,OU=TELV
ENT INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</ds:X509IssuerName>

<ds:X509SerialNumber>6</ds:X509SerialNumber>

</vr:CertificateIdentifier>

<vr:PathValidityDetail>

<vr:CertificateValidity>

<vr:CertificateIdentifier>

<ds:X509IssuerName>EMAIL=ja.roman@telvent.com,CN=PERSONA_ENTIDAD,OU=TELV
ENT INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</ds:X509IssuerName>

<ds:X509SerialNumber>6</ds:X509SerialNumber>

```
                                        </vr:CertificateIdentifier>

        <vr:Subject>EMAIL=perico@telvent.com,CN=Periquillo el de los Palotes,OU=TELVENT
INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</vr:Subject>

                                        <vr:ValidityPeriodOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

        <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidPeriod</dss:Code>

                                        </vr:ValidityPeriodOK>

                                        <vr:ExtensionsOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

        <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidExtension</dss:Co
de>

                                        </vr:ExtensionsOK>

                                        <vr:SignatureOK>

                                                <vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

        <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidSignature</dss:Cod
e>

                                                </vr:SigMathOK>

                                        </vr:SignatureOK>

                                        <vr:CertificateStatus>
```

```
                                                    <vr:CertStatusOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidStatus</dss:Code>

                                                    </vr:CertStatusOK>

                                                    <vr:RevocationEvidence>

                                                    ..... <vr:CRLValidity>

                                                    .....

            <vr:CRLIdentifier>

                                                    .....

            <xades:Issuer>1.2.840.113549.1.9.1=#16146a612e726f6d616e4074656c76656e742e636
f6d,CN=PERSONA_ENTIDAD,OU=TELVENT                    INTERACTIVA,O=TELVENT
INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</xades:Issuer>

                                                    .....

            <xades:IssueTime>2010-04-09T06:23:16.000Z</xades:IssueTime>

                                                    .....

            </vr:CRLIdentifier>

                                                    .....

            <vr:SignatureOK>

                                                    .....

            <vr:SigMathOK Type="urn:afirma:dss:1.0:profile:XSS:detail:RevocationStatusEvidence">

                                                    .....

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:RevocationStatusEvidence:code:ValidSig
nature</dss:Code>

                                                    .....
```

```
            </vr:SigMathOK>

                                                                    .....

            </vr:SignatureOK>

                                                                    ..... </vr:CRLValidity>

                                                                </vr:RevocationEvidence>

                                                        </vr:CertificateStatus>

                                                </vr:CertificateValidity>

                                                <vr:CertificateValidity>

                                                        <vr:CertificateIdentifier>


            <ds:X509IssuerName>EMAIL=ja.roman@telvent.com,CN=DESARROLLO,O=TELVENT
INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</ds:X509IssuerName>


            <ds:X509SerialNumber>3</ds:X509SerialNumber>

                                                        </vr:CertificateIdentifier>


            <vr:Subject>EMAIL=ja.roman@telvent.com,CN=PERSONA_ENTIDAD,OU=TELVENT
INTERACTIVA,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</vr:Subject>

                                                        <vr:ValidityPeriodOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">


            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidPeriod</dss:Code>

                                                        </vr:ValidityPeriodOK>

                                                        <vr:ExtensionsOK
```

```
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidExtension</dss:Co
de>
                                                </vr:ExtensionsOK>
                                                <vr:SignatureOK>
                                                        <vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidSignature</dss:Cod
e>
                                                        </vr:SigMathOK>
                                                </vr:SignatureOK>
                                                <vr:CertificateStatus>
                                                        <vr:CertStatusOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

            <dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidStatus</dss:Code>
                                                        </vr:CertStatusOK>
                                                        <vr:RevocationEvidence>
                                                         ..... <vr:CRLValidity>
                                                         .....
            <vr:CRLIdentifier>
                                                         .....
```

```
<xades:Issuer>1.2.840.113549.1.9.1=#16146a612e726f6d616e4074656c76656e742e636
f6d,CN=DESARROLLO,O=TELVENT INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</xades:Issuer>

                                                    .....
<xades:IssueTime>2010-04-09T06:31:47.000Z</xades:IssueTime>

                                                    .....
</vr:CRLIdentifier>

                                                    .....
<vr:SignatureOK>

                                                    .....
<vr:SigMathOK Type="urn:afirma:dss:1.0:profile:XSS:detail:RevocationStatusEvidence">

                                                    .....

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:RevocationStatusEvidence:code:ValidSig
nature</dss:Code>

                                                    .....
</vr:SigMathOK>

                                                    .....
</vr:SignatureOK>

                                                    ..... </vr:CRLValidity>

                                                </vr:RevocationEvidence>

                                            </vr:CertificateStatus>

                                        </vr:CertificateValidity>

                                        <vr:CertificateValidity>

                                            <vr:CertificateIdentifier>
```

```
<ds:X509IssuerName>EMAIL=ja.roman@telvent.com,CN=DESARROLLO,O=TELVENT
INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</ds:X509IssuerName>

<ds:X509SerialNumber>1</ds:X509SerialNumber>
                                        </vr:CertificateIdentifier>

<vr:Subject>EMAIL=ja.roman@telvent.com,CN=DESARROLLO,O=TELVENT
INTERACTIVA,L=SEVILLA,ST=ANDALUCIA,C=ES</vr:Subject>
                                        <vr:ValidityPeriodOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidPeriod</dss:Code>
                                        </vr:ValidityPeriodOK>
                                        <vr:ExtensionsOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidExtension</dss:Co
de>
                                        </vr:ExtensionsOK>
                                        <vr:SignatureOK>
                                            <vr:SigMathOK
Type="urn:afirma:dss:1.0:profile:XSS:detail:Certificate">

<dss:Code>urn:afirma:dss:1.0:profile:XSS:detail:Certificate:code:ValidSignature</dss:Cod
```

```
e>
                                                    </vr:SigMathOK>
                                                </vr:SignatureOK>
                                            </vr:CertificateValidity>
                                            <vr:TrustOrigin
Type="urn:oasis:names:tc:dss:1.0:trustorigin:certDataBase"/>
                                        </vr:PathValidityDetail>
                                    </vr:CertificatePathValidity>
                            </dss:OptionalOutputs>
</dss:VerifyResponse>
```

