Manual de Programación de Web Services de @firma 6

Documento nº:	@Firma-Global-XMLSOAP-MAN-EN
Revisión:	060
Fecha:	17-07-2019
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

CONTROL DE MODIFICACIONES

Documento nº:	@Firma-Global-XMLSOAP-MAN-EN
Revisión:	060
Fecha:	17-07-2019

Rev.	001
Fecha	09-12-2005
Descripción	Documentación inicial.

Rev.	002
Fecha	19-12-2005
Descripción	Se han añadido al documento los anexos correspondientes a la descripción de códigos de resultado devueltos por la plataforma y a un ejemplo de integración de la plataforma haciendo uso de los Web Services. Se ha actualizado el xsd de solicitud y respuesta. Se ha actualizado el wsdl de los servicios web ValidarCertificado y ObtenerInfoCertificado.

Rev.	003
Fecha	10-01-2006
Descripción	Actualización de los WSDL y mensajes SOAP de los servicios web.

Rev.	004
Fecha	26-01-2006
Descripción	Actualización de los xml de salida y esquemas para soportar certificados de persona jurídica y e-DNI.

Rev.	005
Fecha	6-02-2006
Descripción	Actualización del mensaje SOAP de respuesta error para el WS ObtenerInfoCertificado. Añadido la descripción para el WS ValidarFirma. Añadida información de integración vía OCSP Responder. Actualización de los Namespaces de los documentos xml de entrada, salida y schemas de todos los WS.

Rev.	006
Fecha	7-02-2006
Descripción	Actualización los mensajes SOAP de respuesta ya que se devuelven firmados.

Rev.	007
Fecha	10-02-2006
Descripción	Adición de códigos de validación devueltos por la plataforma.

Rev.	008
Fecha	21-02-2006
Descripción	Actualización de la codificación de las peticiones SOAP y mensajes de entrada de la plataforma a ISO-8859-1. Actualizados el puerto de acceso al OCSPResponder y protocolos de acceso a la plataforma vía WS.

Rev.	009
Fecha	24-02-2006
Descripción	Corrección del dominio redinteradministrativa.

Rev.	010
Fecha	27-02-2006
Descripción	Actualización de los puertos por el cual realizar una petición OCSP Responder y WS (usando el protocolo http).

Rev.	011
Fecha	02-03-2006
Descripción	Actualización de la codificación de las peticiones SOAP y mensajes de entrada de la plataforma a UTF-8.

Rev.	012
Fecha	18-04-2006
Descripción	Actualización del XSchema de los servicios web de Validación para indicar que los elementos fechaRevocacion y motivo de InfoMetofoVerificacion pueden no aparecer en el resultado del servicio web de validación correspondiente.

Rev.	013
Fecha	08-06-2006
Descripción	Adición del código de validación “clasificacion” devuelto por la plataforma y de los valores que puede tomar.

Rev.	014
Fecha	09-06-2006
Descripción	Actualizados los valores que puede tomar el código de validación “clasificación”.

Rev.	014.1
Fecha	19-06-2006
Descripción	Adición del campo numeroSerie en el certificado patrón.

Rev.	014.2
Fecha	21-06-2006
Descripción	Revisión del campo ‘clasificación’ a valores iguales al de la DPC.

Rev.	015
Fecha	22-06-2006
Descripción	Actualización de los mensajes SOAP de respuesta firmados. Actualización del Servicio Web ValidarFirma. Adición de los Servicios Web del Módulo de Firma y de Custodia. Actualización del XSchema para los Servicios Web del Módulo de Firma. Inclusión del XSChema para los Servicios Web del módulo de Custodia.

Rev.	015.1
Fecha	06-07-2006
Descripción	Posibilidad de realizar en una única petición OCSP la validación de varios certificados.

Rev.	016
Fecha	26-07-2006
Descripción	Nivel de securización de peticiones XMLSOAP a la plataforma. Actualización de los WS del módulo de firma. Adición de nuevos WS en el módulo de firma. Actualización de los WS del módulo de custodia. Adición de nuevos WS en el módulo de custodia. Actualización de los XSchemas del módulo de firma y custodia. Adición de nuevos códigos de error devueltos por la plataforma.

Rev.	017
Fecha	19-09-2006
Descripción	Actualización del WS de Firma por Bloques para contemplar la nueva funcionalidad de multifirma selectiva de documentos en bloques. Adición del nuevo WS *obtenerInfoCompletaBloqueFirmas*. Actualización del XSchemas del módulo de firma.

Rev.	017.3
Fecha	20-12-2006
Descripción	Descripcion de los servicios web publicados en inglés. Modificados WSDLs, XMLs y XSDs. Adaptación del ejemplo *TestClient* a los servicios en ingles. Se incorpora el campo 'tokenOCSP' en la información de los métodos de validación OCSP utilizados para la validación del estado de revocación de los certificados en el servicio web *ValidarCertificado*.

Rev.	017.4
Fecha	05-06-2007
Descripción	Se modifica el esquema del servicio ValidarCertificado. El elemento fechaUltimaActualizacion pasa a ser opcional. Se modifica el servicio ValidarFirma. El campo *certificado* de las respuestas se modifica y pasa a devolverse el certificado en Base64 en lugar de una cadena de caracteres con información no parseable.

Rev.	017.5
Fecha	06-08-2007
Descripción	Se ha modificado la descripción del codigo de resultado 4 del proceso de validación de certificados.

Rev.	018
Fecha	28-01-2008
Descripción	Se ha añadido las descripciones de los servicios Web implementado siguiendo las recomendaciones de OASIS – DSS.

Rev.	018.1
Fecha	08-02-2008
Descripción	Se ha añadido elemento TargetSigner al servicio de Firma de Servidor mediante interfaz DSS. Este elemento se encuentra definido en el Schema XSS de @Firma.

Rev.	018.2
Fecha	28-03-2008
Descripción	Se cambian los WSDL y Xshemas por las referencias correspondientes.

Rev.	018.2
Fecha	28-03-2008
Descripción	Se cambian los WSDL y Xshemas por las referencias correspondientes.

Rev.	018.3
Fecha	08-04-2008
Descripción	Se ha actualizado la siguiente información correspondiente a los servicios DSS: - Creación de firmas XML en distintos modos (Enveloping, Enveloped y Detached). - Actualización de firmas generadas mediante el servicio de verificación. - Nuevos códigos de error e identificadores.

Rev.	018.4
Fecha	24-06-2008
Descripción	Se ha incluido elemento “dss:IncludeEContent” en las peticiones de firma de servidor mediante interfaz DSS.

Rev.	018.5
Fecha	30-06-2008
Descripción	Se han incluido los siguientes cambios: - Añadido campo “documento” al mensaje de entrada e “idDocumento” al mensaje de salida del servicio de Firma de Servidor. - URI’s para generación y verificación de firmas ODF y PDF. - Elementos “dss:SignatureType” y “ades:SignatureForm” en los mensajes de respuesta de firma. - Modificada URI de CADES a la versión 1.7.3.

Rev.	018.6
Fecha	06-03-2009
Descripción	Se añade una aclaración en el servicio Firma 2 Fases con respecto al parámetro custodiarDocumento.

Rev.	018.7
Fecha	20-04-2009
Descripción	Se añade una aclaración en el servicio Firma 2 FirmaServidor con respecto al certificado que se utiliza para firmar.

Rev.	019
Fecha	16-07-2009
Descripción	Se actualizan las referencias hacia el MAP por referencias hacia el MPR.

Rev.	020
Fecha	10-09-2009
Descripción	Se actualizan las referencias al entorno de Preproducción por referencias al Entorno de Desarrollo. Se modifica la referencia a la página principal por una referencia a la página del CTT.

Rev.	021
Fecha	22-09-2009
Descripción	Se actualizan las operaciones que constan de varias fases para indicar su futura discontinuación.

Rev.	022
Fecha	01-10-2009
Descripción	Se eliminan los apartados y anexos correspondientes a los Servicios DSS, la información relativas a las Interfaces DSS de la plataformas se trasladará al documento de Descripción de Perfiles DSS de @Firma.

Rev.	023
Fecha	07-04-2010
Descripción	Se adapta la revisión a la versión 5.4 de @firma. Se corrigen las referencias hacia MPR.

Rev.	024
Fecha	20-05-2010
Descripción	Se incluye una anotación en el apartado 4.3.2 para firmas PDF y ODF.

Rev.	025
Fecha	21-07-2010
Descripción	Se incluyen nuevos códigos de error al anexo A.2.

Rev.	026
Fecha	24-08-2010
Descripción	Se modifican referencias para adaptar a MPR.

Rev.	027
Fecha	03-11-2010
Descripción	Se añaden los distintos motivos de revocación en el método de validación de certificados.

Rev.	028
Fecha	23-12-2010
Descripción	Se actualizan las referencias de TI a TGS.

Rev.	029
Fecha	13/05/2011
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. Se añaden recomendaciones para la utilización de los servicios web de forma segura.

Rev.	030
Fecha	13/05/2011
Descripción	Se cambia el logotipo. Se cambian las referencias sa MPR por MPTAP. Se cambian las referencias al CTT por PAE. Se quitan las indicaciones de discontinuación de servicios.

Rev.	031
Fecha	18/05/2011
Descripción	Se crea el anexo A.4 para indicar lo valores de ciertos elementos de validación. Se crea el anexo A.5 que muestra como se puede obtener la versión de @firma contenida en un determinado servidor.

Rev.	032
Fecha	10/06/2011
Descripción	Se incluye en el apartado 4 una aclaración sobre el escapado de los mensajes.

Rev.	033
Fecha	07/09/2011
Descripción	Se renombra el fichero. Se incluyen en el Sevicio Validar Firma y FirmaServidor los formatos extendidos y una nota sobre la generación de firmas CADES-XL. Se actualizan los codigos de error y de validación.

Rev.	034
Fecha	20/09/2011
Descripción	Se indica que el elemento TokenOCSP de la respuesta del servicio ValidateCertificate devuelve un BasicOCSPResponse, y no un OCSPResponse.

Rev.	035
Fecha	21/09/2011
Descripción	Se actualizan las referencias a MPTAP (Ministerio de Política Territorial y Administraciones Públicas) por Gobierno de España. Se formatea adecuadamente el documento y se corrigen títulos. Se indican aquellos servicios que serán discontinuados.

Rev.	036
Fecha	28/11/2011
Descripción	Modificado el Servicio “Firma de Servidor” para permitir la realización de firma a partir del hash de un documento.

Rev.	037
Fecha	30/11/2011
Descripción	Se indica la posibilidad de indicar formato OOXML en servicios de validación.

Rev.	038
Fecha	07/12/2011
Descripción	Actualización de las referencias a la versión 5.5 por 5.6.

Rev.	039
Fecha	28/12/2011
Descripción	Se añaden como formatos de validación PAdES-Basic, PAdES-BES, PAdES-EPES y PAdES-LTV. Se indica que en la validación de una firma, si la firma posee formato PAdES-LTV y contiene al menos un diccionario de tipo Document Time-stamp, la información del sello de tiempo y del certificado de sello de tiempo hará referencia únicamente al sello de tiempo y al certificado de la autoridad emisora de sello de tiempo contenidos en el diccionario de tipo Document Time-stamp más reciente. Se actualizan los códigos de resultado devueltos por la plataforma. Se actualizan los códigos de error devueltos por la plataforma relativos a la actualización de firmas a PAdES-LTV.

Rev.	040
Fecha	09/01/2012
Descripción	Se actualizan los formatos de validación que admiten los servicios de validación y de generación de firmas. Se actualizan las siglas.

Rev.	041
Fecha	10/02/2012
Descripción	Se añade un comentario acerca del formato CMS en el servicio de Validación de firmas.

Rev.	042
Fecha	25/05/2012
Descripción	Se añade un código de error, COD_059 para hacer referencia al error producido al intentar rescatar una propiedad de la tabla PROPERTY de la Base de Datos.

Rev.	043
Fecha	28/06/2012
Descripción	Se añade un código de error, COD_186 para hacer referencia a los errores producidos por los objetos de configuración de la plataforma.

Rev.	044
Fecha	08/02/2013
Descripción	Actualizado al catálogo de servicios ofrecidos por @firma 6.

Rev.	045
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.	046
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.

Rev.	047
Fecha	31/05/2013
Descripción	Se añade una aclaración en el punto 5 con respecto al servicio OCSP de la plataforma.

Rev.	048
Fecha	03/06/2013
Descripción	Se actualiza el listado de códigos de error en el apartado A.2.2.

Rev.	049
Fecha	04/06/2013
Descripción	Actualización de la referencia al documento que indica la lista de los campos devueltos para cada tipo de certificado (apartado 4.2.3).

Rev.	050
Fecha	19/05/2014
Descripción	Se incluye una nota en cada uno de los servicios que ya no es proporcionado por la plataforma central.

Rev.	051
Fecha	15/01/2015
Descripción	Se indica explícitamente en el servicio nativo de validación de certificados que en caso de solicitar una validación del estado de revocación, si el certificado no pasa la validación simple (certificado caducado por ejemplo), el sistema no realizará una comprobación de su estado de revocación.

Rev.	052
Fecha	13/01/2016
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 añaden nuevos códigos de error. Se actualiza la descripción de qué formatos admiten co-firma y contra-firma.

Rev.	053
Fecha	03/08/2016
Descripción	Adaptación de plantillas de documentos

Rev.	054
Fecha	04/08/2016
Descripción	Se añade un comentario en el punto 4.4 (Módulo_Firma. Firma Servidor) indicando que, en el caso de firmas ASN.1, siempre se generarán explícitas, y en el caso de firmas XML, siempre se generarán detached. Se elimina del punto 4.4 (Módulo_Firma. Firma Servidor) la posibilidad de generar firmas AdES-EPES. Se añade un comentario en el punto 4.4 (Módulo_Firma. Firma Servidor) indicando que se permite la generación de formatos CMS-T, CAdES-C y XAdES-C.

Rev.	055
Fecha	28/04/2017
Descripción	Se actualiza el punto 4.5 para indicar que no se permite la co-firma en firmas CAdES-A ni 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 añaden y modifican según procede los comentarios que hacen referencia a los servicios “Legacy” (obsoletos), en proceso de discontinuación y solo disponibles en el modelo federado. Se indica el servicio DSS equivalente en caso de existir.

