@Firma ::Servicios DSS de @firma

Dirección General de Política Digital

Consejería de Hacienda y Administración Pública

Sevilla, 19 de Septiembre de 2013

ÍNDICE

Servicios de firma OASIS-DSS

- DSSAfirmaSign
- DSSAfirmaVerify
- DSSAfirmaArchiveSubmit
- DSSAfirmaArchiveRetrieval
- DSSAfirmaVerifyCertificate

OASIS-DSS (servicios DSS)

Índice

OASIS-DSS (servicios DSS)

¿Qué es OASIS?

Fundación, sin ánimo de lucro, para el establecimiento de estándares abiertos en la sociedad de la información.

Patrocinado por importantes empresas del sector.

OASIS-DSS (servicios DSS)

¿Qué es OASIS-DSS?

Digital Signature Services, define la interfaz para peticiones de servicios web que producen y/o verifican firmas digitales sobre unos datos dados.

Se basa en un par de mensajes XML petición/respuesta. A través de estos servicios un cliente puede enviar un mensaje solicitando la firma del servidor y recibiendo un XML que incluye la firma de los datos solicitados, o puede enviar una firma junto a los datos firmados y solicitar que se verifique, recibiendo una respuesta sobre si la firma es válida y corresponde con los datos enviados.

OASIS-DSS (servicios DSS)

Servicios DSS (perfil Afirma)

Servicios DSS del perfil Afirma

- **DSSAfirmaSign**. Firma y multifirma de servidor.
- **DSSAfirmaVerify**. Verificación de firma y obtención de información sobre la misma. Además permite la realización de un upgrade o actualización sobre la firma a un formato más avanzado (por ejemplo la inclusión de un sello de tiempo).
- **DSSAfirmaArchiveSubmit**. Servicio de registro de firmas.
- **DSSAfirmaArchiveRetrieval**. Servicio de obtención de firmas registradas.
- **DSSAfirmaVerifyCertificate**. Servicio de validación de certificado (a partir de @firma 5.5).
- **DSSBatchVerifyCertificate**. Servicio de validación masiva de certificados (a partir de @firma 5.5).
- **DSSBatchVerifySignature**. Servicio de validación masiva de firmas (a partir de @firma 5.5).
- **DSSAsyncRequestStatus**. Servicio de consulta del estado de peticiones asíncronas (a partir de @firma 5.5).

Limitaciones servicios DSS del perfil Afirma:

En la versión del núcleo 5.3.1, no está disponible un servicio para la validación de certificados.

- No existe servicio de firma en bloque
- No existe servicio para registrar documentos. Sólo se podrán registrar firmas.
- Los servicios nativos estarán obsoletos en la versión 5.5.

OASIS-DSS (servicios DSS)

Tipos y formatos de firma

Las diferentes estructuras de firmas compatibles por la plataforma vendrán especificadas por el tipo y el formato de la misma, ambos identificados por su URI. Los formatos compatibles son:

- **CMS**: urn:ietf:rfc:3369
- **CMS-T**: urn:afirma:dss:1.0:profile:XSS:forms:CMSWithTST
- **CAdES**: http://uri.etsi.org/01733/v1.7.3#
- **XAdES**: http://uri.etsi.org/01903/v1.3.2#
- **ODF**: urn:afirma:dss:1.0:profile:XSS:forms:ODF, firmas de Open Office, disponible en @firma 5.5
- **PDF**: urn:afirma:dss:1.0:profile:XSS:forms:PDF, firmas de PDF, disponible en @firma 5.5.

Los formatos CAdES y XAdES tienen asociado un perfil determinado:

- **BES**: urn:oasis.names:tc:dss:1.0:profiles:AdES:forms:BES: formato básico.
- **T**: urn:oasis:names:tc:dss:1.0:profiles:AdES:formas:ES-T: incluye sello de tiempo.
- **EPES**: urn:oasis:names:tc:dss:1.0:profiles:AdES:formas:EPES: incluye información sobre la política utilizada, a partir de @firma 5.5.
- **C**: urn:oasis:names:tc:dss:1.0:profiles:AdES:formas:ES-C, a partir de @firma 5.5.
- **X**: urn:oasis:names:tc:dss:1.0:profiles:AdES:formas:ES-T , a partir de @firma 5.5.
- **X-L**: urn:oasis:names:tc:dss:1.0:profiles:AdES:formas:ES-X-L , a partir de @firma 5.5.
- **A**: urn:oasis:names:tc:dss:1.0:profiles:AdES:formas:ES-A, a partir de @firma 5.5.

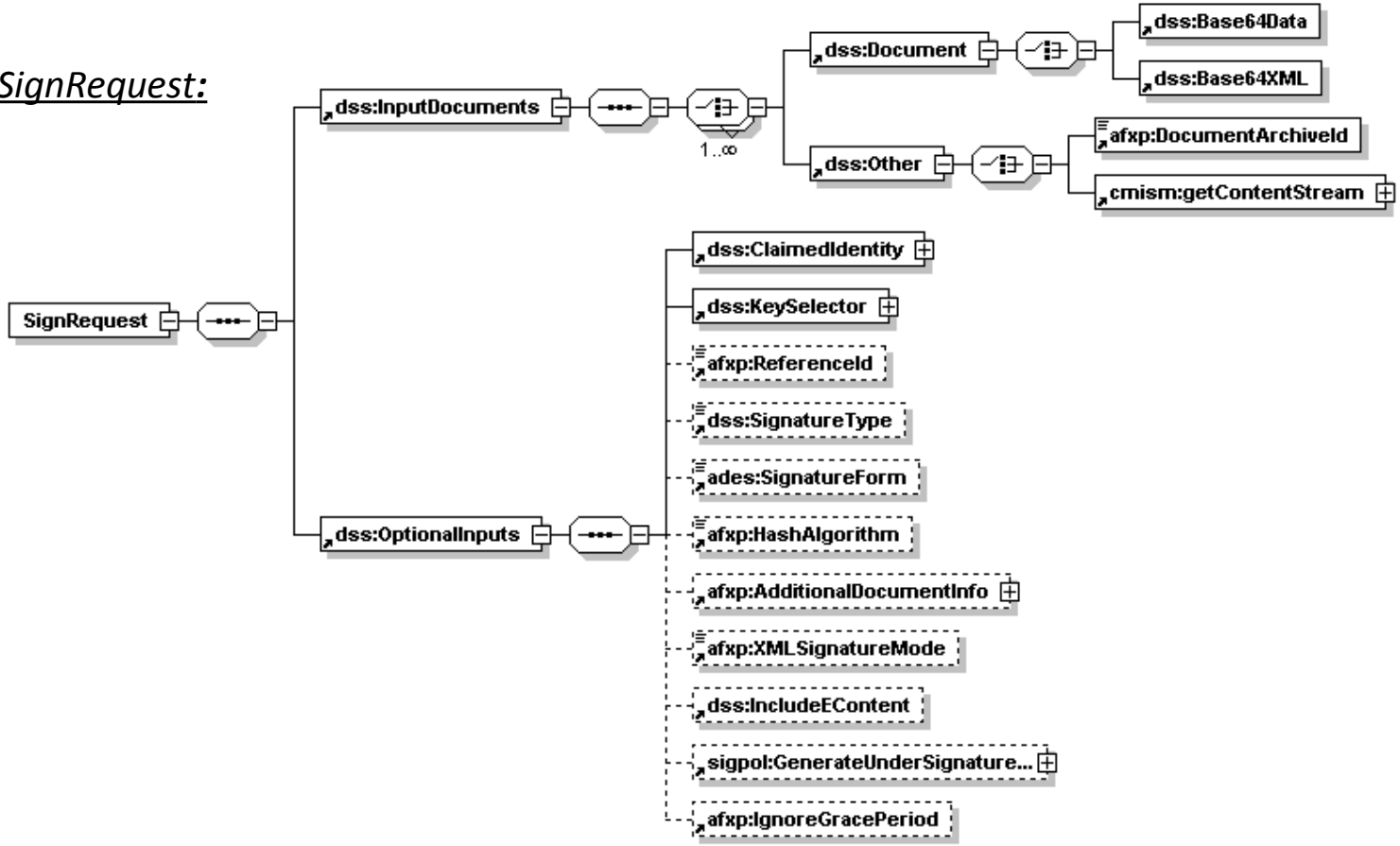
OASIS-DSS (servicios DSS)