A.4.7 Ejemplos de Validaciones de Firmas en Lote

Ejemplo 19. Validación de dos firmas electrónicas

El siguiente ejemplo muestra una petición de validación de firma en lote, en él se solicita la validación de dos firmas electrónicas.

```
<?xml version="1.0" encoding="UTF-8"?>

<afxp:BatchRequest                                          Profile="urn:afirma:dss:1.0:profile:XSS"
Type="urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifySignatureType"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#">

                <dss:OptionalInputs>
```

```
                    <dss:ClaimedIdentity>
                        <dss:Name>tester</dss:Name>
                    </dss:ClaimedIdentity>
                </dss:OptionalInputs>
                <afxp:Requests>
                    <dss:VerifyRequest Profile="urn:afirma:dss:1.0:profile:XSS"
RequestID="BCFFEEHJFADHA0">
                        <dss:OptionalInputs>
                            <vr:ReturnVerificationReport >
                                <vr:ReportOptions>

                <vr:IncludeCertificateValues>false</vr:IncludeCertificateValues>

                <vr:IncludeRevocationValues>false</vr:IncludeRevocationValues>

                <vr:ReportDetailLevel>urn:oasis:names:tc:dss:1.0:reportdetail:noDetails</vr:ReportDetailLev
el>
                                </vr:ReportOptions>
                            </vr:ReturnVerificationReport>
                        </dss:OptionalInputs>
                        <dss:SignatureObject >
                            <dss:Base64Signature
```

```
><![CDATA[MIIR.....]]></dss:Base64Signature>

                    </dss:SignatureObject>

                </dss:VerifyRequest>

                <dss:VerifyRequest                    Profile="urn:afirma:dss:1.0:profile:XSS"
RequestID="BCFFEEEEBEEID1" >

                    <dss:InputDocuments >

                        <dss:Document ID="BCFFEEHJFAGGH1" >


        <dss:Base64XML><![CDATA[PD94b....]]></dss:Base64XML>

                        </dss:Document>

                    </dss:InputDocuments>

                    <dss:OptionalInputs >

                        <vr:ReturnVerificationReport">

                            <vr:ReportOptions">


        <vr:IncludeCertificateValues>false</vr:IncludeCertificateValues>


        <vr:IncludeRevocationValues>false</vr:IncludeRevocationValues>


        <vr:ReportDetailLevel>urn:oasis:names:tc:dss:1.0:reportdetail:noDetails</vr:ReportDetailLev
el>

                            </vr:ReportOptions>
```

```
                    </vr:ReturnVerificationReport>
                </dss:OptionalInputs>
                <dss:SignatureObject >
                    <dss:SignaturePtr WhichDocument="BCFFEEEEBEFDA2" />
                </dss:SignatureObject>
            </dss:VerifyRequest>
        </afxp:Requests>
</afxp:BatchRequest>
```