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	13/06/2019
Descripción	Se eliminan las referencias al Kit de integración (afirmaws.zip) en los diferentes apartados de los servicios integrados .

Rev.	060
Fecha	17/07/2019
Descripción	Se actualizan las referencias de donde obtener los certificados de confianza de las firmas de las respuestas SOAP y de las respuestas OCSP en los apartados 4 y 5 respectivamente.

CONTROL DE DISTRIBUCIÓN

Documento nº:	@Firma-Global-XMLSOAP-MAN-EN
Revisión:	060
Fecha:	17-07-2019

Propiedad del documento:

Este documento pertenece al Gobierno de España y posee un carácter de público para uso y distribución en ámbitos autorizados por este mismo, según se recoge en la declaración de privacidad.

Declaración de privacidad:

El contenido de este documento está sujeto al protocolo de libre distribución dentro del entorno definido para el contexto.

Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

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 22 de julio de 2019

ÍNDICE

1 Objeto 19

2 Alcance 19

3 Siglas 19

4 Descripción de Interfaces Web Services 22

4.1 Módulo_Validación. Validación de Certificado. 24

4.1.1 ValidateCertificate.wsdl 25

4.1.2 Mensaje SOAP de petición. 25

4.1.3 Mensaje SOAP de respuesta OK. 28

4.1.4 Mensaje SOAP de respuesta Error. 41

4.2 Módulo_Validacion. Obtención de Información de Certificado. 44

4.2.1 GetInfoCertificate.wsdl 44

4.2.2 Mensaje SOAP de petición. 45

4.2.3 Mensaje SOAP de respuesta OK. 46

4.2.4 Mensaje SOAP de respuesta Error. 53

4.3 Módulo_Firma. Validar Firmas. 56

4.3.1 SignatureValidation.wsdl 56

4.3.2 Mensaje SOAP de petición. 57

4.3.3 Mensaje SOAP de respuesta OK. 59

4.3.4 Mensaje SOAP de respuesta Error. 63

4.4 Módulo_Firma. Firma Servidor. 67

4.4.1 ServerSignature.wsdl 67

4.4.2 Mensaje SOAP de petición. 68

4.4.3 Mensaje SOAP de respuesta OK. 71

4.4.4 Mensaje SOAP de respuesta Error. 75

4.5 Módulo_Firma. Firma Servidor CoSign. 79

4.5.1 ServerSignatureCoSign.wsdl 79

4.5.2 Mensaje SOAP de petición. 79

4.5.3 Mensaje SOAP de respuesta OK. 81

4.5.4 Mensaje SOAP de respuesta Error. 85

4.6 Módulo_Firma. Firma Servidor CounterSign. 88

4.6.1 ServerSignatureCounterSign.wsdl 89
4.6.2 Mensaje SOAP de petición. 89
4.6.3 Mensaje SOAP de respuesta OK. 91
4.6.4 Mensaje SOAP de respuesta Error. 96
4.7 Módulo_Custodia. Almacenar Documento. 99
4.7.1 StoreDocument.wsdl 99
4.7.2 Mensaje SOAP de petición. 100
4.7.3 Mensaje SOAP de respuesta OK. 101
4.7.4 Mensaje SOAP de respuesta Error. 105
4.8 Módulo_Custodia. Eliminar Contenido Documento. 108
4.8.1 Mensaje SOAP de petición. 108
4.8.2 Mensaje SOAP de respuesta OK. 109
4.8.3 Mensaje SOAP de respuesta Error. 113
4.9 Módulo_Custodia. Obtener Contenido Documento. 116
4.9.1 Mensaje SOAP de petición. 116
4.9.2 Mensaje SOAP de respuesta OK. 117
4.9.3 Mensaje SOAP de respuesta Error. 121
4.10 Módulo_Custodia. Obtener Contenido Identificador de Documento. 125
4.10.1 Mensaje SOAP de petición. 125
4.10.2 Mensaje SOAP de respuesta OK. 126
4.10.3 Mensaje SOAP de respuesta Error. 129
4.11 Módulo_Custodia. Obtener Identificador Documento. 133
4.11.1 Mensaje SOAP de petición. 133
4.11.2 Mensaje SOAP de respuesta OK. 134
4.11.3 Mensaje SOAP de respuesta Error. 138
4.12 Módulo_Custodia. Obtener Firma Transacción. 141
4.12.1 Mensaje SOAP de petición. 141
4.12.2 Mensaje SOAP de respuesta OK. 142
4.12.3 Mensaje SOAP de respuesta Error. 147
5 Integración vía OCSP Responder 151
ANEXO 152
A.1 Sintaxis del XML de solicitud y respuesta 152
A.1.1 XSchema de web services para los WS de Validación 152

A.1.2 XSchema de web services para los WS de Firma 154
A.1.3 XSchema de web services para los WS de Custodia 155
A.1.4 XSchema del perfil XSS de @Firma 156
A.1.5 XSchema del perfil Archive de @Firma 158
A.2 Códigos de resultado devueltos por la plataforma 160
A.2.1 Códigos resultado. 160
A.2.2 Códigos de error. 161
A.3 Integración con la plataforma mediante de Web Services – WSS 167
A.4 Valores de elementos de validación 193
A.4.1 Elemento proceso 193
A.4.2 Elemento detalle 193
A.4.3 Elemento conclusión 194
A.5 Obtener versión de @firma 195
A.6 Guia 807 del Esquema Nacional de Seguridad (ENS). 195

1 Objeto

El objeto de este documento es describir las interfases WebServices de la plataforma @Firma 6 para que los desarrolladores de aplicaciones puedan integrar y utilizar los servicios ofrecidos por la misma.

2 Alcance

Este documento cubre los siguientes aspectos:

- Descripción de la interfaz de Servicios web de la plataforma @Firma mediante la especificación de mensajes XML-SOAP de solicitud y respuesta.
- XSchema general asociado al XML de los parámetros de entrada y salida de los servicios web.
- Descripción de los códigos de resultado devueltos por la plataforma.
- Ejemplo de integración con la plataforma a través de los Web Services.

3 Siglas

SOAP	Simple Object Access Protocol
WSDL	Web Service Description Language
WS	Web Services
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List
RFC	Request For Comments
XML	eXtensible Markup Language
XSD	XML Schema Definition
UTF-8	8-bit Unicode Transformation Format
HTTP	Hypertext Transfer Protocol Secure
MD	Message-Digest
SHA	Secure Hash Algorithm
TSA	TimeStamp Authority
TST	TimeStamp Token

BBDD	Base de Datos
XMLDSig	XML Digital Signature
XAdES	XML Advanced Electronic Signature
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
PKCS7	Public Key Infraestructure Standard #7
CMS	Cryptographic Message Syntax
CAdES	CMS Advanced Electronic Signature
CAdES-BES	CAdES - Basic Electronical Signature
CAdES-EPES	CAdES - Explicit Policy Electronical Signature
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
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
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 Descripción de Interfaces Web Services

La plataforma @firma 6 publicará servicios web de:

- Validación de certificados. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaVerifyCertificate**.

- Obtención de información de certificados. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaVerifyCertificate**.

- Validación de firma electrónica. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaVerify**.

- Firma Servidor. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaSign**.

- Firma Servidor CoSign. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaSign**.

- Firma Servidor CounterSign. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaSign**.

- Almacenar Documento. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**.

- Eliminar el Contenido de un Documento. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado**.

- Obtener Identificador de un Documento. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado**.

- Obtener el Contenido de un Documento. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado.**

- Obtener el Contenido de un Documento haciendo uso de su identificador. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado**.

- Obtener la Firma Electronica de una Transacción. Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado**.

El protocolo de acceso a dichos servicios se define mediante un mensaje de petición y otro de respuesta al mismo. Ambos mensajes se intercambian haciendo uso del protocolo XML-SOAP **siendo obligatorio que dicha petición sea realizada en codificación "UTF-8" vía http (por el puerto 8080) o https**.

Las peticiones XMLSOAP en función de la aplicación que realice la misma deberán estar[1]:

- Sin securizar.
- Securizadas haciendo uso de usuario/password
- Firmadas.

La plataforma devolverá los mensajes SOAP de respuesta firmados haciendo uso del certificado público de la misma. Para ello es necesario que se confíe en el certificado público suministrado en el "Área de Descargas" de la solución "Plataforma de validación de firma electrónica @firma" en el PAe (hay que identificarse como usuario):

https://administracionelectronica.gob.es/ctt/afirma/descargas → Documentación y Kit de certificados → Certificados utilizados por @firma.

Los servicios web publicados reciben como único parámetro de entrada un String con formato XML. Para cada servicio publicado existirá un formato de XML específico que vendrá definido por un XML Schema determinado.

[1] Ver Anexo A.3

Integración con la plataforma mediante de Web Services – WSS

En el anexo A.1 se definen los diferentes esquemas XML que definen los mensajes de petición y respuesta que se pasán como parámetro en la petición Web Service.

Debemos tener en cuenta que un mensaje SOAP básicamente es un documento XML, y tal y como hemos mencionado, los servicios web publicados por la plataforma reciben como único parámetro de entrada un String el cual también tiene formato XML. Por esta razón será necesario “escapar” el contenido de este parámetro, ya que los caracteres “<” y “>” contenidos en este mensaje en este caso no realizan la función como delimitadores de marcación dentro del SOAP, sino que son propios del parámetro. Para “escapar” los mensajes de entrada se utilizará para el símbolo de "mayor que" (>) la cadena ">", para el símbolo de "menor que" (<) la cadena "<" y para el caracter de ampersand (&) la cadena "&". Tambien se puede realizar el escapado mediante los delimitadores de secciones CDATA. Estos métodos de escapado están definidos en las especificaciones XML (Extensible Markup Language) desarrolladas por el World Wide Web Consortium.

Para los mensajes de salida se aplica el mismo método. La plataforma devuelve un mensaje SOAP con un único parámetro de tipo String con formato XML. En este caso, también la plataforma devuelve escapado el mensaje de salida.

Por razones de legibilidad, en todos los ejemplos utilizados en este manual los mensajes de entrada y salida de la plataforma no se muestran escapados. Para el correcto funcionamiento de los ejemplos se debe realizar el correspondiente “escapado”.

4.1 Módulo_Validación. Validación de Certificado.

Este servicio se considera “legacy” (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaVerifyCertificate**.

ValidarCertificado representa al servicio web encargado de validar un certificado X509, tanto tipos finales como entidades intermedias (siempre que sean reconocidos por la plataforma).

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.

4.1.1 ValidateCertificate.wsdl

El WSDL referente a este servicio se puede encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/services/ValidateCertificate?wsdl

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/services/ValidateCertificate?wsdl

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mvalidacion /wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mvalidacion /wseng.xsd

4.1.2 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

        <ValidateCertificate xmlns="http://soapinterop.org/">

        <ValidateCertificateRequest xsi:type="xsd:string" xmlns="">

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

            <inputMessage xmlns=”http://afirmaws/ws/validation”
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:SchemaLocation="
https://localhost/afirmaws/xsd/mvalidacion/wseng.xsd">

                <request>ValidateCertificate</request>
```

```
                        <versionMsg>1.0</versionMsg>
                        <parameters>
                            <certificate><![CDATA[contenido del certificado]]></certificate>
                            <applicationId>[idAplicacion]</applicationId>
                            <validationMode>[modo]</validationMode>
                            <getInfo>[obtenerInfo]</getInfo>
                        </parameters>
                    </inputMessage>
                </ValidteCertificateRequest>
                </ValidateCertificate>
</soapenv:Body>
</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- "Certificado": Contenido del certificado a validar codificado en Base 64.
- "idAplicacion": Identificador de la aplicación que realiza la petición.
- "modoValidacion": Su valor podrá ser:
    - 0, para una validación simple. Donde se validará la caducidad, integridad y confianza del certificado.
    - 1, para una validación intermedia. Donde se validará la misma información del caso 0 + estado de revocación.
    - 2, para una validación compleja. Donde se validará la misma información del caso 1 + validación de la cadena de confianza al completo.

    NOTA: Para los casos de utilizar los modos 1 o 2, si el tipo de certificado no es reconocido por la plataforma para la aplicación seleccionada, se tratará de realizar la verificación del

estado de revocación del certificado mediante la validación ligera de certificados, haciendo uso de las TSL disponibles.

NOTA: Para los casos de utilizar los modos 1 o 2, si el certificado a validar no pasa la validación simple (modo 0), el proceso no continúa, por lo que no se comprobaría el estado de revocación del certificado.

- "obtenerInfo": Su valor será un boolean que especifique si se desea extraer información del certificado a validar o no.

  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, la información mínima que se extrae del certificado es, concretamente los siguientes 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.