DSSAfirmaSign - Firma de servidor

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. Los elementos definidos en OASIS con este objetivo son:

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

dss:SignRequest:



OASIS-DSS (servicios DSS)

DSSAfirmaSign vs FirmaServidor (Petición)

Petición DSS

```
<?xml version="1.0" encoding="UTF-8"?>
<dss:SignRequest>
    <dss:InputDocuments>
        <dss:Document>
            <dss:Base64Data>
                <![CDATA[cHJ1ZWJhLnR4dA==]]>
            </dss:Base64Data>
        </dss:Document>
    </dss:InputDocuments>
    <dss:OptionalInputs>
        <dss:ClaimedIdentity>
            <dss:Name>STERIA_TEST</dss:Name>
        </dss:ClaimedIdentity>
        <dss:KeySelector>
            <ds:KeyInfo>
                <ds:KeyName>default</ds:KeyName>
            </ds:KeyInfo>
        </dss:KeySelector>
        <dss:SignatureType>
            urn:ietf:rfc:3369
        </dss:SignatureType>
        <afxp:HashAlgorithm>
            http://www.w3.org/2000/09/xmldsig#sha1
        </afxp:HashAlgorithm>
        <afxp:AdditionalDocumentInfo>
            <afxp:DocumentName>
                prueba.txt
            </afxp:DocumentName>
            <afxp:DocumentType>txt</afxp:DocumentType>
        </afxp:AdditionalDocumentInfo>
    </dss:OptionalInputs>
</dss:SignRequest>
```

Petición nativa:

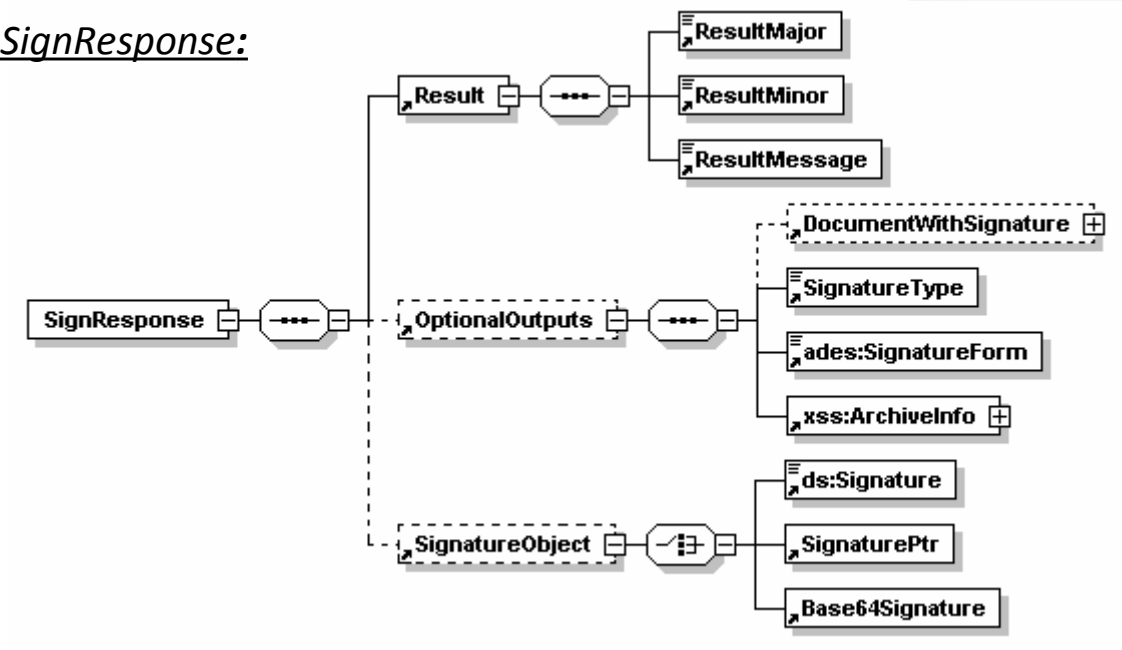
```
<?xml version="1.0" encoding="UTF-8"?>
<mensajeEntrada>
    <peticion>FirmaServidor</peticion>
    <versionMsg>1.0</versionMsg>
    <parametros>

<idAplicacion>STERIA_TEST</idAplicacion>
        <documento>
            <![CDATA[cHJ1ZWJhLnR4dA==]]>
        </documento>
        <nombreDocumento>
            prueba.txt
        </nombreDocumento>
        <tipoDocumento>txt</tipoDocumento>
        <firmante>default</firmante>
        <idReferencia />
        <algoritmoHash>SHA1</algoritmoHash>
        <formatoFirma>CMS</formatoFirma>
    </parametros>
</mensajeEntrada>
```

OASIS-DSS (servicios DSS)

DSSAfirmaSign (Respuesta)

dss:SignResponse:



OASIS-DSS (servicios DSS)

DSSAfirmaSign vs FirmaServidor (Respuesta)

Respuesta DSS:

```
<dss:SignResponse>
    <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:ietf:rfc:3369</dss:SignatureType>
        <xss:ArchiveInfo>
            <arch:ArchiveIdentifier>
                1340100597551030
            </arch:ArchiveIdentifier>
        </xss:ArchiveInfo>
    </dss:OptionalOutputs>
    <dss:SignatureObject>
        <dss:Base64Signature Type="urn:ietf:rfc:3369">
    <![CDATA[MIIH6wYJKoZIhvcNAQcIIH3DCCB...]]>
        </dss:Base64Signature>
    </dss:SignatureObject>
</dss:SignResponse>
```