Ante una petición de este tipo la respuesta del servidor debe ser del tipo “pendiente de procesado”, como la mostrada a continuación.

```
<?xml version="1.0" encoding="UTF-8"?>
<afxp:BatchResponse Profile="urn:afirma:dss:1.0:profile:XSS"
Type="urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifySignatureType"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:async="urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <dss:Result>

        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmaj
or:Pending</dss:ResultMajor>
            <dss:ResultMessage xml:lang="es">El proceso se encuentra pendiente de
procesado.</dss:ResultMessage>
```

```
            </dss:Result>

            <dss:OptionalOutputs>

                  <async:ResponseID> 1255447914911003</async:ResponseID>

                  <afxp:ResponseTime>2009-10-14T07:35:00.545Z</afxp:ResponseTime>

            </dss:OptionalOutputs>

</afxp:BatchResponse>
```

Una vez procesada la petición la respuesta generada incluirá el resultado de cada verificación. En la siguiente figura podemos ver la respuesta a la consulta anterior.

```
<?xml version="1.0" encoding="UTF-8"?>

<afxp:BatchResponse Profile="urn:afirma:dss:1.0:profile:XSS" RequestID="BCFFEEIDGIGEC0"
Type="urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifySignatureType"
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>


            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                  <dss:ResultMessage xml:lang="es">Proceso en lote finalizado
correctamente</dss:ResultMessage>

            </dss:Result>

            <afxp:Responses>

                  <dss:VerifyResponse Profile="urn:afirma:dss:1.0:profile:XSS"
```

```
RequestID="BCFFEEHJFAGGH1">

                        <dss:Result>

        <dss:ResultMajor>urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature</dss:ResultMaj
or>

                            <dss:ResultMessage xml:lang="es">La firma es
valida</dss:ResultMessage>

                        </dss:Result>

                        <dss:OptionalOutputs>

                            <vr:VerificationReport>

                                <vr:IndividualSignatureReport>

                                    <vr:SignatureIdentifier>

                                    .....<vr:DigestAlgAndValue>

                                    .....
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

                                    .....
        <ds:DigestValue><![CDATA[tU/klWcaC6YgSlhb1Rb/CrJbl/M=]]></ds:DigestValue>

                                    ..... </vr:DigestAlgAndValue>

                                    </vr:SignatureIdentifier>

                                    <dss:Result>

        <dss:ResultMajor>urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature</dss:ResultMaj
or>
```

```
                                        <dss:ResultMessage xml:lang="es">La firma es
valida</dss:ResultMessage>

                                        </dss:Result>

                                    </vr:IndividualSignatureReport>

                                </vr:VerificationReport>

                            </dss:OptionalOutputs>

                        </dss:VerifyResponse>

                        <dss:VerifyResponse                    Profile="urn:afirma:dss:1.0:profile:XSS"
RequestID="BCFFEEHJFADHA0">

                            <dss:Result>

                <dss:ResultMajor>urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature</dss:ResultMaj
or>

                                <dss:ResultMessage    xml:lang="es">La    firma    es
valida</dss:ResultMessage>

                            </dss:Result>

                            <dss:OptionalOutputs>

                                <vr:VerificationReport>

                                    <vr:IndividualSignatureReport>

                                        <vr:SignatureIdentifier>

                                        .....<vr:DigestAlgAndValue>

                                        .....
```

```
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

                                                                    .....
            <ds:DigestValue><![CDATA[VjlGeP1yC0nApBz9ESuARg1cTuU=]]></ds:DigestValue>

                                                                    ..... </vr:DigestAlgAndValue>

                                                                    </vr:SignatureIdentifier>

                                                                    <dss:Result>


            <dss:ResultMajor>urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature</dss:ResultMaj
or>

                                                                    <dss:ResultMessage xml:lang="es">La firma es
valida</dss:ResultMessage>

                                                                    </dss:Result>

                                                            </vr:IndividualSignatureReport>

                                                    </vr:VerificationReport>

                                            </dss:OptionalOutputs>

                                    </dss:VerifyResponse>

            </afxp:Responses>

</afxp:BatchResponse>
```