4.1.3 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

        1uLg9O8Bhhp3saZfk56Ta7CegbG5
```

```
</wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#binaryToken">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
        JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
        hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
        8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
```

```
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1:ValidateCertificateResponse xmlns:ns1="http://soapinterop.org/">
    <ValidateCertificateReturn xsi:type="soapenc:string" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
    <?xml version="1.0?>
    <outputMessage  xmlns=”http://afirmaws/ws/validation” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mvalidacion/wseng.xsd">
        <request>ValidateCertificate</request>
        <versionMsg>1.0</versionMsg>
        <response>
            <ProcessResult>
                <InfoCertificate>
                    <Field>
                        <idField>tipoCertificado</idField>
                        <fieldValue>[tipo_certificado]</fieldValue>
                    </Field>
```

```
<Field>
    <idField>subject</idField>
    <fieldValue>[subject]</fieldValue>
</Field>
<Field>
    <idField>nombreResponsable</idField>
    <fieldValue>[nombre]</fieldValue>
</Field>
<Field>
    <idField>segundoApellidoResponsable</idField>
    <fieldValue>[segundo_apellido]</fieldValue>
</Field>
<Field>
    <idField>primerApellidoResponsable</idField>
    <fieldValue>[primer_apellido]</fieldValue>
</Field>
<Field>
    <idField>idEmisor</idField>
    <fieldValue>[idEmisor]</fieldValue>
</Field>
<Field>
    <idField>NIF-CIF</idField>
    <fieldValue>[cif]</fieldValue>
</Field>
```

```
<Field>
    <idField>email</idField>
    <fieldValue>[email]</fieldValue>
</Field>
<Field>
    <idField>NIFResponsable</idField>
    <fieldValue>[nifResponsable]</fieldValue>
</Field>
<Field>
    <idField>fechaNacimiento</idField>
    <fieldValue>[fechaNacimiento]</fieldValue>
</Field>
<Field>
    <idField>razonSocial</idField>
    <fieldValue>[razonSocial]</fieldValue>
</Field>
<Field>
    <idField> clasificacion </idField>
    <fieldValue>[clasificacion]</fieldValue>
</Field>
<Field>
    <idField> numeroSerie </idField>
    <fieldValue>[numero de serie del certificado]</fieldValue>
</Field>
```

```
            <Field>
                <idField>certQualified</idField>
                <fieldValue>[TSL: Indica si se considera cualificado]</fieldValue>
            </Field>
            <Field>
                <idField>certClassification</idField>
                <fieldValue>[TSL: Tipo de certificado]</fieldValue>
            </Field>
            <Field>
                <idField>qscd</idField>
                <fieldValue>[TSL: Si se almacena en dispositivo seguro cualificado]</fieldValue>
            </Field>
        </InfoCertificate>
        <ValidationResult>
            <result>[cod_resultado]</result>
            <description>[descripción_resultado]</description>
            <SimpleValidation>
                <resultCode>[cod_resultado]</resultCode>
                <resultDescription>[des_resultado]</resultDescription>
                <exception>[desc_excepcion]</exception>
            </SimpleValidation>
            <StatusValidation>
                <status>[cod_estado]</status>
                <statusDescription>[descripción_estado]</statusDescription>
```

```
<VerificationMethodInfo>
    <status>[cod_estado]</status>
    <statusDescription>[descripción_estado]</statusDescription>
    <lastUpdateDate>[fecha_actualizacion]</ lastUpdateDate>
    <revocationDate>[fecha_revocacion]</revocationDate>
    <motive>[motivo_revocacion]</motive>
    <Method>
        <serverURL>[url_servidor]</serverURL>
        <protocol>[protocolo]</protocol>
    </Method>
<tokenOCSP><![CDATA[token OCSP en Base64]]></tokenOCSP>
    <exception>[desc_excepcion]</exception>
</VerificationMethodInfo>
<VerificationMethodInfo>
    <status>[cod_estado]</status>
    <statusDescription>[descripción_estado]</statusDescription>
    <lastUpdateDate>[fecha_actualizacion]</ lastUpdateDate >
    <revocationDate>[fecha_revocacion]</revocationDate>
    <motive>[motivo_revocacion]</motive>
    <Method>
        <serverURL>[url_servidor]</serverURL>
        <protocol>[protocolo]</protocol>
    </Method>
    <exception>[desc_excepcion]</exception>
```

```
            </VerificationMethodInfo>
        </StatusValidation>
        <ChainValidation>
            <resultCode>[cod_resultado]</resultCode>
            <resultDescription>[descripción_resultado]</resultDescription>
            <certificateError>
                <idCertificate>[subject]</idCertificate>
                <SimpleValidation>
                    <resultCode>[cod_resultado]</resultCode>
                    <resultDescription>[descripción_resultado]</resultDescription>
                    <exception>[desc_excepcion]</exception>
                </SimpleValidation>
                <StatusValidation>
                    <status>[cod_estado]</status>
                    <statusDescription>[descripción_estado]</statusDescription>
                    <VerificationMethodInfo>
                        <status>[cod_estado]</status>
                        <statusDescription>[descripción_estado]</statusDescription>
                        <lastUpdateDate>[fecha_actualizacion]</ lastUpdateDate >
                        <revocationDate>[fecha_revocacion]</revocationDate>
                        <motive>[motivo_revocacion]</motive>
                        <Method>
                          <serverURL>[url_servidor]</serverURL>
                          <protocol>[protocolo]</protocol>
```

```
                                    </Method>
                                    <excepcion>[cod_excepcion]</excepcion>
                                </VerificationMethodInfo>
                            </StatusValidation>
                        </certificateError>
                    </ChainValidation>
                </ValidationResult>
            </ProcessResult>
        </response>
    </outputMessage>
    </ValidateCertificateReturn>
    </ns1:ValidateCertificateResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los elementos enumerados en la respuesta se identifican con:

- Elemento **InfoCertificado**: Información del certificado validado en caso de haber especificado en la llamada "obtenerInfo" a true.
- Elemento **ResultadoValidacion**: Información resultado de la validación del certificado pasado como parámetro.
    1. Elemento **ValidacionSimple**: resultado de la validación de la caducidad, integridad y confianza del certificado
    2. Elemento **ValidacionEstado**: resultado de validación del estado del certificado. Solo será devuelto en caso de realización de una validación compleja (parámetro modoValidacion en el mensaje de entrada es 1).

Nota: en la información de validación de estado se ha incluido un nuevo campo informativo donde, en el caso de utilizar algún método de consulta OCSP, se incluye el OCSP Response recibido del servidor OCSP consultado. De esta forma se dota al cliente de un elemento de confianza adicional que puede ser utilizado para la generación de firmas y otros procesos que requieran un nivel más elevado de seguridad. El token incluido es la serialización en bytes convertida a Base64 de una estructura BasicOCSPResponse, tal y como se define en la RFC 2560.

El token OCSP será incluido únicamente en todos aquellos métodos de consulta OCSP que se utilicen para la consulta de estado de un certificado contra un determinado PSC. En caso de haberse producido cualquier error en la consulta OCSP, el elemento irá vacío en el XML de respuesta.

3. Elemento **ValidacionCadena**: resultado de validación de la cadena de confianza del certificado. Solo será devuelto en caso de realización de una validación compleja (parámetro modoValidacion en el mensaje de entrada es 2).

Los items enumerados en la respuesta se identifican con:

- “tipo_certificado”: Tipo de certificado.
- “subject”: información del responsable del certificado.
- “nombre”: Nombre del responsable del certificado.
- “segundo_apellido”: Segundo apellido del responsable del certificado.
- “primer_apellido”: Primer apellido del responsable del certificado.
- “idEmisor”: Identificador del emisor del certificado.
- “cif”: número de identificación de la persona jurídica para certificados de entidad.
- “email”: email del responsable del certificado.
- “nifResponsable”: Nif del responsable del certificado
- “fechaNacimiento”: Fecha de nacimiento de la persona responsable, en caso de e-DNI.
- “razonSocial”: razón social de la persona jurídica.

- "clasificacion": Clasificación del certificado en base a su naturaleza. Puede tomar los valores [0,1,2] con los siguientes criterios:

    - valor "0". Tipo de certificado para PERSONA FÍSICA.
    - valor "1". Tipo de certificado para PERSONA JURÍDICA.
    - valor "2". Tipo de certificado para COMPONENTES.

  En la DPC de la plataforma se detallan los valores asociados a cada tipo de certificado dado de alta en la plataforma @firma.

- "numeroSerie": número de serie del certificado.
- "cod_resultado": código resultado
- "descripción_resultado": descripción asociada al código de resultado.
- "desc_excepcion": item opcional que mostrará la descripción de la excepción en caso de producirse.
- "cod_estado": código del estado del certificado.
- "descripción_estado": descripción del estado del certificado.
- "fecha_actualizacion": fecha de ultima actualización.
- "fecha_revocacion": fecha de revocación del certificado.
- "motivo_revocacion": motivo de revocación del certificado. Puede tomar los siguientes valores:

    - valor "0". Motivo no especificado: La razón de la revocación no concuerda con ninguna de las razones predefinidas.
    - valor "1". Clave comprometida: Una persona que no es el asunto de la clave puede haber descubierto el valor de la clave privada.
    - valor "2". Autoridad de Certificación comprometida: Alguna persona puede haber revelado la clave privada del emisor del certificado.

- valor “3”. Cambio de Afiliación: El asunto del certificado no funciona por más tiempo para la empresa.
- valor “4”: Reemplazado: Un certificado nuevo sustituye al certificado existente.
- valor “5”: Cese de operaciones: El asunto del certificado no requiere por más tiempo el certificado.
- valor “6”: Certificado en estudio (revocado temporalmente).
- valor “7”: No se usa.
- valor “8”: Certificado eliminado de la lista de revocación. Este motivo tan solo puede aparecer en una Delta-CRL.
- valor “9”: Se retiran los privilegios del certificado.
- valor “10”: Atributo de certificado comprometido.

- “url_servidor”: url del servidor contra el cual se ha producido la verificación de estado del certificado.
- “protocolo”: protocolo por el cual se ha verificado el estado del certificado.
- “tokenOCSP”: en la información de validación de estado se ha incluido un nuevo campo informativo donde, en el caso de utilizar algún método de consulta OCSP, se incluye el OCSP Response recibido del servidor OCSP consultado. De esta forma se dota al cliente de un elemento de confianza adicional que puede ser utilizado para la generación de firmas y otros procesos que requieran un nivel más elevado de seguridad. El token incluido es la serialización en bytes convertida a Base64 de una estructura BasicOCSPResponse, tal y como se define en la RFC 2560.

El número de items y la información contenida en el xml de respuesta variará en función del certificado y tipo de certificado a validar.

NOTA: La estructura de campos presentada es la información básica que devuelve la plataforma. Los campos pueden venir en otro orden al marcado en este manual, y por lo tanto las aplicaciones cliente deben adaptar sus sistemas a tal efecto. Existe la posibilidad por parte de la plataforma @Firma 5.6 de definir e incluir aquellos otros campos que consideren de interés los organismos y vengan incluidos en los certificados dados de alta en la plataforma. De tal manera que en un futuro se irán

definiendo otras políticas de parseado de campos que se incuirán en los anexos en sucesivas versiones para que estén a disposición de los organismos interesados.

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):

```
<InfoCertificate>
        <Field>
                <idField>subject</idField>
                <fieldValue>[Asunto del certificado]</fieldValue>
        </Field>
        <Field>
                <idField>issuer</idField>
                <fieldValue>[Emisor del certificado]</fieldValue>
        </Field>
        <Field>
                <idField>serialNumber</idField>
                <fieldValue>[Número de serie del certificado]</fieldValue>
        </Field>
        <Field>
                <idField>cn</idField>
                <fieldValue>[Campo Common Name del asunto del certificado]</fieldValue>
        </Field>
        <Field>
                <idField>country</idField>
                <fieldValue>[Campo Country indicado en el asunto del
certificado]</fieldValue>
        </Field>
        <Field>
                <idField>extendedKeysUsage</idField>
                <fieldValue>[Listado separado por comas de los OID de los ExtendedKeyUsage
del certificado]</fieldValue>
        </Field>
        <Field>
                <idField>country</idField>
```

```
                    <fieldValue>[Campo Country indicado en el asunto del certificado]</
fieldValue>
                </Field>
</InfoCertificate>
```

4.1.4 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
    message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
    x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
```

```
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
```

```
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
      <ns1:ValidateCertificateResponse xmlns:ns1="http://soapinterop.org/">
      <ValidateCertificateReturn xsi:type="soapenc:string"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
          <?xml version="1.0" ?>
          <outputMessage  xmlns=”http://afirmaws/ws/validation” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mvalidacion/wseng.xsd">
                        <request>ValidateCertificate</request>
                        <versionMsg>1.0</versionMsg>
                        <response>
                            <Exception>
                                <errorCode>[cod_error]</errorCode>
```

```
                    <description>[descripcion]</description>
                    <associatedException>[excepcion_asociada]</associatedException>
                </Exception>
            </response>
        </outputMessage>
    </ValidateCertificateReturn>
    </ns1:ValidateCertificateResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.2 Módulo_Validacion. Obtención de Información de Certificado.

Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaVerifyCertificate**.

ObtenerInfoCertificado permite extraer la información de un certificado mediante la aplicación del mapeo definido para su tipo. Este proceso verificará que el tipo de certificado se encuentra definido en la plataforma y que la aplicación que realiza la petición tiene acceso a dicho tipo de certificado.

4.2.1 GetInfoCertificate.wsdl

El WSDL referente a este servicio se puede encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/services/GetInfoCertificate?wsdl

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/services/GetInfoCertificate?wsdl

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mvalidacion/wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mvalidacion/wseng.xsd

4.2.2 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <GetInfoCertificate xmlns="http://soapinterop.org/">

  <GetInfoCertificateRequest xsi:type="xsd:string" xmlns="">

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

      <inputMessage xmlns=”http://afirmaws/ws/validation” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mvalidacion/wseng.xsd">

            <request>GetInfoCertificate</request>

            <versionMsg>1.0</versionMsg>

            <parameters>

                  <certificate><![CDATA[contenido del certificado]]></certificate>

                  <applicationId>[idAplicacion]</applicationId>

            </parameters>
```

```
        </inputMessage>

    </GetInfoCertificateRequest>

    </GetInfoCertificate>

</soapenv:Body>

</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- "Certificado": Contenido del certificado a validar codificado en Base 64.
- "idAplicacion": Identificador de la aplicación que realiza la petición.

4.2.3 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

     <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

          MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

          DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

          YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

          QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

          czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN
```

```
        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h
        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B
        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz
        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd
        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
```

```
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1: GetInfoCertificateResponse xmlns:ns1="http://soapinterop.org/">
    <GetInfoCertificateReturn xsi:type="soapenc:string" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
    <?xml version="1.0"?>
    <outputMessage  xmlns=”http://afirmaws/ws/validation” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance" xsi: SchemaLocation="https://localhost/afirmaws/xsd/mvalidacion/wseng.xsd">
        <request>GetInfoCertificate</request>
        <versionMsg>1.0</versionMsg>
        <response>
                <ProcessResult>
                    <InfoCertificate>
                        <Field>
                            <idField>tipoCertificado</idField>
                            <fieldValue>[tipo_certificado]</fieldValue>
                        </Field>
                        <Field>
                            <idField>subject</idField>
                            <fieldValue>[subject]</fieldValue>
                        </Field>
                        <Field>
                            <idField>nombreResponsable</idField>
                            <fieldValue>[nombre]</fieldValue>
                        </Field>
                        <Field>
                            <idField>segundoApellidoResponsable</idField>
                            <fieldValue>[segundo_apellido]</fieldValue>
                        </Field>
                        <Field>
                            <idField>primerApellidoResponsable</idField>
```

```
        <fieldValue>[primer_apellido]</fieldValue>
    </Field>
    <Field>
        <idField>idEmisor</idField>
        <fieldValue>[idEmisor]</fieldValue>
    </Field>
    <Field>
        <idField>NIF-CIF</idField>
        <fieldValue>[cif]</fieldValue>
    </Field>
    <Field>
        <idField>email</idField>
        <fieldValue>[email]</fieldValue>
    </Field>
    <Field>
        <idField>NIFResponsable</idField>
        <fieldValue>[nifResponsable]</fieldValue>
    </Field>
    <Field>
        <idField>fechaNacimiento</idField>
        <fieldValue>[fechaNacimiento]</fieldValue>
    </Field>
    <Field>
        <idField>razonSocial</idField>
```

```
                                    <fieldValue>[razonSocial]</fieldValue>
                                </Field>
                                <Field>
                                    <idField> clasificacion </idField>
                                    <fieldValue>[clasificacion]</fieldValue>
                                </Field>
                                <Field>
                                    <idField> numeroSerie </idField>
                                    <fieldValue>[numero de serie del certificado]</fieldValue>
                                </Field>
                            </InfoCertificate>
                        </ProcessResult>
                </response>
    </outputMessage>
    </GetInfoCertificateReturn>
    </ns1: GetInfoCertificateResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- “tipo_certificado”: Tipo de certificado.
- “subject”: información del responsable del certificado.
- “nombre”: Nombre del responsable del certificado.
- “segundo_apellido”: Segundo apellido del responsable del certificado.