Respuesta nativa:

```
<mensajeSalida>
    <peticion>FirmaServidor</peticion>
    <versionMsg>1.0</versionMsg>
    <respuesta>
        <Respuesta>
            <estado>true</estado>
            <descripcion>
      Proceso de generación de firma en servidor
realizado correctamente.
            </descripcion>
            <idTransaccion>
                1340100597551030
            </idTransaccion>
            <firmaElectronica>
                <![CDATA[MIIH6wYJKo...]]>
            </firmaElectronica>
            <formatoFirma>CMS</formatoFirma>
        </Respuesta>
    </respuesta>
</mensajeSalida>
```

OASIS-DSS (servicios DSS)

DSSAfirmaVerify - Validación y actualización de firma

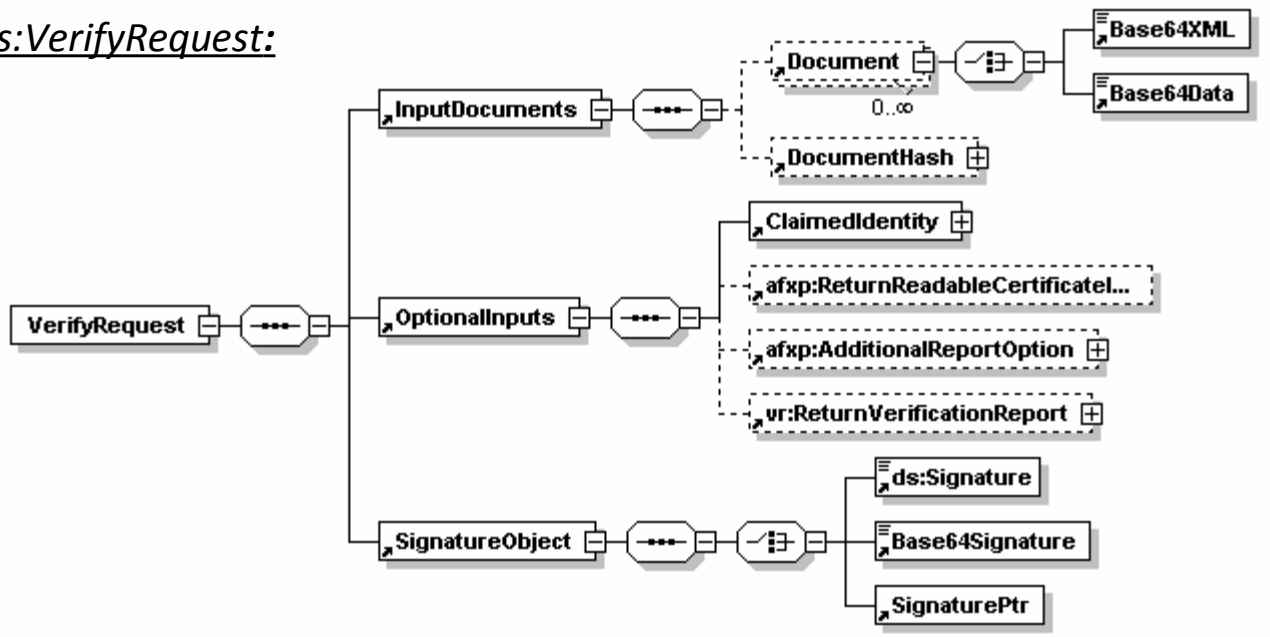
Validación de firmas electrónicas en los formatos admitidos por el sistema. Para la validación existen distintos niveles de validación (dependiendo del nivel se enviarán unos datos u otros):

- *Validación de firma electrónica.*
- *Validación de firma electrónica y el fichero firmado.*
- *Validación de firma electrónica y el hash del fichero firmado.*
- *Validación de firma electrónica, fichero firmado y su hash.*

Los elementos definidos en OASIS para este propósito son:

- dss:VerifyRequest.
- dss:VerifyResponse.

dss:VerifyRequest:



OASIS-DSS (servicios DSS)

DSSAfirmaVerify vs ValidarFirma (Petición)

Petición DSS:

```
<dss:VerifyRequest>
    <dss:InputDocuments>
        <dss:Document>
            <dss:Base64Data>
                <![CDATA[cHJ1ZWJhLnR4dA==]]>
            </dss:Base64Data>
        </dss:Document>
    </dss:InputDocuments>
    <dss:OptionalInputs>
        <dss:ClaimedIdentity>
            <dss:Name>STERIA_TEST</dss:Name>
        </dss:ClaimedIdentity>
        <vr:ReturnVerificationReport>
            <vr:ReportOptions>
                <vr:IncludeCertificateValues>
                    false
                </vr:IncludeCertificateValues>
                <vr:ReportDetailLevel>
                urn:oasis:names:tc:dss:1.0:reportdetail:noDetails
                </vr:ReportDetailLevel>
            </vr:ReportOptions>
        </vr:ReturnVerificationReport>
    </dss:OptionalInputs>
    <dss:SignatureObject>
        <dss:Base64Signature><![CDATA[MIIKhwYJKoZIhv...
            +iag3Ku74iVpXCTJBZfCEOJo3h04Ls=]]>
        </dss:Base64Signature>
    </dss:SignatureObject>
</dss:VerifyRequest>
```

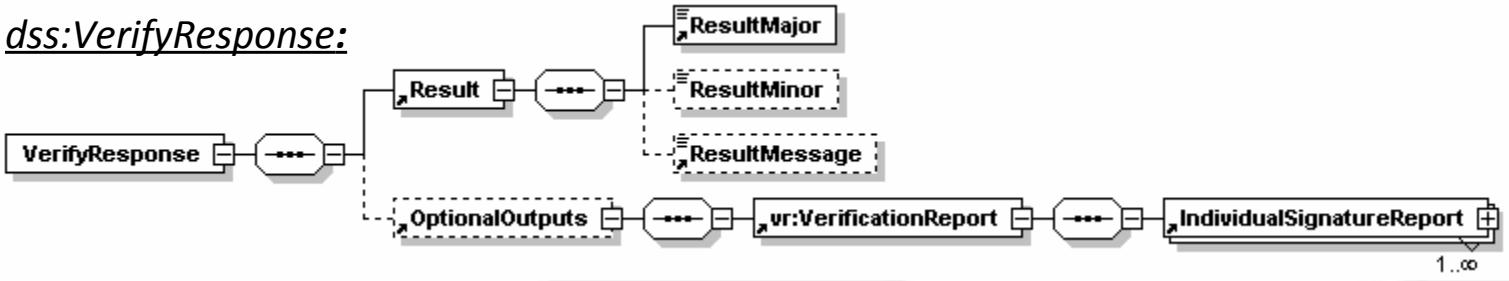
Petición nativa :

```
<mensajeEntrada>
    <peticion>ValidarFirma</peticion>
    <versionMsg>1.0</versionMsg>
    <parametros>
        <idAplicacion>STERIA_TEST</idAplicacion>
        <firmaElectronica>
            <![CDATA[MIIKhwYJKoZIhv...
            +iag3Ku74iVpXCTJBZfCEOJo3h04Ls=]]>
        </firmaElectronica>
        <formatoFirma>CADES</formatoFirma>
        <hash />
        <algoritmoHash />
        <datos>
            <![CDATA[cHJ1ZWJhLnR4dA==]]>
        </datos>
    </parametros>
</mensajeEntrada>
```