A.4.8 Ejemplos de Validaciones de Certificados en Lote

Ejemplo 20. Validación de dos certificados

En el siguiente ejemplo se muestra una petición de validación de certificados en lotes en el que se solicita la validación de dos certificados.

```
<?xml version="1.0" encoding="UTF-8"?>

<afxp:BatchRequest                                    Profile="urn:afirma:dss:1.0:profile:XSS"
Type="urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifyCertificateType"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:vr="urn:oasis:names:tc:dss:1.0:profiles:verificationreport:schema#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

        <dss:OptionalInputs>

                <dss:ClaimedIdentity>

                        <dss:Name>tester</dss:Name>

                </dss:ClaimedIdentity>

        </dss:OptionalInputs>

        <afxp:Requests>

                <dss:VerifyRequest                    Profile="urn:afirma:dss:1.0:profile:XSS"
RequestID="BCFFFAEBAICIJ0">

                        <dss:OptionalInputs>

                                <vr:ReturnVerificationReport>

                                        <vr:CheckOptions">
```

```
            <vr:CheckCertificateStatus>true</vr:CheckCertificateStatus>
                                        </vr:CheckOptions>
                                        <vr:ReportOptions">

            <vr:IncludeCertificateValues>false</vr:IncludeCertificateValues>

            <vr:IncludeRevocationValues>false</vr:IncludeRevocationValues>

            <vr:ReportDetailLevel>urn:oasis:names:tc:dss:1.0:reportdetail:noDetails</vr:ReportDetailLev
el>
                                        </vr:ReportOptions>
                                    </vr:ReturnVerificationReport>
                                </dss:OptionalInputs>
                                <dss:SignatureObject>
                                    <dss:Other>
                                        <ds:X509Data>

            <ds:X509Certificate><![CDATA[MIID....]]></ds:X509Certificate>
                                        </ds:X509Data>
                                    </dss:Other>
                                </dss:SignatureObject>
                            </dss:VerifyRequest>
```

```
<dss:VerifyRequest Profile="urn:afirma:dss:1.0:profile:XSS"
RequestID="BCFFFAEBAICIJ1">

<dss:OptionalInputs>

<vr:ReturnVerificationReport">

<vr:CheckOptions">

<vr:CheckCertificateStatus>true</vr:CheckCertificateStatus>

</vr:CheckOptions>

<vr:ReportOptions">

<vr:IncludeCertificateValues>false</vr:IncludeCertificateValues>

<vr:IncludeRevocationValues>false</vr:IncludeRevocationValues>

<vr:ReportDetailLevel>urn:oasis:names:tc:dss:1.0:reportdetail:noDetails</vr:ReportDetailLev
el>

</vr:ReportOptions>

</vr:ReturnVerificationReport>

</dss:OptionalInputs>

<dss:SignatureObject>

<dss:Other>

<ds:X509Data>
```

```
            <ds:X509Certificate><![CDATA[MIIDP….]]></ds:X509Certificate>
                                                    </ds:X509Data>
                                                </dss:Other>
                                            </dss:SignatureObject>
                                        </dss:VerifyRequest>
                                    </afxp:Requests>
</afxp:BatchRequest>
```

Ante una petición de este tipo el servidor registrará la misma para su posterior procesado devolviendo al cliente una respuesta como la mostrada a continuación.

```
<?xml version="1.0" encoding="UTF-8"?>

<afxp:BatchResponse                                    Profile="urn:afirma:dss:1.0:profile:XSS"
Type="urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifyCertificateType"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:async="urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

            <dss:Result>


            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmaj
or:Pending</dss:ResultMajor>

                        <dss:ResultMessage xml:lang="es">El proceso se encuentra pendiente de
procesado.</dss:ResultMessage>

            </dss:Result>
```

```
        <dss:OptionalOutputs>
            <async:ResponseID>1255503778157003</async:ResponseID>
            <afxp:ResponseTime>2009-10-14T15:42:00.693Z</afxp:ResponseTime>
        </dss:OptionalOutputs>
</afxp:BatchResponse>
```