- “primer_apellido”: Primer apellido del responsable del certificado.
- “idEmisor”: Identificador del emisor del certificado.
- “cif”: número de identificación de la persona jurídica para certificados de entidad.
- “email”: email del responsable del certificado.
- “nifResponsable”: Nif del responsable del certificado
- “fechaNacimiento”: Fecha de nacimiento de la persona responsable, en caso de e-DNI.
- “razonSocial”: razón social de la persona jurídica.
- “clasificacion”: Clasificación del certificado en base a su naturaleza. Puede tomar los valores [0,1,2] con los siguientes criterios:
    - valor “0”. Tipo de certificado para PERSONA FÍSICA.
    - valor “1”. Tipo de certificado para PERSONA JURÍDICA.
    - valor “2”. Tipo de certificado para COMPONENTES.

  En la DPC de la plataforma se detallan los valores asociados a cada tipo de certificado dado de alta en la plataforma @firma.
- “numeroSerie”: número de serie del certificado.

Debido a que no todos los certificados contienen la misma información, la respuesta devuelta por este servicio puede variar de un certificado a otro. En aquellos casos en que un campo determinado no aplique a un certificado o no se pueda extraer de la información contenida en el mismo, el campo se devolverá vacío.

Por otro lado, el número de campos o su orden dentro de la respuesta puede variar a lo largo del tiempo. Para evitar errores al interpretar la respuesta, hay que tratar los campos por su nombre y no por su posición dentro de la respuesta. La lista de todos los campos devueltos para cada tipo de certificado se puede consultar en el documento "Procedimiento de inclusión y clasificación de certificados en @firma. Versión 2.6 Integradores” (apartados 5 y 6).

4.2.4 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

        1uLg9O8Bhhp3saZfk56Ta7CegbG5
```

```
</wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#binaryToken">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
        JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
        hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
        8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
```

```
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
      <ns1: GetInfoCertificateResponse xmlns:ns1="http://soapinterop.org/">
      <GetInfoCertificateReturn xsi:type="soapenc:string"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
      <?xml version="1.0"?>
      <outputMessage  xmlns=”http://afirmaws/ws/validation” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mvalidacion/wseng.xsd">
                <request>GetInfoCertificate</request>
                <versionMsg>1.0</versionMsg>
                <response>
                    <Exception>
                        <errorCode>[cod_error]</errorCode>
                        <description>[descripción error]</description>
                        <associatedException>[excepcion_asociada]</associatedException>
                    <Exception>
                </response>
```

```
        </outputMessage>

        </GetInfoCertificateReturn>

        </ns1: GetInfoCertificateResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.3 Módulo_Firma. Validar Firmas.

Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaVerify**.

ValidarFirma representa el proceso de validar una firma dada, ya sea en formato PKCS7 v1.5, CMS, CAdES-BES, CAdES-EPES, CAdES-T, CAdES-C, CAdES-X1, CAdES-X2, CAdES-XL1, CAdES-XL2, CAdES-A, XMLDSIG, XAdES, XAdES-BES, XAdES-EPES, XAdES-T, XAdES-C, XAdES-X1, XAdES-X2, XAdES-XL1, XAdES-XL2, XAdES-A, PDF, PAdES-Basic, PADES-BES, PAdES-EPES, PAdES-LTV, ODF, OOXML, CAdES B-Level, CAdES T-Level, CAdES LT-Level, CAdES LTA-Level, XAdES B-Level, XAdES T-Level, XAdES LT-Level, XAdES LTA-Level, PAdES B-Level, PAdES T-Level, PAdES LT-Level, PAdES LTA-Level, y ASiC-S. En caso de indicar un formato de firma más avanzado en la petición al que realmente tiene la firma, la validación se considerará incorrecta.

4.3.1 SignatureValidation.wsdl

El WSDL referente a este servicio se puede encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/services/SignatureValidation?wsdl

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/services/SignatureValidation?wsdl

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

4.3.2 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <SignatureValidation xmlns="http://soapinterop.org/">

  <SignatureValidationRequest xsi:type="xsd:string" xmlns="">

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

      <inputMessage xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">

            <request>SignatureValidation</request>

            <versionMsg>1.0</versionMsg>

            <parameters>

                  <applicationId>[idAplicacion]</applicationId>

                  <eSignature><![CDATA[firma_electronica]]></eSignature >

                  <eSignatureFormat>[formato_firma]</eSignatureFormat>
```

```
                    <hash><![CDATA[hash]]></hash>
                    <hashAlgorithm>[algoritmo_hash]</hashAlgorithm>
                    <data><![CDATA[datos]]></data>
                </parameters>
            </inputMessage>
        </SignatureValidationRequest>
        </SignatureValidation>
</soapenv:Body>
</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- "idAplicacion": Identificador de la aplicación que realiza la petición. Esta información permitirá obtener la política asociada para determinar el marco en el que se realizará el proceso requerido.
- "firma_electronica": Firma electronica a validar codificado en Base 64.
- "formato_firma": Formato de la firma a validar (PKCS7, CMS, CADES, CADES-BES, CADES-EPES, CADES-T, CADES-C, CADES-X, CADES-X1, CADES-X2, CADES-XL, CADES-XL1, CADES-XL2, CADES-A, XMLDSIG, XADES, XADES-BES, XADES-EPES, XADES-T, XADES-C, XADES-X, XADES-X1, XADES-X2, XADES-XL, XADES-XL1, XADES-XL2, XADES-A, PDF, PADES, PADES-BES, PADES-EPES, PADES-LTV, ODF, OOXML, CADES-B-LEVEL, CADES-T-LEVEL, CADES-LT-LEVEL, CADES-LTA-LEVEL, XADES-B-LEVEL, XADES-T-LEVEL, XADES-LT-LEVEL, XADES-LTA-LEVEL, PADES-B-LEVEL, PADES-T-LEVEL, PADES-LT-LEVEL, PADES-LTA-LEVEL, ASIC-S-B-LEVEL, ASIC-S-T-LEVEL, ASIC-S-LT-LEVEL y ASIC-S-LTA-LEVEL). El formato CADES es equivalente a CADES-BES, CADES-X a CADES-X1, CADES-XL a CADES-XL1, XADES a XADES-BES, XADES-X a XADES-X1, XADES-XL a XADES-XL1. En caso de no indicarse formato, la plataforma lo detectará automáticamente.
- "hash": Hash de los datos cuya firma se va a validar, codificado en Base 64. En caso de indicarse, deberá indicarse también el parámetro algoritmoHash. Se admiten los valores MD2, MD5, SHA1, SHA256, SHA384 y SHA512.

- "algoritmo_hash": Algoritmo de hash con el que se calculó el valor anterior. Sólo tiene sentido en caso de indicar el valor del hash (parámetro anterior).

- "datos": Datos cuya firma se va a validar codificado en Base 64. En firmas ODF, PDF, PADES, PADES-BES, PADES-EPES, PADES-LTV, OOXML, PADES-B-LEVEL, PADES-T-LEVEL, PADES-LT-LEVEL, y PADES-LTA-LEVEL la firma no se validará contra estos datos ya que la propia firma contiene el documento.

4.3.3 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
```

```
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
```

```
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1: SignatureValidationResponse xmlns:ns1="http://soapinterop.org/">
    <SignatureValidationReturn xsi:type="soapenc:string" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
          <?xml version="1.0"?>
          <outputMessage  xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">
                <request>SignatureValidation</request>
                <versionMsg>1.0</versionMsg>
                <response>
                     <Response>
```

```
                    <status>[estado]</status>
                    <description>
                        <eSignatureValidation>
                            <process>[proceso]</process>
                            <detail>[detalle]</detail>
                            <conclusion>[conclusion]</conclusion>
                            <additionalInformation>
                                <signer>
                                    <certificate>[certificado]</certificate>
                                    <timeStamp>[sello_tiempo]</timeStamp>
                                    <certificateTSA>[cert_TSA]</ certificateTSA >
                                </signer>
                            </additionalInformation>
                        </eSignatureValidation>
                    </description>
                </Response>
            </response>
        </outputMessage>
    </SignatureValidationReturn>
    </ns1: SignatureValidationResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.

- "proceso": Indica si se ha podido llevar a cabo de forma completa el proceso de validación de la firma electrónica. Consulte el apartado A.4.1 para ver los posibles valores.

- "detalle": Indica el resultado de cada una de las subetapas que se realizan en un proceso de validación de firma electrónica. Consulte el apartado A.4.2 para ver los posibles valores.

- "conclusion": Indica el resultado final del proceso de validación de firma electrónica. Indica el resultado final del proceso de validación de firma electrónica. Consulte el apartado A.4.3 para ver los posibles valores

Para cada uno de los firmantes contenidos en la firma electrónica:

- "certificado": Indica el certificado del firmante empleado en la firma electrónica. Este certificado se incluye formateado en Base64.

- "sello_tiempo": Time-Stamp del sello de tiempo de la firma electrónica. **Si la firma posee formato PAdES-LTV y además contiene al menos un diccionario de firma de tipo Document Time-stamp, este valor indicará únicamente la información del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente**.

- "cert_TSA": Certificado empleado por la TSA para firmar el TimeStampToken de la firma electrónica. **Si la firma posee formato PAdES-LTV y además contiene al menos un diccionario de firma de tipo Document Time-stamp, este valor indicará únicamente la información del certificado de la autoridad emisora de sello de tiempo del sello de tiempo contenido en el diccionario de firma de tipo Document Time-stamp más reciente**.

4.3.4 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
```

```
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
    message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
    x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