OASIS-DSS (servicios DSS)

DSSAfirmaVerify (Respuesta)

dss:VerifyResponse:



OASIS-DSS (servicios DSS)

DSSAfirmaVerify vs ValidarFirma (Respuesta)

Respuesta DSS:

```
<dss:VerifyResponse>
    <dss:Result>
        <dss:ResultMajor>
        urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature
        </dss:ResultMajor>
        <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:DigestMethod>
                        <ds:DigestValue>
                        <![CDATA[udEI2RCxZmLfJQSI1Oof8LQUO4A=]]>
                        </ds:DigestValue>
                    </vr:DigestAlgAndValue>
                </vr:SignatureIdentifier>
                <dss:Result>
                    <dss:ResultMajor>
            urn:afirma:dss:1.0:profile:XSS:resultmajor:ValidSignature
                    </dss:ResultMajor>
                    <dss:ResultMessage xml:lang="es">
                        La firma es valida
                    </dss:ResultMessage>
                </dss:Result>
            </vr:IndividualSignatureReport>
        </vr:VerificationReport>
    </dss:OptionalOutputs>
</dss:VerifyResponse>
```

Respuesta nativa:

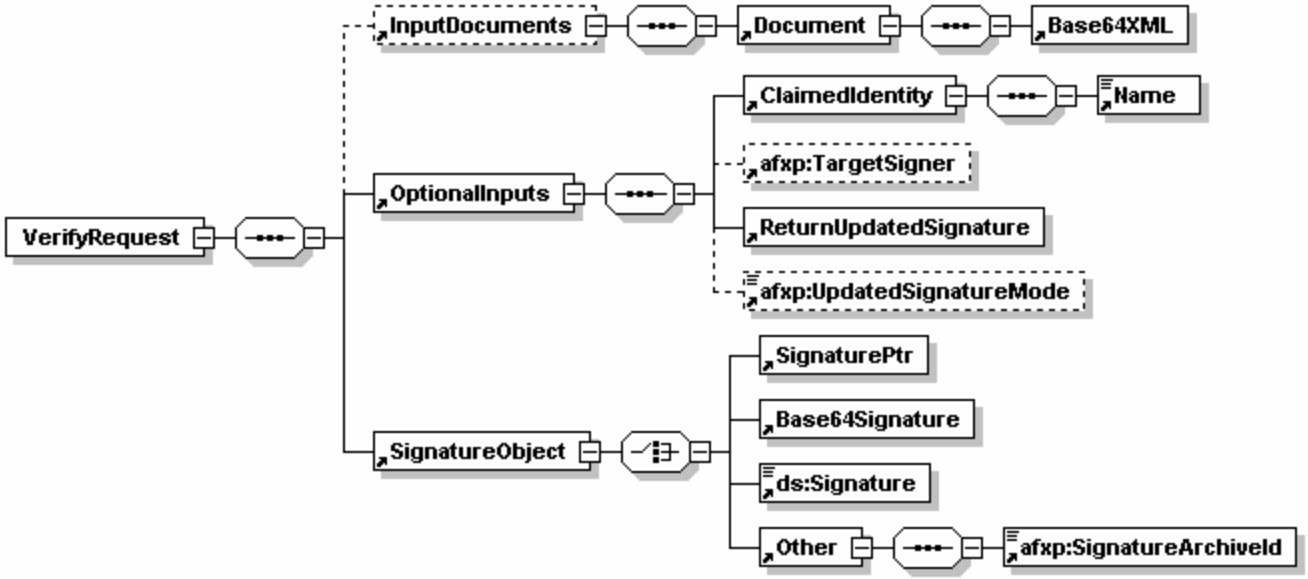
```
<mensajeSalida>
    <peticion>ValidarFirma</peticion>
    <versionMsg>1.0</versionMsg>
    <respuesta>
        <Respuesta>
            <estado>true</estado>
            <descripcion>
                <validacionFirmaElectronica>
                    <proceso>
                    Proceso de verificación de Firma Electrónica
                        completo
                    </proceso>
                    <detalle>Firma Digital correcta |
                        Firma Electrónica correcta |
                        Los certificados contenidos en la Firma
                        Electrónica sonválidos (integridad,
                        periodo de validez, estado de
                        revocación)
                    </detalle>
                    <conclusion>
                        Firma Electrónica correcta
                    </conclusion>
                </validacionFirmaElectronica>
            </descripcion>
        </Respuesta>
    </respuesta>
</mensajeSalida>
```

OASIS-DSS (servicios DSS)

DSSAfirmaVerify - Actualización de firma (Petición)

Actualización o upgrade de firmas electrónicas a un formato más avanzado (por ejemplo para la inclusión del sello de tiempo). Los pares de mensajes son los mismos que para la verificación, pero la inclusión de un elementos como dss:ReturnUpdatedSignature indicará al sistema que lo que se desea es una actualización de firma.

dss:VerifyRequest:



OASIS-DSS (servicios DSS)

DSSAfirmaVerify - Actualización de firma (Petición)