Una vez procesada la petición se obtendría una respuesta como la mostrada a continuación.

```
<?xml version="1.0" encoding="UTF-8"?>
<afxp:BatchResponse Profile="urn:afirma:dss:1.0:profile:XSS" RequestID="BCFFFAFAJEBDA0"
Type="urn:afirma:dss:1.0:profile:XSS:BatchProtocol:VerifyCertificateType"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <dss:Result>

        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            <dss:ResultMessage xml:lang="es">Proceso en lote finalizado
correctamente</dss:ResultMessage>
        </dss:Result>
        <afxp:Responses>
            <dss:VerifyResponse Profile="urn:afirma:dss:1.0:profile:XSS"
RequestID="BCFFFAEBAICIJ0">
                <dss:Result>
```

<dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

<dss:ResultMinor>urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:invalid:certificate:Revoked</dss:ResultMinor>

<dss:ResultMessage xml:lang="es">El certificado se encuentra revocado</dss:ResultMessage>

</dss:Result>

</dss:VerifyResponse>

<dss:VerifyResponse Profile="urn:afirma:dss:1.0:profile:XSS" RequestID="BCFFFAEBAICIJ1">

<dss:Result>

<dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

<dss:ResultMinor>urn:oasis:names:tc:dss:1.0:profiles:XSS:resultminor:valid:certificate:Definitive</dss:ResultMinor>

<dss:ResultMessage xml:lang="es">El certificado es válido</dss:ResultMessage>

</dss:Result>

</dss:VerifyResponse>

</afxp:Responses>

</afxp:BatchResponse>

A.4.9 Ejemplos de Consulta de Petición Asíncrona

Ejemplo 21. Consulta del estado de un proceso asíncrono

En la siguiente figura se muestra un ejemplo de consulta de petición asíncrona

```
<?xml version="1.0" encoding="UTF-8"?>

<async:PendingRequest RequestID="BCFFEEIDGIGEC0"
xmlns:async="urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:1.0"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema">

        <dss:OptionalInputs >

                <dss:ClaimedIdentity>

                        <dss:Name>tester</dss:Name>

                </dss:ClaimedIdentity>

                <async:ResponseID>1255447914911003</async:ResponseID>

        </dss:OptionalInputs>

</async:PendingRequest>
```

Si la petición es válida se devolverá una respuesta acorde al servicio inicialmente invocado, en este ejemplo “Validaciones de Firmas en Lote”, en este caso el proceso todavía no ha finalizado.

```
<?xml version="1.0" encoding="UTF-8"?>

<afxp:BatchResponse Profile="urn:afirma:dss:1.0:profile:XSS" RequestID=" BCFFEEIDGIGEC0"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:async="urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
        <dss:Result>

        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmaj
or:Pending</dss:ResultMajor>

            <dss:ResultMessage xml:lang="es">El proceso se encuentra pendiente de
procesado.</dss:ResultMessage>

        </dss:Result>

        <dss:OptionalOutputs>

            <async:ResponseID>1255447914911015</async:ResponseID>

            <afxp:ResponseTime>2009-10-14T15:38:00.693Z</afxp:ResponseTime>

        </dss:OptionalOutputs>

</afxp:BatchResponse>
```

Si la petición de consulta no fuera válida se devolvería una respuesta como la siguiente.

```
<?xml version="1.0" encoding="UTF-8"?>

<dss:Response Profile="urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing"
RequestID="BCFFEEJCGIFDB0" xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:Result>

        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError</dss:ResultMa
jor>

        <dss:ResultMinor>urn:oasis:names:tc:dss:1.0:profiles:asynchronousprocessing:resultmin
```

```
or:ResponseIdUnknown</dss:ResultMinor>

                <dss:ResultMessage xml:lang="es">No existe proceso asíncrono 31051998 para
la aplicación tester</dss:ResultMessage>

        </dss:Result>

</dss:Response>
```

A.4.10 Ejemplos de Obtención de Firma por Identificador de Transacción

Ejemplo 22. Obtener firma mediante identificador de transacción

En la siguiente figura se muestra un ejemplo de petición de obtención de firma registrada.

```
<?xml version="1.0" encoding="UTF-8"?>

<arch:ArchiveRetrievalRequest                    Profile="urn:afirma:dss:1.0:profile:archive"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:OptionalInputs>

                <dss:ClaimedIdentity>

                        <dss:Name>tester</dss:Name>

                </dss:ClaimedIdentity>

        </dss:OptionalInputs>

        <arch:ArchiveIdentifier>1228379610138025</arch:ArchiveIdentifier>

</arch:ArchiveRetrievalRequest>
```