        1uLg9O8Bhhp3saZfk56Ta7CegbG5

    </wsse:BinarySecurityToken>

    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

        <ds:SignedInfo>

            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

```
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#binaryToken">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
        JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
        hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
        8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
    </ds:SignatureValue>
    <ds:KeyInfo>
        <wsse:SecurityTokenReference>
            <wsse:Reference URI="#binaryToken"/>
```

```
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1:SignatureValidationResponse xmlns:ns1="http://soapinterop.org/">
    <SignatureValidationReturn xsi:type="soapenc:string"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
        <?xml version="1.0" ?>
        < mensajeSalida xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">
            <request>SignatureValidation</request>
            <versionMsg>1.0</versionMsg>
            <response>
                <Exception>
                    <errorCode>[cod_error]</errorCode>
                    <description>[descripción error]</description>
                    <associatedException>[excepcion_asociada]</associatedException>
                <Exception>
            </response>
        </outputMessage>
    </SignatureValidationReturn>
    </ns1: SignatureValidationResponse>
</soapenv:Body>
```

```
</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.4 Módulo_Firma. Firma Servidor.

FirmaServidor representa el proceso de llevar a cabo una firma digital en servidor.

Este servicio se considera "legacy" (obsoleto), **no será evolucionado,** y se encuentra en proceso de discontinuación. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaSign**.

En el caso de que la firma a generar sea de tipo ASN.1, dicha firma se generará siempre explícita, y en el caso de que la firma a generar sea de tipo XML, la firma se generará siempre "detached".

No se permite la generación de firmas que incluyan política de firma (formatos AdES-EPES).

Se debe de tener en cuenta que las firmas generadas sólo podrán ser XMLDsig/XAdES Detached (no Enveloped/Enveloping).

Indicar que este modo de firma se puede considerar como firma delegada, dado que los organismos indican a la plataforma con qué certificado realizar la Firma Electrónica. Este certificado se localiza por tanto en plataforma @Firma y debe haber sido dado de alta por los administradores de la plataforma haciendo uso de la Herramienta de Administración.

Así pues, cada organismo puede tener definidos sus propios certificados para firmas servidor, haciendo uso en la invocación a este Servicio Web del certificado deseado mediante el parámetro *firmante* (el cual es el alias dado a dicho certificado mediante la Herramienta de Administración).

4.4.1 ServerSignature.wsdl

El WSDL referente a este servicio se puede encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/services/ServerSignature?wsdl

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/services/ServerSignature?wsdl

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

4.4.2 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <ServerSignature xmlns="http://soapinterop.org/">

  <ServerSignature Request xsi:type="xsd:string" xmlns="">

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

      <inputMessage xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">

            <request> ServerSignature </request>

            <versionMsg>1.0</versionMsg>

            <parameters>
```

```
                    <applicationId>[idAplicacion]</applicationId>
                    <documentId>[idDocumento]</documentId>
                <document><![CDATA[documento]]></document>
                    <documentName>[nombre_documento]</documentName>
                    <documentType>[tipo_documento]</documentType>
                <hash>[hash_documento]</hash>
                    <signer>[firmante]</signer>
                    <reference>[idReferencia]</reference>
                    <hashAlgorithm>[algoritmo_hash]</hashAlgorithm>
                    <eSignatureFormat>[formato_firma]</eSignatureFormat>
                </parameters>
        </inputMessage>
    </ ServerSignature Request>
    </ ServerSignature >
</soapenv:Body>
</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- "idAplicacion": Identificador de la aplicación que realiza la petición. Esta información permitirá obtener la política asociada para determinar el marco en el que se realizará el proceso requerido.
- Documento a firmar. El servicio permite especificar los datos a firmar en uno de los siguientes modos:

    1. Mediante identificador de registro de documento. En este caso la petición debe incluir el elemento siguiente:

- "idDocumento": Identificador único del documento a firmar, para ello se debe haber registrado previamente mediante las interfaces proporcionadas por el módulo de Custodia. Este elemento es obligatorio en el caso de no incluir en la petición el documento a firmar o el hash del mismo.

2. Incluyendo el fichero a firma, para ello la petición debe incluir los siguientes elementos:

   - "documento": Datos a firmar codificado en Base 64. Este elemento es obligatorio en el caso de no haber registrado previamente el documento en la plataforma o no se haya incluido el hash del documento.

   - "nombre_documento": Nombre del documento. Sólo tiene sentido que se indique en caso de indicar también el documento.

   - "tipo_documento": Formato del documento. Sólo tiene sentido que se indique en caso de indicar también el documento.

3. Suministrando el hash del documento a firmar. Si se desea realizar la firma de servidor sobre el hash de un documento se debe incluir en la petición el siguiente elemento:

   - "hash_documento". Hash del documento a firma codificado en Base 64. El documento debe ser resumido en el algoritmo de hash especificado en el elemento "algoritmo_hash" o en caso de no indicarse este elemento en SHA1. Este elemento es obligatorio en el caso de no haber registrado previamente el documento en la plataforma o no se haya enviado el mismo en la petición.

   Este modo de firma es incompatible con los formatos de firma PDF u ODF ya que estos exigen tener el documento original completo.

- "firmante": Identificador único de firmante.

- "idReferencia": Identificador externo a la plataforma y manejado internamente por la aplicación. Sólo se indica en caso que se necesite por parte de dicha aplicación.

- "algoritmo_hash": Indica el algoritmo de hash a emplear en el cálculo de la firma. Debe ser uno de los asociados con el documento en el momento de registrarlo en la plataforma (interfaz de Custodia). En caso de no indicarse, se supondrá SHA1. Se admiten los valores SHA1, SHA256, SHA384 y SHA512 (en combinación con cualquier formato de firma).

- "formato_firma": Indica el formato de la firma a generar (CMS, CMS-T, CADES, CADES-BES, CADES-T, CAdES-C, CADES-X, CADES-X1, CADES-X2, CADES-XL, CADES-XL1, CADES-XL2, CADES-A, XMLDSIG, XADES, XADES-BES, XADES-T, XAdES-C, XADES-X, XADES-X1, XADES-X2, XADES-XL, XADES-XL1, XADES-XL2, XADES-A, PDF, ODF, PADES, PADES-BES, PADES-LTV, CADES-B-LEVEL, CADES-T-LEVEL, CADES-LT-LEVEL, CADES-LTA-LEVEL, XADES-B-LEVEL, XADES-T-LEVEL, XADES-LT-LEVEL, XADES-LTA-LEVEL, PADES-B-LEVEL, PADES-T-LEVEL, PADES-LT-LEVEL y PADES-LTA-LEVEL). El formato CADES es equivalente a CADES-BES, CADES-X a CADES-X1, CADES-XL a CADES-XL1, XADES a XADES-BES, XADES-X a XADES-X1, XADES-XL a XADES-XL1. En caso de no indicarse, se supondrá CMS.

4.4.3 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz
```

```
        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd
        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
 <ns1: ServerSignature Response soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">
      < ServerSignature Return xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
    xsi:type="soapenc:string">
        <?xml version="1.0"?>
        <outputMessage  xmlns="http://afirmaws/ws/signature" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
        instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd ">
          <request>ServerSignature</request>
```

```
        <versionMsg>1.0 </versionMsg>
        <response>
          <Response>
            <status>[estado]</status>
            <description>[descripcion]</description>
            <transactionId>[id_transaccion]</transactionId>
            <eSignature><![CDATA[firma_electronica]]></eSignature>
            <eSignatureFormat>[formato_firma]</eSignatureFormat>
            <documentId>[id_documento]</documentId>
          </ Response>
        </response>
      </outputMessage>
    </ ServerSignatureReturn>
  </ns1: ServerSignatureResponse>
 </soapenv:Body>
</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.
- "descripción": Contiene una descripción del error o excepción producido en el módulo.
- "id_transaccion": Identificador único de la transacción generada.
- "firma_electronica": Firma Electrónica. Está codificada en Base64.

- "formato_firma": Indica el formato de la firma generada (CMS, CADES, CADES-BES, CADES-EPES, CADES-T, CADES-X, CADES-X1, CADES-X2, CADES-XL, CADES-XL1, CADES-XL2, CADES-A, XMLDSIG, XADES, XADES-BES, XADES-EPES, XADES-T, XADES-X, XADES-X1, XADES-X2, XADES-XL, XADES-XL1, XADES-XL2, XADES-A, PDF, PADES, PADES-BES, PADES-EPES, PADES-LTV, ODF, CADES-B-LEVEL, CADES-T-LEVEL, CADES-LT-LEVEL, CADES-LTA-LEVEL, XADES-B-LEVEL, XADES-T-LEVEL, XADES-LT-LEVEL, XADES-LTA-LEVEL, PADES-B-LEVEL, PADES-T-LEVEL, PADES-LT-LEVEL y PADES-LTA-LEVEL). El formato CADES es equivalente a CADES-BES, CADES-X a CADES-X1, CADES-XL a CADES-XL1, XADES a XADES-BES, XADES-X a XADES-X1, XADES-XL a XADES-XL1. Se corresponde con el parámetro formatoFirma de entrada.

- "id_documento": Identificador de registro del documento. Este componente sólo se retorna en los mensajes de respuesta que se generen como resultado de peticiones que incluyan los datos a firmar en lugar del identificador de documentos.

4.4.4 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN
```

```
        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h
        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B
        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz
        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd
        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
```

```
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1: ServerSignatureResponse xmlns:ns1="http://soapinterop.org/">
    <ServerSignatureReturn xsi:type="soapenc:string" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
        <?xml version="1.0" ?>
        <outputMessage  xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">
                <request>ServerSignature</request>
                <versionMsg>1.0</versionMsg>
                <response>
                        <Exception>
                                <errorCode>[cod_error]</errorCode>
                                <description>[descripción error]</description>
                                <associatedException>[excepcion_asociada]</associatedException>
                        <Exception>
                </response>
            </outputMessage>
      </ServerSignatureReturn>
      </ns1: ServerSignatureResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.5 Módulo_Firma. Firma Servidor CoSign.

Este servicio se considera “legacy” (obsoleto), **no será evolucionado,** y se encuentra en proceso de discontinuación. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaSign**.

Esta operación no está permitida para los formatos de firma: CAdES-A, CAdES LTA-Level, OOXML, PDF, PAdES-Basic, PAdES-BES, PAdES-EPES, PAdES-LTV, PAdES B-Level, PAdES T-Level, PAdES LT-Level, y PAdES LTA-Level.

4.5.1 ServerSignatureCoSign.wsdl

El WSDL referente a este servicio se puede encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/services/ServerSignatureCoSign?wsdl

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/services/ServerSignatureCoSign?wsdl

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

4.5.2 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<soapenv:Body>

  <ServerSignatureCoSign xmlns="http://soapinterop.org/">

  <ServerSignatureCoSignRequest xsi:type="xsd:string" xmlns="">

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

      <inputMessage xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">

            <request>ServerSignatureCoSign</request>

            <versionMsg>1.0</versionMsg>

            <parameters>

                  <applicationId>[idAplicacion]</applicationId>

                  <transactionId>[idTransaccion]</transactionId>

                  <signer>[firmante]</signer>

                  <reference>[idReferencia]</reference>

                  <hashAlgorithm>[algoritmo_hash]</hashAlgorithm>

            </parameters>

      </inputMessage>

  </ServerSignatureCoSignRequest>

  </ServerSignatureCoSign>

</soapenv:Body>

</soapenv:Envelope
```

Cada uno de los parámetros enumerados se identifican con:

- “idAplicacion”: Identificador de la aplicación que realiza la petición. Esta información permitirá obtener la política asociada para determinar el marco en el que se realizará el proceso requerido.

- “idTransaccion”: Identificador único de la transacción de firma sobre la que se desea hacer la multifirma coSign. Se debe, por tanto, haber realizado una firma (simple, coSign o counterSign) previamente para haber obtenido dicho identificador de transacción

- “firmante”: Identificador único de firmante.

- “idReferencia”: Identificador externo a la plataforma y manejado internamente por la aplicación. Sólo se indica en caso que se necesite por parte de dicha aplicación.

- “algoritmo_hash”: Indica el algoritmo de hash a emplear en el cálculo de la firma. Debe ser uno de los asociados con el documento en el momento de registrarlo en la plataforma (interfaz de Custodia). En caso de no indicarse, se supondrá SHA1. Se admiten los valores SHA1, SHA256, SHA384 y SHA512 (en combinación con cualquier formato de firma).

4.5.3 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h
```

```
        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B
        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz
        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd
        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

```
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
 <ns1: ServerSignatureCoSignResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">
    < ServerSignatureCoSignReturn xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
   xsi:type="soapenc:string">
        <?xml version="1.0"?>
        <outputMessage  xmlns="http://afirmaws/ws/signature" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
        instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd ">
          <request>ServerSignatureCoSign</request>
          <versionMsg>1.0 </versionMsg>
          <response>
            <Response>
              <status>[estado]</status>
              <description>[descripcion]</description>
              <transactionId>[id_transaccion]</transactionId>
              <eSignature><![CDATA[firma_electronica]]></eSignature>
              <eSignatureFormat>[formato_firma]</eSignatureFormat>
            </Response>
          </response>
        </outputMessage>
    </ServerSignatureCoSignReturn>
 </ns1: ServerSignatureCoSignResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.
- "descripción": Contiene una descripción del error o excepción producido en el módulo.
- "id_transaccion": Identificador único de la transacción generada.
- "firma_electronica": Firma Electrónica. Está codificada en Base64.

- "formato_firma": Indica el formato de la firma generada (CMS, CADES, CADES-BES, CADES-EPES, CADES-T, CADES-X, CADES-X1, CADES-X2, CADES-XL, CADES-XL1, CADES-XL2, CADES-A, XMLDSIG, XADES, XADES-BES, XADES-EPES, XADES-T, XADES-X, XADES-X1, XADES-X2, XADES-XL, XADES-XL1, XADES-XL2, XADES-A, CADES-B-LEVEL, CADES-T-LEVEL, CADES-LT-LEVEL, CADES-LTA-LEVEL, XADES-B-LEVEL, XADES-T-LEVEL, XADES-LT-LEVEL y XADES-LTA-LEVEL). El formato CADES es equivalente a CADES-BES, CADES-X a CADES-X1, CADES-XL a CADES-XL1, XADES a XADES-BES, XADES-X a XADES-X1, XADES-XL a XADES-XL1. Se corresponde con el parámetro formatoFirma de entrada.

4.5.4 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd
```

```
        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
```

```
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
      <ns1: ServerSignatureCoSignResponse xmlns:ns1="http://soapinterop.org/">
      <ServerSignatureCoSignReturn xsi:type="soapenc:string"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
            <?xml version="1.0" ?>
            < mensajeSalida xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">
                  <request>ServerSignatureCoSign</request>
                  <versionMsg>1.0</versionMsg>
                  <response>
```

```
                    <Exception>
                        <errorCode>[cod_error]</errorCode>
                        <description>[descripción error]</description>
                        <associatedException>[excepcion_asociada]</associatedException>
                    <Exception>
                </response>
            </outputMessage>
        </ServerSignatureCoSignReturn>
        </ns1: ServerSignatureCoSignResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.6 Módulo_Firma. Firma Servidor CounterSign.

ServerSignatureCounterSign representa el proceso de llevar a cabo una multifirma counterSignature en servidor.

Este servicio se considera "legacy" (obsoleto), **no será evolucionado,** y se encuentra en proceso de discontinuación. Se recomienda a aquellas aplicaciones que integren este servicio, sustituirlo por su equivalente DSS: **DSSAfirmaSign**.

Esta operación no está permitida para los formatos de firma: XMLDSIG, ODF, PDF, PAdES-Basic, PAdES-BES, PAdES-EPES, PAdES-LTV, PAdES B-Level, PAdES T-Level, PAdES LT-Level, PAdES LTA-Level, CAdES-A, CAdES LTA-Level, XAdES-A y XAdES-LTA.

4.6.1 ServerSignatureCounterSign.wsdl

El WSDL referente a este servicio se puede encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/services/ServerSignatureCounterSign?wsdl

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/services/ServerSignatureCounterSign?wsdl

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

4.6.2 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <ServerSignatureCounterSign xmlns="http://soapinterop.org/">

  <ServerSignatureCounterSignRequest xsi:type="xsd:string" xmlns="">

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

      <inputMessage xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">

            <request>ServerSignatureCounterSign</request>
```

```
            <versionMsg>1.0</versionMsg>
            <parameters>
                <applicationId>[idAplicacion]</applicationId>
                <transactionId>[idTransaccion]</transactionId>
                <signer>[firmante]</signer>
                <reference>[idReferencia]</reference>
                <hashAlgorithm>[algoritmo_hash]</hashAlgorithm>
                <targetSigner><![CDATA[firmante_objetivo]]></targetSigner>
            </parameters>
        </inputMessage>
    </ServerSignatureCounterSignRequest>
    </ServerSignatureCounterSign>
</soapenv:Body>
</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- "idAplicacion": Identificador de la aplicación que realiza la petición. Esta información permitirá obtener la política asociada para determinar el marco en el que se realizará el proceso requerido.
- "idTransaccion": Identificador único de la transacción de firma sobre la que se desea hacer la multifirma counterSignature. Se debe, por tanto, haber realizado una firma (simple, coSign o counterSign) previamente para haber obtenido dicho identificador de transacción.
- "firmante": Identificador único de firmante.
- "idReferencia": Identificador externo a la plataforma y manejado internamente por la aplicación. Sólo se indica en caso que se necesite por parte de dicha aplicación.
- "algoritmo_hash": Indica el algoritmo de hash a emplear en el cálculo de la firma. Debe ser uno de los asociados con el documento en el momento de registrarlo en la plataforma

(interfaz de Custodia). En caso de no indicarse, se supondrá SHA1. Se admiten los valores SHA1, SHA256, SHA384 y SHA512 (en combinación con cualquier formato de firma).

- "firmante_objetivo": Certificado X509 codificado en base64 del firmante sobre el que realizar la firma counterSign. En caso de no indicarlo, se hará una firma counterSign sobre todos los firmantes localizados en las hojas del árbol de firmantes.

4.6.3 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
```

```
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
```

```
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
 <ns1:ServerSignatureCounterSignResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">
    <ServerSignatureCounterSignReturn xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
   xsi:type="soapenc:string">
        <?xml version="1.0"?>
        <outputMessage  xmlns="http://afirmaws/ws/signature" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
        instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd ">
          <request>ServerSignatureCounterSign</request>
          <versionMsg>1.0 </versionMsg>
          <response>
```

```
            <Response>
                <status>[estado]</status>
                <description>[descripcion]</description>
                <transactionId>[id_transaccion]</transactionId>
                <eSignature><![CDATA[firma_electronica]]></eSignature>
                <eSignatureFormat>[formato_firma]</eSignatureFormat>
            </Response>
        </response>
      </outputMessage>
   </ ServerSignatureCounterSignReturn>
 </ns1: ServerSignatureCounterSignResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.
- "descripción": Contiene una descripción del error o excepción producido en el módulo.
- "id_transaccion": Identificador único de la transacción generada.
- "firma_electronica": Firma Electrónica. Está codificada en Base64.
- "formato_firma": Indica el formato de la firma generada (CMS, CADES, CADES-BES, CADES-EPES, CADES-T, CADES-X, CADES-X1, CADES-X2, CADES-XL, CADES-XL1, CADES-XL2, XMLDSIG, XADES, XADES-BES, XADES-EPES, XADES-T, XADES-X, XADES-X1, XADES-X2, XADES-XL, XADES-XL1, XADES-XL2, CADES-B-LEVEL, CADES-T-LEVEL, CADES-LT-LEVEL, XADES-B-LEVEL, XADES-T-LEVEL, XADES-LT-LEVEL). El formato CADES es equivalente a CADES-BES, CADES-X a CADES-X1,

CADES-XL a CADES-XL1, XADES a XADES-BES, XADES-X a XADES-X1, XADES-XL a XADES-XL1. Se corresponde con el parámetro formatoFirma de entrada.

4.6.4 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
```

```
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
```

```
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
      <ns1: ServerSignatureCounterSignResponse xmlns:ns1="http://soapinterop.org/">
      <ServerSignatureCounterSignReturn xsi:type="soapenc:string"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
            <?xml version="1.0" ?>
            < mensajeSalida xmlns=”http://afirmaws/ws/signature” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mfirma/wseng.xsd">
                  <request>ServerSignatureCounterSign</request>
                  <versionMsg>1.0</versionMsg>
                  <response>
                        <Exception>
                              <errorCode>[cod_error]</errorCode>
                              <description>[descripción error]</description>
                              <associatedException>[excepcion_asociada]</associatedException>
                        <Exception>
```

```
                </response>

            </outputMessage>

      </ ServerSignatureCounterSignReturn>

      </ns1: ServerSignatureCounterSignResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.7 Módulo_Custodia. Almacenar Documento.

StoreDocument custodia el documento especificado junto con su nombre y tipo asignándole un identificador único al mismo.

Este servicio se considera "legacy" (obsoleto), **no será evlucionado**, y se encuentra en proceso de discontinuación.

4.7.1 StoreDocument.wsdl

El WSDL referente a este servicio se puede encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/services/StoreDocument?wsdl

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/services/StoreDocument?wsdl

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mcustodia/wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mcustodia/wseng.xsd

4.7.2 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <StoreDocument xmlns="http://soapinterop.org/">

  <StoreDocumentRequest xsi:type="xsd:string">

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

      <inputMessage xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">

            <request>StoreDocument</request>

            <versionMsg>1.0</versionMsg>

            <parameters>

                  <applicationId>[idAplicacion]</applicationId>

                  <document><![CDATA[documento]]></document>

                  <documentName>[nombre_documento]</documentName>

                  <documentType>[nombre_documento]</documentType>

            </parameters>
```

```
        </inputMessage>

    </StoreDocumentRequest>

    </StoreDocument>

</soapenv:Body>

</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- "idAplicacion": Identificador de la aplicación que realiza la petición.
- "documento": Contenido del documento a custodiar. Debe estar codificado en Base64.
- "nombre_documento": Nombre del documento a custodiar.
- "tipo_documento": Tipo del documento a custodiar.

4.7.3 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

     <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

         MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

         DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

         YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN
```

QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

1uLg9O8Bhhp3saZfk56Ta7CegbG5

```
</wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
```

```
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
 <ns1:StoreDocumentResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">
      <StoreDocumentReturn xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
```

```
    xsi:type="soapenc:string">

        <?xml version="1.0"?>

        <outputMessage  xmlns="http://afirmaws/ws/custody" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
        instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd ">

          <request>StoreDocument</request>

          <versionMsg>1.0 </versionMsg>

          <response>

            <Response>

              <status>[estado]</status>

              <description>[descripcion]</description>

              <documentId>[id_documento]</documentId>

            </Response>

          </response>

        </outputMessage>

    </StoreDocumentReturn>

 </ns1:StoreDocumentResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.
- "descripción": Contiene una descripción del error o excepción producido en el módulo.
- "id_documento": Identificador único asignado al documento custodiado.

4.7.4 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

        1uLg9O8Bhhp3saZfk56Ta7CegbG5
```

```
</wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#binaryToken">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
        JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
        hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
        8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
```

```
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1:StoreDocumentResponse xmlns:ns1="http://soapinterop.org/">
    <StoreDocumentReturn xsi:type="soapenc:string" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
        <?xml version="1.0" ?>
        <outputMessage  xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">
            <request>StoreDocument</request>
            <versionMsg>1.0</versionMsg>
            <response>
                <Exception>
                    <errorCode>[cod_error]</errorCode>
                    <description>[descripción error]</description>
                    <associatedException>[excepcion_asociada]</associatedException>
                <Exception>
            </response>
```

```
            </outputMessage>

        </StoreDocumentReturn>

        </ns1: StoreDocumentResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.8 Módulo_Custodia. Eliminar Contenido Documento.

Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado**.

DeleteDocumentContent elimina el contenido del documento con el identificador dado, dejando registro de la fecha de borrado. El resto de información asociada se mantiene por lo que se pueden seguir iniciando transacciones de firma sobre dicho documento.

4.8.1 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <DeleteDocumentContent xmlns="http://soapinterop.org/">

  <DeleteDocumentContentRequest xsi:type="xsd:string">
```

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

<inputMessage xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">

        <request>DeleteDocumentContent</request>

        <versionMsg>1.0</versionMsg>

        <parameters>

            <applicationId>[idAplicacion]</applicationId>

            <documentId>[id_documento]</documentId>

        </parameters>

    </inputMessage>

  </DeleteDocumentContentRequest>

  </DeleteDocumentContent>

</soapenv:Body>

</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- “idAplicacion”: Identificador de la aplicación que realiza la petición.
- “id_documento”: Identificador del documento custodiado cuyo contenido se desea eliminar.

4.8.2 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>
```

```
<wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">
    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">
        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3
        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN
        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN
        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l
        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN
        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h
        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B
        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz
        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd
        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
```

```
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#binaryToken">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
        JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
        hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
        8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
    </ds:SignatureValue>
    <ds:KeyInfo>
        <wsse:SecurityTokenReference>
            <wsse:Reference URI="#binaryToken"/>
        </wsse:SecurityTokenReference>
    </ds:KeyInfo>
```

```
    </ds:Signature>

 </wsse:Security>

</soapenv:Header>

<soapenv:Body wsu:Id="body">

 <ns1:DeleteDocumentContentResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">

      <DeleteDocumentContentReturn xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
    xsi:type="soapenc:string">

        <?xml version="1.0"?>

        <outputMessage  xmlns="http://afirmaws/ws/custody" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
        instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd ">

          <request>DeleteDocumentContent</request>

          <versionMsg>1.0 </versionMsg>

          <response>

            <Response>

              <status>[estado]</status>

              <description>[descripcion]</description>

            </Response>

          </response>

        </outputMessage>

    </DeleteDocumentContentReturn>

 </ns1:DeleteDocumentContentResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.
- "descripción": Contiene una descripción del error o excepción producido en el módulo.

4.8.3 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd
```

```
        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
```

```
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
      <ns1:DeleteDocumentContentResponse xmlns:ns1="http://soapinterop.org/">
      <DeleteDocumentContentReturn xsi:type="soapenc:string"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
            <?xml version="1.0" ?>
            <outputMessage  xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">
                  <request>DeleteDocumentContent</request>
                  <versionMsg>1.0</versionMsg>
                  <response>
```

```
                    <Exception>
                        <errorCode>[cod_error]</errorCode>
                        <description>[descripción error]</description>
                        <associatedException>[excepcion_asociada]</associatedException>
                    <Exception>
                </response>
            </outputMessage>
        </DeleteDocumentContentReturn>
        </ns1:DeleteDocumentContentResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.9 Módulo_Custodia. Obtener Contenido Documento.

Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado**.

GetDocumentContent devuelve, para un identificador de transacción de firma dado, el contenido del documento asociado a la misma codificado en Base 64.

4.9.1 Mensaje SOAP de petición.

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

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <GetDocumentContent xmlns="http://soapinterop.org/">

  <GetDocumentContentRequest xsi:type="xsd:string">

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

      <inputMessage xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">

            <request>GetDocumentContent</request>

            <versionMsg>1.0</versionMsg>

            <parameters>

                  <applicationId>[idAplicacion]</applicationId>

                  <transactionId>[id_transaccion]</transactionId>

            </parameters>

      </inputMessage>

  </GetDocumentContentRequest>

  </GetDocumentContent>

</soapenv:Body>

</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- “idAplicacion”: Identificador de la aplicación que realiza la petición.
- “id_transaccion”: Identificador de transacción de firma de la cual se desea obtener el contenido del documento.

4.9.2 Mensaje SOAP de respuesta OK.

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

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

        1uLg9O8Bhhp3saZfk56Ta7CegbG5

    </wsse:BinarySecurityToken>

    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
<ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#body">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#binaryToken">
        <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
    </ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
    JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
    hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
    8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
</ds:SignatureValue>
<ds:KeyInfo>
```

```
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
 <ns1:GetDocumentContentResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">
    <GetDocumentContentReturn xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xsi:type="soapenc:string">
      <?xml version="1.0"?>
      <outputMessage  xmlns="http://afirmaws/ws/custody" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
      instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd ">
        <request>GetDocumentContent</request>
        <versionMsg>1.0 </versionMsg>
        <response>
          <Response>
            <status>[estado]</status>
            <description>[descripcion]</description>
            <document><![CDATA[documento]]></document>
          </Response>
        </response>
      </outputMessage>
```

```
    </GetDocumentContentReturn>

 </ns1:GetDocumentContentResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.
- "descripción": Contiene una descripción del error o excepción producido en el módulo.
- "documento": Contenido del documento, codificado en Base64, asociado al identificador de transacción dado.

4.9.3 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN
```

QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

1uLg9O8Bhhp3saZfk56Ta7CegbG5

```
</wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
```

```
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1:GetDocumentContentResponse xmlns:ns1="http://soapinterop.org/">
    <GetDocumentContentReturn xsi:type="soapenc:string"
```

```
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">

        <?xml version="1.0" ?>

        <outputMessage  xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">

            <request>GetDocumentContent</request>

            <versionMsg>1.0</versionMsg>

            <response>

                <Exception>

                    <errorCode>[cod_error]</errorCode>

                    <description>[descripción error]</description>

                    <associatedException>[excepcion_asociada]</associatedException>

                <Exception>

            </response>

        </outputMessage>

    </GetDocumentContentReturn>

    </ns1:GetDocumentContentResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- “cod_error”: código de error.
- “descripcion”: descripción del error.
- “excepcion_asociada”: Excepción que ha provocado el error.

4.10 Módulo_Custodia. Obtener Contenido Identificador de Documento.

Este servicio se considera “legacy” (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado**.

GetDocumentContentByDocId devuelve, para un identificador de documento dado, el contenido del mismo codificado en Base 64.

4.10.1 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <GetDocumentContentByDocId xmlns="http://soapinterop.org/">

  <GetDocumentContentByDocIdRequest xsi:type="xsd:string">

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

      <inputMessage xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">

            <request>GetDocumentContentByDocId</request>

            <versionMsg>1.0</versionMsg>

            <parameters>

                  <applicationId>[idAplicacion]</applicationId>

                  <documentId>[id_documento]</documentId>

            </parameters>

      </inputMessage>

  </GetDocumentContentByDocIdRequest>

  </GetDocumentContentByDocId>
```

```
</soapenv:Body>

</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- "idAplicacion": Identificador de la aplicación que realiza la petición.
- "id_documento": Identificador del documento del cual se desea obtener su contenido.

4.10.2 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz
```

```
        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd
        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3
        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR
        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
 <ns1:GetDocumentContentByDocIdResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">
      <GetDocumentContentByDocIdReturn xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
    xsi:type="soapenc:string">
        <?xml version="1.0"?>
        <outputMessage  xmlns="http://afirmaws/ws/custody" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
        instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd ">
          <request>GetDocumentContentByDocId</request>
```

```
        <versionMsg>1.0 </versionMsg>
        <response>
          <Response>
            <status>[estado]</status>
            <description>[descripcion]</description>
            <document><![CDATA[documento]]></document>
          </Response>
        </response>
      </outputMessage>
    </GetDocumentContentByDocIdReturn>
 </ns1:GetDocumentContentByDocIdResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.
- "descripción": Contiene una descripción del error o excepción producido en el módulo.
- "documento": Contenido del documento, codificado en Base64, asociado al identificador de documento dado.