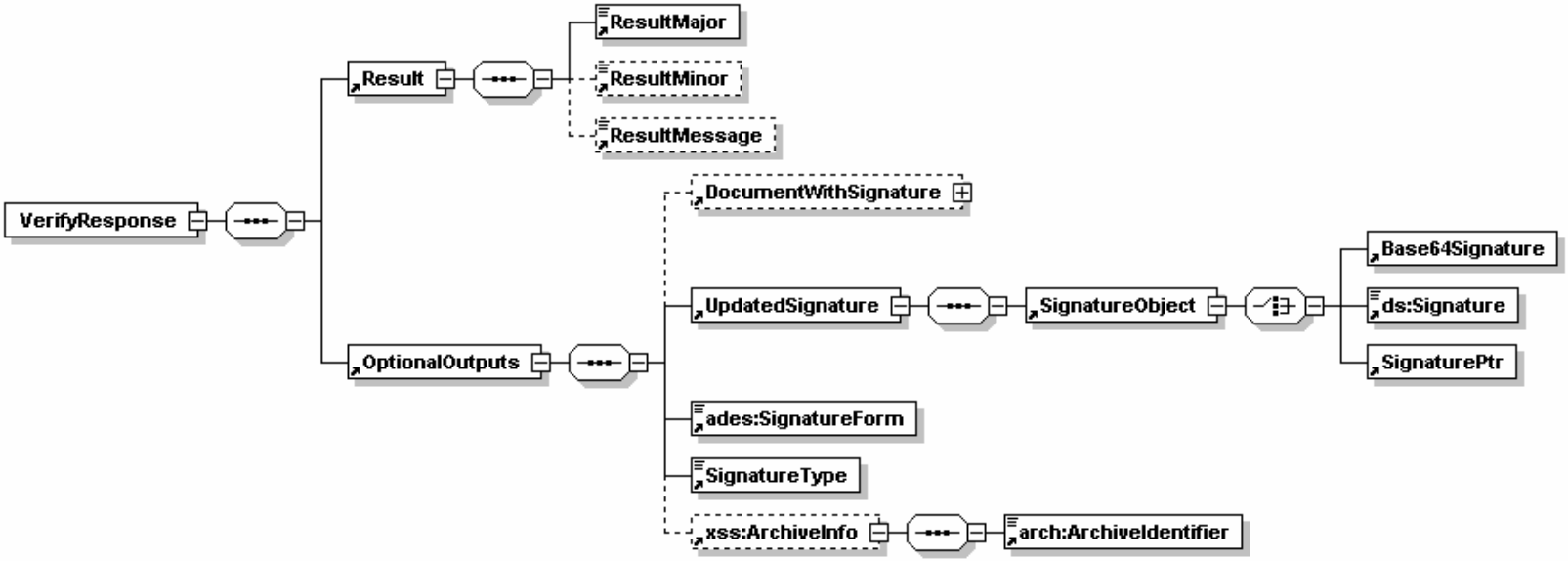
Petición dss:

```
<dss:VerifyRequest Profile="urn:afirma:dss:1.0:profile:XSS">
    <dss:OptionalInputs>
        <dss:ClaimedIdentity>
            <dss:Name>STERIA_TEST</dss:Name>
        </dss:ClaimedIdentity>
        <dss:ReturnUpdatedSignature
            Type="urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T" />
    </dss:OptionalInputs>
    <dss:SignatureObject>
        <dss:Base64Signature><![CDATA[MIIKhwYJKo...
        EmTmkm655ywUUOIMts+3QXLnj3rbwGK
        O+Q8tgWgghh+iag3Ku74iVpXCTJBZfCEOJo3h04Ls=]]>
        </dss:Base64Signature>
    </dss:SignatureObject>
</dss:VerifyRequest>
```

OASIS-DSS (servicios DSS)

DSSAfirmaVerify - Actualización de firma (Respuesta)

dss:VerifyResponse:



OASIS-DSS (servicios DSS)

DSSAfirmaVerify - Actualización de firma (Respuesta)

Respuesta dss:

```
<dss:VerifyResponse Profile="urn:afirma:dss:1.0:profile:XSS">
    <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[MIIQYJKoZIhvcNAQcCoIIQBjCCE...
                    OrnCJoI9wWvntSFerkolRO5sP4c9+xB0k4=]]>
                </dss:Base64Signature>
            </dss:SignatureObject>
        </dss:UpdatedSignature>
        <xss:ArchiveInfo>
            <arch:ArchiveIdentifier>
                1340269416581074
            </arch:ArchiveIdentifier>
        </xss:ArchiveInfo>
        <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>
```

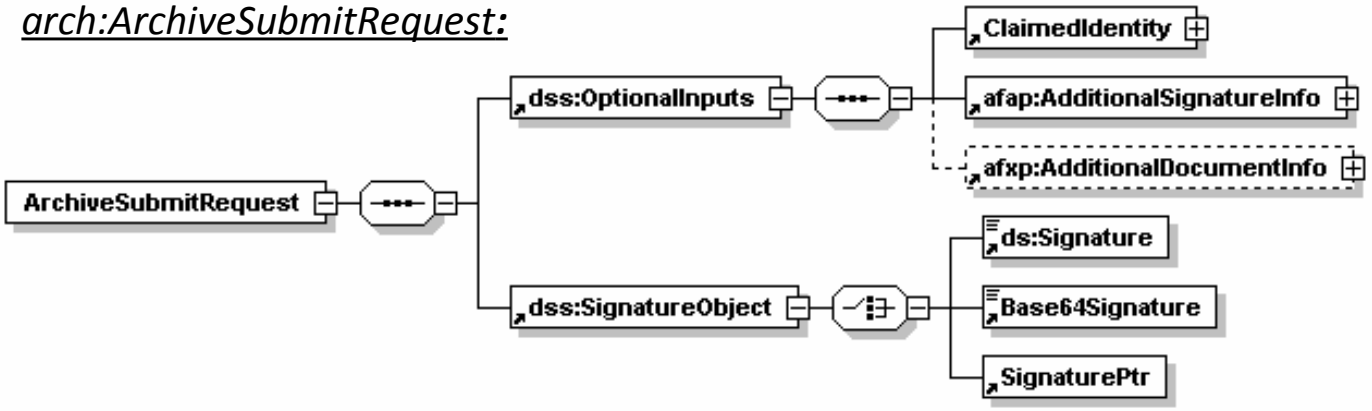
OASIS-DSS (servicios DSS)

DSSAfirmaArchiveSubmit - Registro de firma

Permite el registro o custodia en el sistema, de firmas realizadas externamente. El perfil de OASIS define los siguientes mensajes:

- arch:ArchiveSubmitRequest.
- arch:ArchiveSubmitResponse.

arch:ArchiveSubmitRequest:



OASIS-DSS (servicios DSS)

DSSAfirmaArchiveSubmit vs FirmaUsuario2FasesF2 (Petición)

Petición dss:

```
<arch:ArchiveSubmitRequest>
    <dss:OptionalInputs>
        <dss:ClaimedIdentity>
            <dss:Name>STERIA_TEST</dss:Name>
        </dss:ClaimedIdentity>
        <afap:AdditionalSignatureInfo>
            <ds:X509Data>
                <ds:X509Certificate><![CDATA[MIIFTDC...
                    yXeqlVRsWQp5e/anZHTWnaMnEb+7XQ==]]>
                </ds:X509Certificate>
            </ds:X509Data>
        </afap:AdditionalSignatureInfo>
    </dss:OptionalInputs>
    <dss:SignatureObject>
        <dss:Base64Signature><![CDATA[MIIG4AYJKoZ...
        Go2wdBtb8bgLMt5IdZZRGu4hGqjhCYmsKzy3+zSNafFN1Uq]]>
        </dss:Base64Signature>
    </dss:SignatureObject>
</arch:ArchiveSubmitRequest>
```

Petición nativa:

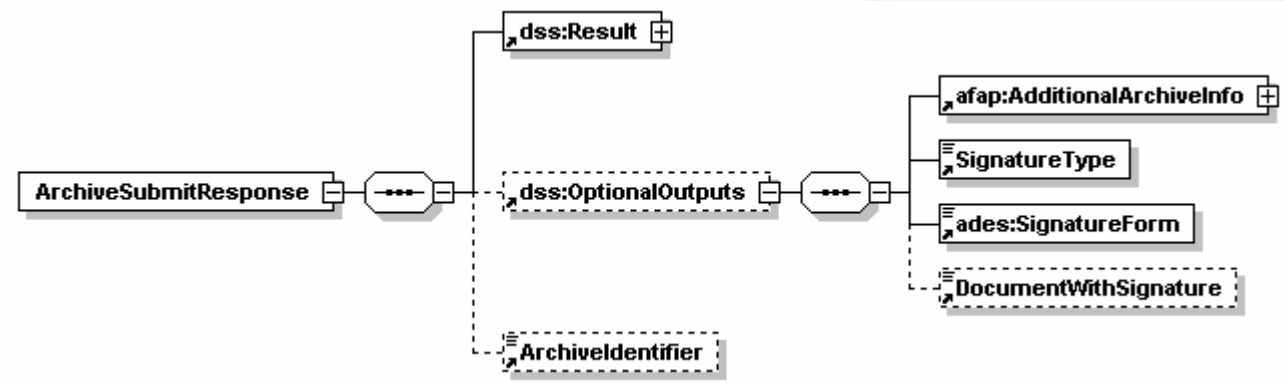
```
<?xml version="1.0" encoding="UTF-8"?>
<mensajeEntrada>
    <peticion>FirmaUsuario2FasesF2</peticion>
    <versionMsg>1.0</versionMsg>
    <parametros>
        <idAplicacion>STERIA_TEST</idAplicacion>
        <firmaElectronica>
            <![CDATA[MIIG4AYJKoZ...

Go2wdBtb8bgLMt5IdZZRGu4hGqjhCYmsKzy3+zSNafFN1Uq]]>
        </firmaElectronica>
        <certificadoFirmante>
            <![CDATA[MIIFTDC...
            yXeqlVRsWQp5e/anZHTWnaMnEb+7XQ==]]>
            </certificadoFirmante>
        <idReferencia />
        <formatoFirma><![CDATA[CMS]]></formatoFirma>
        <algoritmoHash>SHA1</algoritmoHash>
    </parametros>
</mensajeEntrada>
```

OASIS-DSS (servicios DSS)

DSSAfirmaArchiveSubmit - Registro de firma (Respuesta)

arch:ArchiveSubmitResponse:



OASIS-DSS (servicios DSS)

DSSAfirmaArchiveSubmit vs FirmaUsuario2FasesF2 (Respuesta)

Respuesta dss:

```
<?xml version="1.0" encoding="UTF-8"?>
<arch:ArchiveSubmitResponse>
    <dss:Result>
        <dss:ResultMajor>
            urn:oasis:names:tc:dss:1.0:resultmajor:Success
        </dss:ResultMajor>
        <dss:ResultMessage xml:lang="es">
            Proceso de fase 2 de firma de usuario en 2 fases
            realizado correctamente.  Justificante [CADES-T] –
            Firma Usuario [CMS]
        </dss:ResultMessage>
    </dss:Result>
    <dss:OptionalOutputs>
        <afap:AdditionalArchiveInfo>
            <afap:EvidenceOfESignature>
                <dss:SignatureObject>
                    <dss:Base64Signature>
                        <![CDATA[MIIQ4AYJKoZ…
                        Ym2rvP+yukJ6IcnPQ1PM381w==]]>
                    </dss:Base64Signature>
                </dss:SignatureObject>
                <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>
            </afap:EvidenceOfESignature>
        </afap:AdditionalArchiveInfo>
        <dss:SignatureType>
            urn:ietf:rfc:3369
        </dss:SignatureType>
    </dss:OptionalOutputs>
    <arch:ArchiveIdentifier>1340345037383004</arch:ArchiveIdentifier>
</arch:ArchiveSubmitResponse>
```

Respuesta nativa:

```
<?xml version="1.0"?>
<mensajeSalida xmlns="https://afirmaws/ws/firma"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="https://afirmaws/ws/firma
https://10.90.29.30/afirmaws/xsd/mfirma/ws.xsd ">
    <peticion>FirmaUsuario2FasesF2</peticion>
    <versionMsg>1.0</versionMsg>
    <respuesta>
        <Respuesta>
            <estado>true</estado>
            <descripcion>Proceso de fase 2 de firma de usuario en 2 fases
                realizado correctamente. Justificante [CADES-T] –
                Firma Usuario  [CMS-T]
            </descripcion>
            <idTransaccion>1340346930982041</idTransaccion>
            <justificanteFirmaElectronica><![CDATA[MIIQ4AYJKoZ…
                5zItPk3Xm9PriBYIKSceOPUOiGfhRoLXuTb+42SBpg==]]>
            </justificanteFirmaElectronica>
        </Respuesta>
    </respuesta>
</mensajeSalida>
```

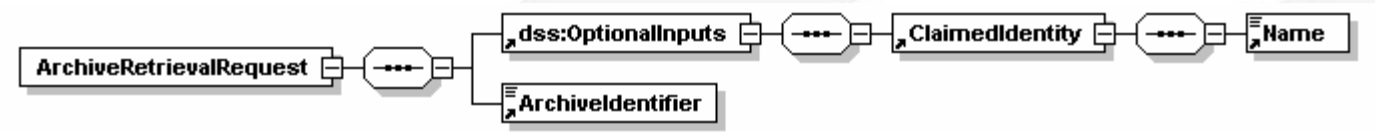
OASIS-DSS (servicios DSS)

DSSAfirmaArchiveRetrieval - Obtención de firma

El cliente incluye en la petición el identificador de transacción de la firma a recuperar y obtiene una respuesta con el resultado del proceso y la firma asociada. OASIS define la siguiente pareja de mensajes:

- arch:ArchiveRetrievalRequest.
- arch:ArchiveRetrievalResponse.

arch:ArchiveSubmitRequest:



OASIS-DSS (servicios DSS)

DSSAfirmaArchiveRetrieval vs ObtenerFirmaTransaccion (Petición)

Petición DSS:

```
<?xml version="1.0" encoding="UTF-8"?>
<arch:ArchiveRetrievalRequest
      Profile="urn:afirma:dss:1.0:profile:archive">
      <dss:OptionalInputs>
            <dss:ClaimedIdentity>
                  <dss:Name>STERIA_TEST</dss:Name>
            </dss:ClaimedIdentity>
      </dss:OptionalInputs>
      <arch:ArchiveIdentifier>
            1340346930982017
      </arch:ArchiveIdentifier>
</arch:ArchiveRetrievalRequest>
```