La respuesta a la petición anterior sería:

```
<?xml version="1.0" encoding="UTF-8"?>

<arch:ArchiveRetrievalResponse                    Profile="urn:afirma:dss:1.0:profile:archive"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:arch="urn:oasis:names:tc:dss:1.0:profiles:archive"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <dss:Result>


        <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>

                <dss:ResultMessage xml:lang="es">Proceso de obtención de la Firma Electrónica
realizado correctamente.</dss:ResultMessage>

        </dss:Result>

        <dss:OptionalOutputs>

                <dss:DocumentWithSignature>

                        <dss:Document ID="BCCIEHICCDEHC2">


        <dss:Base64XML><![CDATA[PD94bWwgdm....]]></dss:Base64XML>

                        </dss:Document>

                </dss:DocumentWithSignature>

        </dss:OptionalOutputs>

        <dss:SignatureObject>

                <dss:SignaturePtr WhichDocument="BCCIEHICCDEHC2"/>
```

```
            </dss:SignatureObject>

</arch:ArchiveRetrievalResponse>
```

A.5 Notas Sobre los Procesos de Upgrade de Firma

A continuación se detallan algunos aspectos importantes a tener en cuenta respecto a procesos de actualización de firma, o bien, en los procesos de generación de firma en formato no básico, en base a las respuestas que puede ofrecer la plataforma:

a) Si se indica realizar una operación de actualización a un formato en el que ya se encuentran todos los firmantes/contra-firmantes objetivo (salvo en los casos de resellado de archivado) la plataforma devolverá una respuesta con

ResultMajor → urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError

ResultMinor → urn:afirma:dss:1.0:profile:XSS:resultminor:IncorrectUpdateSignatureType

Y una descripción más precisa del error.

b) Si en un proceso de actualización al menos un firmante se actualiza al formato solicitado (siempre que no se haya producido un error en la inclusión u obtención de un sello de tiempo) la plataforma devolverá una respuesta con

ResultMajor → urn:oasis:names:tc:dss:1.0:resultmajor:Success

c) Si en un proceso de actualización se detecta al menos un contra-firmante que no puede ser actualizado al formato solicitado porque pertenece a un firmante con sello de tiempo de archivado, y ningún firmante/contra-firmante ha podido ser actualizado, la plataforma devolverá una respuesta con

ResultMajor → urn:oasis:names:tc:dss:1.0:resultmajor:Warning

ResultMinor → urn:afirma:dss:1.0:profile:XSS:resultminor:UnnecessaryUpgradeOperation

Y una descripción más precisa del error.

d) Si en un proceso de actualización alguno de los firmantes no puede ser actualizado con sello de tiempo, y para la aplicación utilizada se ha definido el sello de tiempo como **No Crítico**, la plataforma devolverá una respuesta con

ResultMajor → urn:oasis:names:tc:dss:1.0:resultmajor:Warning

ResultMinor → urn:afirma:dss:1.0:profile:XSS:resultminor:IncompleteUpgradeOperation

Y una descripción más precisa del error.

e) Si en un proceso de actualización alguno de los firmantes no puede ser actualizado con sello de tiempo, y para la aplicación utilizada se ha definido el sello de tiempo como **Crítico**, en el momento en que se produzca el primer error relacionado con la obtención de un sello de tiempo el proceso finalizará devolviendo la plataforma una respuesta con

ResultMajor → urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError

Y una descripción más precise del error.

A.6 Guía 807 del Esquema Nacional de Seguridad (ENS).

Les comunicamos que los productos de la Suite de @firma pueden contener entre los algoritmos disponibles, algunos no recomendados por la Guía 807 del Esquema Nacional de Seguridad (ENS; editada por el Centro Criptológico Nacional, CCN) vigente en el momento de publicación de este documento. Por lo que queda bajo la responsabilidad de las aplicaciones que hacen uso de estos productos el configurar adecuadamente las llamadas a los mismos para generar el resultado esperado, válido y adecuado para ese momento y el nivel de seguridad deseado, utilizando para ello algoritmos de la familia SHA-2 tal y como especifica dicha norma para la generación de firmas electrónicas.

Pueden consultar la norma vigente en el siguiente enlace:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html