4.10.3 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
```

```
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
    message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
    x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

        1uLg9O8Bhhp3saZfk56Ta7CegbG5

    </wsse:BinarySecurityToken>

    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

        <ds:SignedInfo>

            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

```
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#binaryToken">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
        JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
        hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
        8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
    </ds:SignatureValue>
    <ds:KeyInfo>
        <wsse:SecurityTokenReference>
            <wsse:Reference URI="#binaryToken"/>
```

```
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1:GetDocumentContentByDocIdResponse xmlns:ns1="http://soapinterop.org/">
    <GetDocumentContentByDocIdReturn xsi:type="soapenc:string"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
        <?xml version="1.0" ?>
        <outputMessage  xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">
            <request>GetDocumentContentByDocId</request>
            <versionMsg>1.0</versionMsg>
            <response>
                <Exception>
                    <errorCode>[cod_error]</errorCode>
                    <description>[descripción error]</description>
                    <associatedException>[excepcion_asociada]</associatedException>
                <Exception>
            </response>
        </outputMessage>
    </GetDocumentContentByDocIdReturn>
    </ns1:GetDocumentContentByDocIdResponse>
</soapenv:Body>
```

```
</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.11 Módulo_Custodia. Obtener Identificador Documento.

Este servicio se considera "legacy" (obsoleto), y **no será evolucionado**. **Este servicio solo está disponible en el modelo federado**.

GetDocId devuelve, para un identificador de transacción de firma dado, el identificador del documento asociado a la misma codificado en Base 64.

4.11.1 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>

  <GetDocId xmlns="http://soapinterop.org/">

  <GetDocIdRequest xsi:type="xsd:string">

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

      <inputMessage xmlns="http://afirmaws/ws/custody" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">

            <request>GetDocId</request>

            <versionMsg>1.0</versionMsg>
```

```
            <parameters>
                <applicationId>[idAplicacion]</applicationId>
                <transactionId>[id_transaccion]</transactionId>
            </parameters>
        </inputMessage>
    </GetDocIdRequest>
    </GetDocId>
</soapenv:Body>
</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- "idAplicacion": Identificador de la aplicación que realiza la petición.
- "id_transaccion": Identificador de transacción de firma de la cual se desea obtener el identificador del documento.

4.11.2 Mensaje SOAP de respuesta OK.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3
```

DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

1uLg9O8Bhhp3saZfk56Ta7CegbG5

```
</wsse:BinarySecurityToken>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
```

```
<ns1:ObtenerIdDocumentoResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">

  <ObtenerIdDocumentoReturn xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
 xsi:type="soapenc:string">

    <?xml version="1.0"?>

    <outputMessage  xmlns="http://afirmaws/ws/custody" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd ">

      <request>ObtenerIdDocumento</request>

      <versionMsg>1.0 </versionMsg>

      <response>

        <Response>

          <status>[estado]</status>

          <description>[descripcion]</description>

          <documentId>[id_documento]</documentId>

        </Response>

      </response>

    </outputMessage>

  </GetDocIdReturn>

 </ns1:GetDocIdResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- "estado": Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.

- "descripción": Contiene una descripción del error o excepción producido en el módulo.
- "id_documento": Identificador del documento, codificado en Base64, asociado al identificador de transacción dado.

4.11.3 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn
```

```
        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf
        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
```

```
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh

            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI

            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=

        </ds:SignatureValue>

        <ds:KeyInfo>

            <wsse:SecurityTokenReference>

                <wsse:Reference URI="#binaryToken"/>

            </wsse:SecurityTokenReference>

        </ds:KeyInfo>

    </ds:Signature>

 </wsse:Security>

</soapenv:Header>

<soapenv:Body wsu:Id="body">

    <ns1:GetDocIdResponse xmlns:ns1="http://soapinterop.org/">

    <GetDocIdReturn xsi:type="soapenc:string" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">

        <?xml version="1.0" ?>

        <outputMessage  xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">

            <request>GetDocId</request>

            <versionMsg>1.0</versionMsg>

            <response>

                <Exception>

                    <errorCode>[cod_error]</errorCode>

                    <description>[descripción error]</description>
```

```
                    <associatedException>[excepcion_asociada]</associatedException>
                </Exception>
            </response>
        </outputMessage>
    </GetDocIdReturn>
    </ns1:GetDocIdResponse>
</soapenv:Body>
</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

4.12 Módulo_Custodia. Obtener Firma Transacción.

GetESignature permite obtener la firma electrónica, codificada en Base 64, asociada al identificador de transacción dado.

Este servicio se considera "legacy" (obsoleto), **no será evlucionado**, y se encuentra en proceso de discontinuación. **Este servicio solo está disponible en el modelo federado**.

4.12.1 Mensaje SOAP de petición.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Body>
```

```
<GetESignature xmlns="http://soapinterop.org/">
<GetESignatureRequest xsi:type="xsd:string">
<?xml version="1.0" encoding="UTF-8"?>
<inputMessage xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">
<request>GetESignature</request>
<versionMsg>1.0</versionMsg>
<parameters>
<applicationId>[idAplicacion]</applicationId>
<transactionId>[id_transaccion]</transactionId>
</parameters>
</inputMessage>
</GetESignatureRequest>
</GetESignature>
</soapenv:Body>
</soapenv:Envelope>
```

Cada uno de los parámetros enumerados se identifican con:

- “idAplicacion”: Identificador de la aplicación que realiza la petición.
- “id_transaccion”: Identificador de transacción cuya firma electrónica se desea obtener.

4.12.2 Mensaje SOAP de respuesta OK.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
```

```
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
    message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
    x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq

        1uLg9O8Bhhp3saZfk56Ta7CegbG5

    </wsse:BinarySecurityToken>

    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

        <ds:SignedInfo>

            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

```
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#body">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference URI="#binaryToken">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
        JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
        hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
        8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
    </ds:SignatureValue>
    <ds:KeyInfo>
        <wsse:SecurityTokenReference>
            <wsse:Reference URI="#binaryToken"/>
```

```
            </wsse:SecurityTokenReference>

        </ds:KeyInfo>

    </ds:Signature>

 </wsse:Security>

</soapenv:Header>

<soapenv:Body wsu:Id="body">

 <ns1:GetESignatureResponse soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:ns1="http://soapinterop.org/">

    <GetESignatureReturn xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
   xsi:type="soapenc:string">

      <?xml version="1.0"?>

      <outputMessage  xmlns="http://afirmaws/ws/custody" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
      instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd ">

        <request>GetESignature</request>

        <versionMsg>1.0 </versionMsg>

        <response>

          <Response>

            <status>[estado]</status>

            <description>[descripcion]</description>

            <eSignature><![CDATA[firma_electronica]]></eSignature>

            <eSignatureFormat>[formato_firma]</eSignatureFormat>

          </Response>

        </response>

      </outputMessage>

   </GetESignatureReturn>
```

```
 </ns1:GetESignatureResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los items enumerados en la respuesta se identifican con:

- “estado”: Valor booleano que indica si la operación ha sido satisfactoria o erronea, true o false respectivamente.
- “descripción”: Contiene una descripción del error o excepción producido en el módulo.
- “firma_electronica”: Contenido de la firma electrónica asociada al identificador de transacción solicitado, codificado en Base 64.
- “formato_firma”: Formato de la Firma Electronica asociada al identificador de transacción (PKCS7, CMS, CADES, CADES-BES, CADES-EPES, CADES-T, CADES-C, CADES-X1, CADES-X2, CADES-XL1, CADES-XL2, CADES-A XMLDSIG, XADES, XADES-BES, XADES-EPES, XADES-T, XADES-C, XADES-X1, XADES-X2, XADES-XL1, XADES-XL2, XADES-A, PDF, PADES, PADES-BES, PADES-EPES, PADES-LTV, ODF, CADES-B-LEVEL, CADES-T-LEVEL, CADES-LT-LEVEL, CADES-LTA-LEVEL, XADES-B-LEVEL, XADES-T-LEVEL, XADES-LT-LEVEL, XADES-LTA-LEVEL, PADES-B-LEVEL, PADES-T-LEVEL, PADES-LT-LEVEL, PADES-LTA-LEVEL).

4.12.3 Mensaje SOAP de respuesta Error.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <soapenv:Header>

  <wsse:Security soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next" soapenv:mustUnderstand="0">

    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="binaryToken">

        MIICsTCCAhqgAwIBAAIEQ8zySzANBgkqhkiG9w0BAQUFADCBnDEgMB4GCSqGSIb3

        DQEJARYRc29wb3J0ZS5ydEBtYXAuZXMxCzAJBgNVBAYTAkVTMQ8wDQYDVQQIEwZN

        YWRyaWQxDzANBgNVBAcTBk1hZHJpZDEMMAoGA1UEChMDTUFQMQwwCgYDVQQLEwNN

        QVAxLTArBgNVBAMTJHByZS1hZmlybWEucmVkaW50ZXJhZG1pbmlzdHJhdGl2YS5l

        czAeFw0wNjAxMTcxMzM0MDNaFw0zMzA2MDQxMzM0MDNaMIGcMSAwHgYJKoZIhvcN

        AQkBFhFzb3BvcnRlLnJ0QG1hcC5lczELMAkGA1UEBhMCRVMxDzANBgNVBAgTBk1h

        ZHJpZDEPMA0GA1UEBxMGTWFkcmlkMQwwCgYDVQQKEwNNQVAxDDAKBgNVBAsTA01B

        UDEtMCsGA1UEAxMkcHJlLWFmaXJtYS5yZWRpbnRlcmFkbWluaXN0cmF0aXZhLmVz

        MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpmDks3oqpTVhj69pu3gZtU3fd

        MLv2sEPW4yq5/DZb4nWhhufwwUKHJrBtDadJyCv6x9sUaJEQMI9fyiP3br4t3So3

        VC2+ki3ouUqAM7R1oWd0qbxn7xZ4qN5UvwgSGbJLmT9omi8CqeIAAecJt/Jhd3CR

        MMknvDg2TKiH9Y2j2wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAH12TSqTvkyY8Odn

        Ervl6814griyxw+DkLcYXQN3L2/0OTZTV/wUElsar2KzGacmTQykH3zQeyt4hOMf

        FX3A6cMuLyVzgc4Eoo6B3hGeRuaUoa92OxbwX79iBcYoIFGgxmgPrQUi1dHeuxQq
```

```
        1uLg9O8Bhhp3saZfk56Ta7CegbG5
    </wsse:BinarySecurityToken>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#body">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>51LC9KDsVLdge5sl+mnShoSsmXY=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#binaryToken">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VqClygkINsFb33W6zo4tH7fN/xY=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            JVojJiGr7UJWMF7x9Y9Wlxv8jpkaQwWvOwfwvQo1h7zzxtYE8NIMgD5mTvk4z5eh
            hoHJShgavYAgw9POW0Sq0LHyLFvrXeAwX9banNDTfJg0l6ev9izAl+xsli+pGHXI
```

```
            8jhwrjzF0hZXwqUwRrM1oybBKdftN+tW0yzxoGGlaWA=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <wsse:SecurityTokenReference>
                <wsse:Reference URI="#binaryToken"/>
            </wsse:SecurityTokenReference>
        </ds:KeyInfo>
    </ds:Signature>
 </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
    <ns1:GetESignatureResponse xmlns:ns1="http://soapinterop.org/">
    <GetESignatureReturn xsi:type="soapenc:string" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
            <?xml version="1.0" ?>
            <outputMessage  xmlns=”http://afirmaws/ws/custody” xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:SchemaLocation="https://localhost/afirmaws/xsd/mcustodia/wseng.xsd">
                <request>GetESignature</request>
                <versionMsg>1.0</versionMsg>
                <response>
                    <Exception>
                        <errorCode>[cod_error]</errorCode>
                        <description>[descripción error]</description>
                        <associatedException>[excepcion_asociada]</associatedException>
                    <Exception>
```

```
                </response>

            </outputMessage>

        </GetESignatureReturn>

        </ns1:GetESignatureResponse>

</soapenv:Body>

</soapenv:Envelope>
```

Los item enumerados en la respuesta se identifican con:

- "cod_error": código de error.
- "descripcion": descripción del error.
- "excepcion_asociada": Excepción que ha provocado el error.

5 Integración vía OCSP Responder

El servicio OCSP (Online Certificate Status Protocol), permite comprobar el estado de revocación de cualquier tipo de certificado X509, incluido e-DNI, de forma online. En una misma petición se podrán especificar más de un certificado a validar siempre y cuando éstos sean del mismo Prestador de Servicios de Certificación. Al igual que un Servicio Web, el servicio de obtención del estado de un certificado online, responde ante una petición OCSP válida. Dicha petición se deberá realizar a la url de publicación del servicio. Al ser el servicio OCSP estándar se puede usar cualquier cliente OCSP (también estándar).

El servicio OCSP se encuentra publicado, dependiendo del entorno, en las siguientes url:

- Desarrollo: http://des-afirma.redsara.es
- Producción: http://afirma.redsara.es

Por defecto la plataforma no requiere peticiones firmadas, pero como mecanismo de autorización de cara al servicio OCSP, puede requerir a las aplicaciones cliente que las peticiones OCSP vayan firmadas. También puede requerir que el campo '*requestorName*' incluido en la petición deba tener un valor concreto independientemente del hecho de que la petición vaya firmada o no. En dicho campo, se especificará un identificador de aplicación dado de alta en la plataforma, con el formato: [UNIDAD_ORGANIZATIVA].[ID_APLICACION].

Ante una petición OCSP, la plataforma devolverá el estado del certificado como una respuesta firmada haciendo uso del certificado público de la misma. Para ello es necesario que se confíe en el certificado público suministrado en el "Área de Descargas" de la solución "Plataforma de validación de firma electrónica @firma" en el PAe (hay que identificarse como usuario):

https://administracionelectronica.gob.es/ctt/afirma/descargas → Documentación y Kit de certificados → Certificados utilizados por @firma.

ANEXO

A.1 Sintaxis del XML de solicitud y respuesta

Un fichero XML está asociado a un XSchema que permite definir la sintaxis correcta que ha de cumplir el mismo para ser un documento XML válido. Es por ello que a continuación se muestra el XSchema general que han de cumplir los XML especificados como parámetros de entrada y salida asociados a cada servicio web.

A.1.1 XSchema de web services para los WS de Validación

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mvalidacion /wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mvalidacion /wseng.xsd

Todos los servicios web comparten como estructura común de entrada el XSchema anteriormente expuesto. En el distinguimos los siguientes elementos:

- **request**, string que coincidirá con el método de la plataforma que implementará el servicio web solicitado.