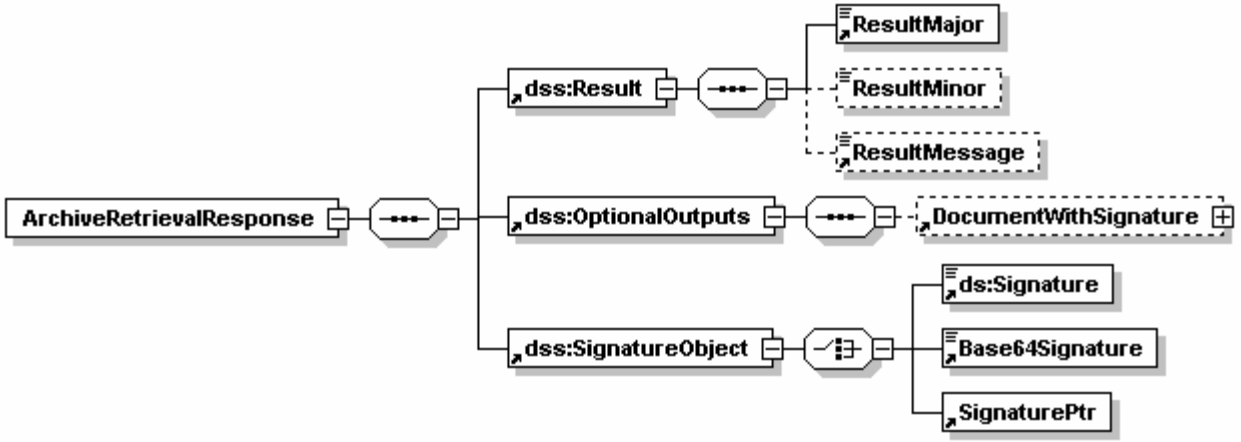
Petición nativa:

```
<?xml version="1.0" encoding="UTF-8"?>
<mensajeEntrada>
      <peticion>ObtenerFirmaTransaccion</peticion>
      <versionMsg>1.0</versionMsg>
      <parametros>
            <idAplicacion>STERIA_TEST</idAplicacion>
            <idTransaccion>
                  1340346930982017
            </idTransaccion>
      </parametros>
</mensajeEntrada>
```

OASIS-DSS (servicios DSS)

DSSAfirmaArchiveRetrieval (Respuesta)

arch:ArchiveSubmitResponse:



OASIS-DSS (servicios DSS)

DSSAfirmaArchiveRetrieval vs ObtenerFirmaTransaccion (Respuesta)

Respuesta DSS:

```
<?xml version="1.0" encoding="UTF-8"?>
<arch:ArchiveRetrievalResponse
      Profile="urn:afirma:dss:1.0:profile:archive">
      <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 FirmaElectrónica
                  realizado correctamente.
            </dss:ResultMessage>
      </dss:Result>
      <dss:SignatureObject>
            <dss:Base64Signature>
                  <![CDATA[MIIMbgYJKoZIhvcNAQcCoI...
                  6cXTZ/SHlGwJy1f0A4mJGCfl3Im1EQMVX2O]]>
            </dss:Base64Signature>
      </dss:SignatureObject>
</arch:ArchiveRetrievalResponse>
```

Respuesta nativa:

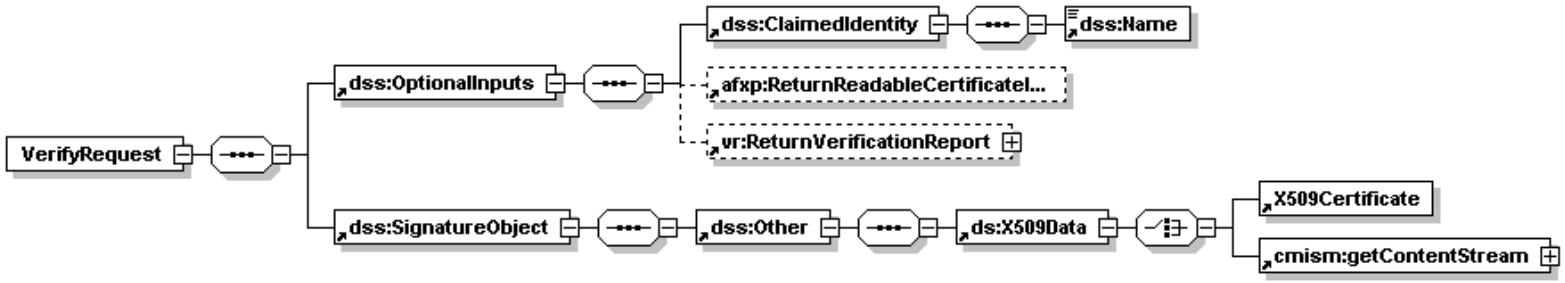
```
<?xml version="1.0"?>
<mensajeSalida>
      <peticion>ObtenerFirmaTransaccion</peticion>
      <versionMsg>1.0</versionMsg>
      <respuesta>
            <Respuesta>
                  <estado>true</estado>
                  <descripcion>
                        Proceso de obtención de la FirmaElectrónica
                        realizado correctamente.
                  </descripcion>
                  <firmaElectronica>
                        <![CDATA[MIIMbgYJKoZIhvcNAQcCoI...
                  6cXTZ/SHlGwJy1f0A4mJGCfl3Im1EQMVX2O]]>
                  </firmaElectronica>
                  <formatoFirma>CMS-T</formatoFirma>
            </Respuesta>
      </respuesta>
</mensajeSalida>
```

OASIS-DSS (servicios DSS)

DSSAfirmaVerifyCertificate - Validación de certificado

Permite la verificación de certificados X509 finales. 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.
La petición de validación de certificado similar a la de validación de firma.

dss:VerifyRequest:



OASIS-DSS (servicios DSS)

DSSAfirmaVerifyCertificate vs ValidarCertificado (Petición)

Petición dss:

```
<?xml version="1.0" encoding="UTF-8"?>
<dss:VerifyRequest>
    <dss:OptionalInputs>
        <dss:ClaimedIdentity>
            <dss:Name>STERIA_TEST</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:ReportDetailLevel>
            </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>
```

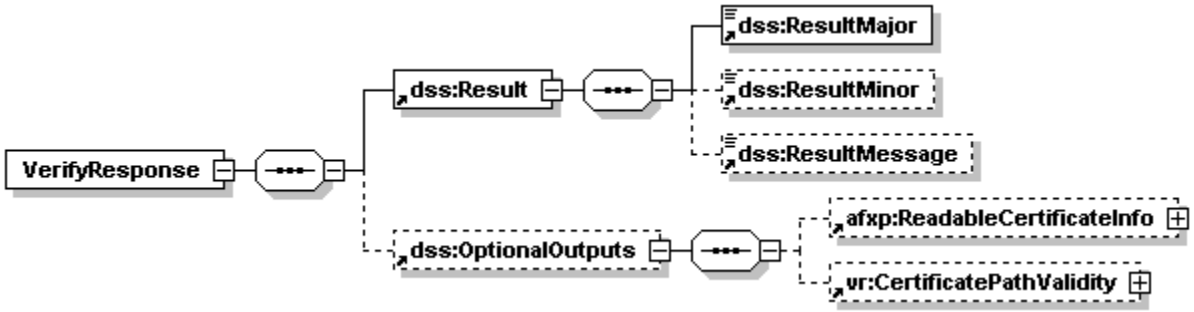
Petición nativa:

```
<?xml version="1.0" encoding=" UTF-8"?>
<mensajeEntrada>
    <peticion>ValidarCertificado</peticion>
    <versionMsg>1.0</versionMsg>
    <parametros>
        <certificado>
            <![CDATA[MIIDP….]]>
        </certificado>
        <idAplicacion>STERIA_TEST</idAplicacion>
        <modoValidacion>1</modoValidacion>
        <obtenerInfo>true</obtenerInfo>
    </parametros>
</mensajeEntrada>
```

OASIS-DSS (servicios DSS)

DSSAfirmaVerifyCertificate (Respuesta)

dss:VerifyResponse:



OASIS-DSS (servicios DSS)

DSSAfirmaVerifyCertificate vs ValidarCertificado (Respuesta)

Respuesta dss:

```
<?xml version="1.0" encoding="UTF-8"?>
<dss:VerifyResponse>
    <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:OptionalOutputs>
        <afxp:ReadableCertificateInfo>
            ...
        </afxp:ReadableCertificateInfo>
        <vr:CertificatePathValidity>
            ...
        </vr:CertificatePathValidity>
    </dss:OptionalOutputs>
</dss:VerifyResponse>
```

```
<mensajeSalida>
    <peticion>ValidarCertificado</peticion>
    <versionMsg>1.0</versionMsg>
    <respuesta>
        <ResultadoProcesamiento>
            <InfoCertificado>
                <Campo>
                    <idCampo>usoCertificado</idCampo>
                    <valorCampo>
                        digitalSignature | nonRepudiation
                    </valorCampo>
                </Campo>
                ...
            </InfoCertificado>
            <ResultadoValidacion>
                <resultado>0</resultado>
                <descripcion>
                    Validacion Satisfactoria
                </descripcion>
                <ValidacionSimple>
                    <codigoResultado>0</codigoResultado>
                    <descResultado>
                        Validacion Satisfactoria
                    </descResultado>
                </ValidacionSimple>
            </ResultadoValidacion>
        </ResultadoProcesamiento>
    </respuesta>
</mensajeSalida>
```

OASIS-DSS (servicios DSS)

Validación de firmas y certificados masivas (asíncronas)

Mediante estos servicios se puede solicitar la validación de múltiples firmas o certificados con una sola petición.

Estas peticiones serán procesadas de manera asíncrona por el servidor, el cual generará una respuesta del tipo «pendiente de procesado».

- DSSBatchVerifyCertificate
- DSSBatchVerifySignature

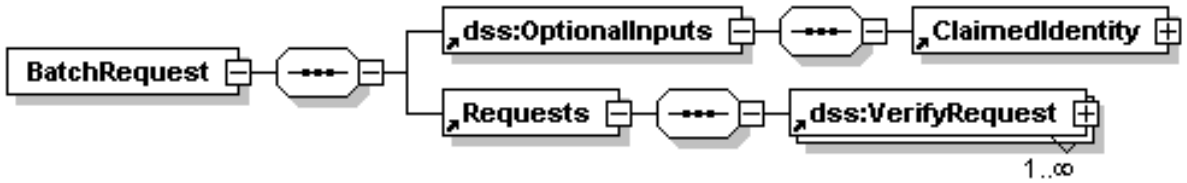
Posteriormente se podrá solicitar al servidor, utilizando el identificador de petición (recibido en la respuesta de la solicitud de verificación) junto al identificador de aplicación, el estado de la petición mediante los mensajes:

- async:PendingRequest
- afxp:BatchResponse

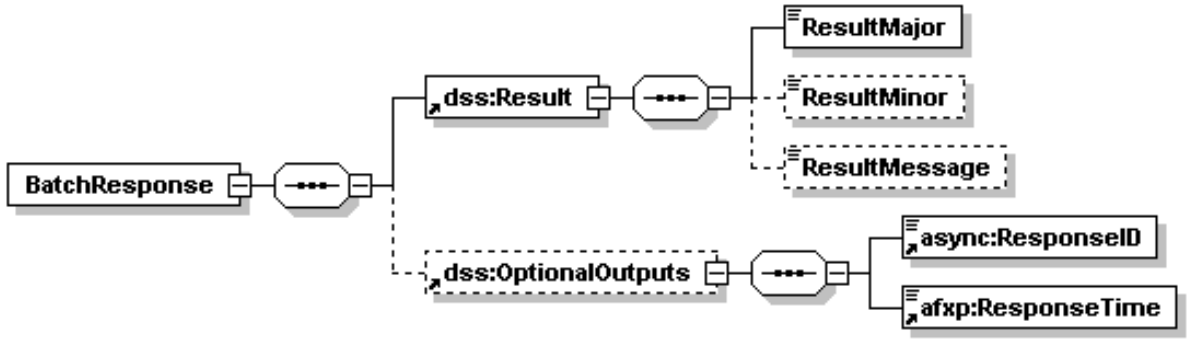
OASIS-DSS (servicios DSS)

Validaciones masivas (Petición)

BatchVerify:



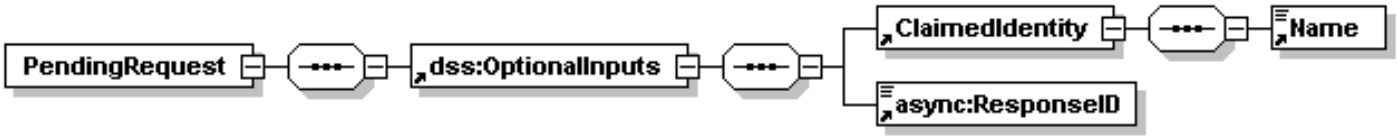
BatchResponse:



OASIS-DSS (servicios DSS)

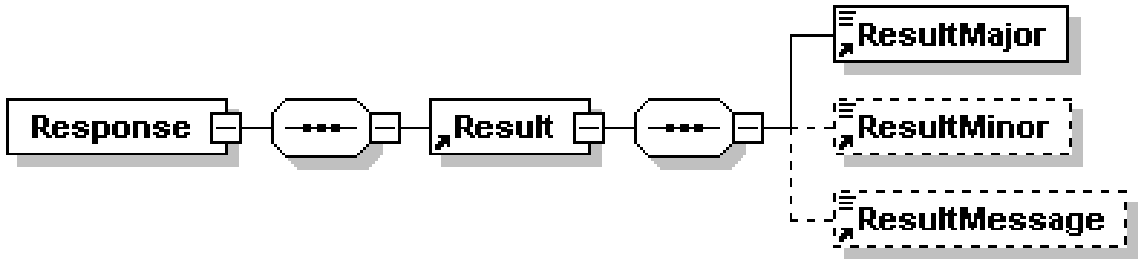
Validaciones masivas (consulta de estado y respuesta)

async:PendingRequest:



Respuesta:

- 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.
- 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.



Muchas gracias

Dirección General de Política Digital

Consejería de Hacienda y Administración Pública