- **versionMsg**, de cara a facilitar futuras modificaciones de funcionalidad de la plataforma que requieran un cambio en la información proporcionada a un servicio web, los mensajes se encuentran versionados. Este campo indicará, por tanto, la versión de la información asociada a la petición realizada, por ejemplo 1.0.

- **parameters**, secuencia de elementos necesarios para realizar la petición asociada al servicio web. Por tanto, esta secuencia de parámetros variará en función del servicio web.

Ante una petición de servicio, la plataforma devolverá la información requerida en el mismo. Para ello el XML de respuesta comparte como estructura común para los servicios web. En el distinguimos los siguientes elementos:

- **request**, string que coincidirá con el método de la plataforma que implementará el servicio web solicitado y cuya información resultante concluye en la respuesta de dicho servicio.

- **versionMsg**, de cara a facilitar futuras modificaciones de funcionalidad de la plataforma que requieran un cambio en la información de respuesta proporcionada por un servicio web, los mensajes se encuentran versionados. Este campo indicará, por tanto, la versión de la información de respuesta asociado al servicio web, por ejemplo 1.0.

- **response**, secuencia de elementos que conforman la respuesta dada por un servicio web.

A.1.2 XSchema de web services para los WS de Firma

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

En el entorno de Desarrollo: https://des-afirma.redsara.es/afirmaws/xsd/ mfirma/wseng.xsd

En el entorno de Producción: https://afirma.redsara.es/afirmaws/xsd/mfirma/wseng.xsd

Todos los servicios web comparten como estructura común de entrada el XSchema anteriormente expuesto. En el distinguimos los siguientes elementos:

- **request**, string que coincidirá con el método de la plataforma que implementará el servicio web solicitado.

- **versionMsg**, de cara a facilitar futuras modificaciones de funcionalidad de la plataforma que requieran un cambio en la información proporcionada a un servicio web, los mensajes se encuentran versionados. Este campo indicará, por tanto, la versión de la información asociada a la petición realizada, por ejemplo 1.0.

- **parameters**, secuencia de elementos necesarios para realizar la petición asociada al servicio web. Por tanto, esta secuencia de parámetros variará en función del servicio web.

Ante una petición de servicio, la plataforma devolverá la información requerida en el mismo. Para ello el XML de respuesta comparte como estructura común para los servicios web. En el distinguimos los siguientes elementos:

- **request**, string que coincidirá con el método de la plataforma que implementará el servicio web solicitado y cuya información resultante concluye en la respuesta de dicho servicio.

- **versionMsg**, de cara a facilitar futuras modificaciones de funcionalidad de la plataforma que requieran un cambio en la información de respuesta proporcionada por un servicio web, los mensajes se encuentran versionados. Este campo indicará, por tanto, la versión de la información de respuesta asociado al servicio web, por ejemplo 1.0.

- **response**, secuencia de elementos que conforman la respuesta dada por un servicio web.

A.1.3 XSchema de web services para los WS de Custodia

Los XML SCHEMA (XSD) que definen los mensajes de petición y respuesta se pueden encontrar en las siguientes ubicaciones:

- En el entorno de Desarrolloen la url:

  https://des-afirma.redsara.es/afirmaws/xsd/mcustodia /wseng.xsd

- En el entorno de Producción en la url:

  https://afirma.redsara.es/afirmaws/xsd/mcustodia/wseng.xsd

Todos los servicios web comparten como estructura común de entrada el XSchema anteriormente expuesto. En el distinguimos los siguientes elementos:

- **request**, string que coincidirá con el método de la plataforma que implementará el servicio web solicitado.

- **versionMsg**, de cara a facilitar futuras modificaciones de funcionalidad de la plataforma que requieran un cambio en la información proporcionada a un servicio web, los mensajes se encuentran versionados. Este campo indicará, por tanto, la versión de la información asociada a la petición realizada, por ejemplo 1.0.

- **parameters**, secuencia de elementos necesarios para realizar la petición asociada al servicio web. Por tanto, esta secuencia de parámetros variará en función del servicio web.

Ante una petición de servicio, la plataforma devolverá la información requerida en el mismo. Para ello el XML de respuesta comparte como estructura común para los servicios web. En el distinguimos los siguientes elementos:

- **request**, string que coincidirá con el método de la plataforma que implementará el servicio web solicitado y cuya información resultante concluye en la respuesta de dicho servicio.

- **versionMsg**, de cara a facilitar futuras modificaciones de funcionalidad de la plataforma que requieran un cambio en la información de respuesta proporcionada por un servicio web, los

mensajes se encuentran versionados. Este campo indicará, por tanto, la versión de la información de respuesta asociado al servicio web, por ejemplo 1.0.

- **response**, secuencia de elementos que conforman la respuesta dada por un servicio web.

A.1.4 XSchema del perfil XSS de @Firma

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" targetNamespace="urn:afirma:dss:1.0:profile:XSS:schema"
elementFormDefault="qualified">
	<xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
	<!-- Elemento que contiene información adicional del proceso de verificación -->
	<xs:element name="AdditionalDetails">
		<xs:complexType>
			<xs:sequence>
				<xs:element name="SignerDetails" type="afxp:SignerDetailsType"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>

	<!-- Elemento que contiene la información del firmante y del TST -->
	<xs:complexType name="SignerDetailsType">
		<xs:sequence>
			<xs:element ref="afxp:X509SignerIdentity"/>
			<xs:element name="timeStamp" type="xs:dateTime"/>
			<xs:element ref="afxp:TSASignerIdentity"/>
		</xs:sequence>
	</xs:complexType>

	<!-- Elemento que contiene el certificado firmante -->
	<xs:element name="X509SignerIdentity">
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="ds:X509Data"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>

	<!-- Elemento que contiene el certificado del firmante objetivo-->
	<xs:element name="TargetSigner">
```

```
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="ds:X509Data"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>
	<!-- Elemento que contiene el certificado de la TSA -->
	<xs:element name="TSASignerIdentity">
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="ds:X509Data"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>
	<!-- Elemento identificador de transacción -->
	<xs:element name="TransactionId" type="xs:string"/>
	<!-- Elemento identificador de referencia -->
	<xs:element name="ReferenceId" type="xs:string"/>
	<!-- Identificador del algoritmo de hash-->
	<xs:element name="HashAlgorithm">
		<xs:simpleType>
			<xs:restriction base="xs:string">
				<xs:enumeration value="MD2"/>
				<xs:enumeration value="MD5"/>
				<xs:enumeration value="SHA"/>
				<xs:enumeration value="SHA1"/>
				<xs:enumeration value="SHA256"/>
				<xs:enumeration value="SHA384"/>
				<xs:enumeration value="SHA512"/>
			</xs:restriction>
		</xs:simpleType>
	</xs:element>
	<!-- InformaciÃ³n adicional del documento -->
	<xs:element name="AdditionalDocumentInfo">
		<xs:complexType>
			<xs:sequence>
				<xs:element name="DocumentName" type="xs:string"/>
				<xs:element name="DocumentType" type="xs:string"/>
			</xs:sequence>
			<xs:attribute name="WhichDocument" type="xs:IDREF"/>
		</xs:complexType>
	</xs:element>
```

```
        <!-- Modo de actualización de firma-->
        <xs:element name="UpdatedSignatureMode" type="xs:anyURI"/>

        <!-- Modo de firma en formato XML -->
        <xs:element name="XMLSignatureMode" type="xs:anyURI"/>
</xs:schema>
```

A.1.5 XSchema del perfil Archive de @Firma

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:afap="urn:afirma:dss:1.0:profile:archive:schema"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema" xmlns:xssp="urn:oasis:names:tc:dss:1.0:profiles:XSS"
xmlns:afxp="urn:afirma:dss:1.0:profile:XSS:schema" targetNamespace="urn:afirma:dss:1.0:profile:archive:schema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
        <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
        <xs:import namespace="urn:oasis:names:tc:dss:1.0:core:schema" schemaLocation="http://docs.oasis-
open.org/dss/v1.0/oasis-dss-core-schema-v1.0-os.xsd"/>
        <xs:import namespace="urn:afirma:dss:1.0:profile:XSS:schema" schemaLocation="afirma-dss-1.0-profiles-
XSS-schema.xsd"/>
        <xs:import namespace="urn:oasis:names:tc:dss:1.0:profiles:XSS" schemaLocation="oasis-dss-1.0-profiles-
XSS-schema-wd02.xsd"/>
        <!-- Información adicional de la firma -->
        <xs:element name="AditionalSignatureInfo">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element ref="dss:Document"/>
                                <xs:element ref="ds:X509Data"/>
                                <xs:element ref="afxp:ReferenceId"/>
                                <xs:element ref="dss:SignatureType"/>
                                <xs:element ref="xssp:SignatureForm"/>
                                <xs:element ref="afxp:HashAlgorithm"/>
                                <xs:element name="StoreDocument" type="xs:boolean"/>
                        </xs:sequence>
                </xs:complexType>
        </xs:element>
        <!-- información adicional de archivo -->
        <xs:element name="AditionalArchiveInfo">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="DocumentId" type="xs:string"/>
```

```
                                        <xs:element name="EvidenceOfESignature"
type="afap:EvidenceOfESignatureType"/>
                                </xs:sequence>
                        </xs:complexType>
                </xs:element>
                <xs:complexType name="EvidenceOfESignatureType">
                        <xs:sequence>
                                <xs:element ref="dss:SignatureObject"/>
                        </xs:sequence>
                </xs:complexType>
</xs:schema>
```

A.2 Códigos de resultado devueltos por la plataforma

A continuación, mostramos la relación de códigos que devuelve la plataforma.

A.2.1 Códigos resultado.

Validación

0	Certificado OK
1	El certificado no pasó la validación
2	La cadena de certificación no es correcta
3	El certificado está revocado
4	No se ha podido determinar el estado del Certificado

Validación cadena de certificación

0	Cadena de certificación OK
1	Modo de validación de cadena no válido
2	La cadena está formada por certificados que no pertenecen a la misma
3	Un certificado de la cadena no pasó la validación
4	No se ha podido determinar el estado de la cadena

Validación simple

0	Validación Satisfactoria
1	Certificado caducado
2	Certificado aún no válido
3	Firma no válida

4	El emisor del certificado no es de confianza o no se encuentra registrado
5	El certificado posee extensiones que no son válidas
10	El certificado no posee la extensión crítica “id-kp-timestamping”

Verificación del estado

0	Estado Certificado OK
1	Certificado REVOCADO
2	Certificado EN OBSERVACION
3	No se ha podido determinar el estado del Certificado
4	El Certificado ha sido elminado de la CRL

A.2.2 Códigos de error.

A continuación, se muestra una relación de códigos de error devueltos por la plataforma junto con una descripción genérica del motivo que causó el error. En aquellos errores en los que sea necesario, la plataforma especificará la causa concreta del problema mediante un mensaje más detallado.

Genéricos

COD_000	Error no esperado.
COD_152	Error inicializando el TreeCache.
COD_153	El TreeCache no puede ser detenido al no haberse inicializado correctamente.
COD_154	Error manejando algún objeto en el TreeCache.
COD_155	El path indicado para almacenar un objeto en el TreeCache está mal formado.
COD_178	Error durante el acceso o escritura en el esquema del modulo de eventos de alarmas de la BBDD.

Web Services

COD_001	Error en parámetros de entrada de WebServices.
COD_117	Error obtenido en el proceso de autorización de una aplicación mediante un Servicio

	Web.
COD_179	Error durante el procesamiento de la cabecera de seguridad.
COD_189	El servicio no está autorizado para la aplicación indicada.

Validación

COD_024	Certificado con extensiones inválidas.
COD_025	La firma del certificado no es válida.
COD_045	Tipo de certificado no soportado.
COD_046	Implementación de método de verificación no existente.
COD_047	Error en validación OCSP. No existe el algoritmo de hash.
COD_048	Error en envio de petición OCSP.
COD_049	Error al validar el certificado firmante de la respuesta OCSP.
COD_050	Error en la respuesta OCSP, no contiene extensión ExtendedKeyUsage, o no se confía en el responder.
COD_053	Error en la respuesta OCSP, identificadores de envío de respuesta no coinciden.
COD_054	Error en la respuesta OCSP, intervalo de confianza sobrepasado.
COD_055	Respuesta OCSP errónea.
COD_056	Error al acceder al prestador para obtener la respuesta OCSP.
COD_057	Error al validar estado del certificado.
COD_058	Error al obtener info del certificado.
COD_060	Error al validar la CRL.
COD_061	No se ha podido obtener la CRL.

COD_062	Error relacionado con la configuración de una aplicación.
COD_063	El tipo de certificado a validar se encuentra deshabilitado para la politica especificada.
COD_064	El tipo de certificado a validar se encuentra deshabilitado.
COD_065	El emisor del certificado se encuentra dado de baja o revocado en el sistema.
COD_066	El certificado a validar no es soportado por el sistema.
COD_080	Certificado de prestador revocado.
COD_083	Error interno en el servidor afirma al realizar una validación.
COD_156	Error al manejar una CRL en el TreeCache.
COD_173	Error procesando la respuesta del servicio de validación histórica.
COD_174	El prestador no existe en la política o está deshabilitado.
COD_180	No existe la política especificada o no hay políticas definidas en el sistema.
COD_187	Error gestionando una TSL.

Administración

COD_177	Error durante la gestión de las alarmas configuradas en la plataforma.
COD_186	Error manejando un objeto de configuración de la plataforma.
COD_191	No se ha podido acceder al caché de configuración.

Firma

COD_084	Error en la generación de la Firma Electrónica del fichero de registro de Eventos.
COD_085	Error en el proceso de firmado de las tramas OCSPResponse.
COD_086	Error en la generación de la Firma Electrónica de la respuesta SOAP de la plataforma.

COD_087	Error en la generación de la Firma Electrónica Servidor.
COD_088	Error en la generación de la Firma Electrónica Servidor cosign.
COD_089	Error en la generación de la Firma Electrónica Servidor countersign.
COD_090	Error en la generación de la Firma Electrónica Servidor countersign específico.
COD_091	Error en la autorización de la aplicación para la generación de Firma Servidor con un certificado servidor concreto.
COD_103	Error en la Validación de Firma Electrónica.
COD_157	Error al realizar la actualización de una firma.
COD_159	La firma a actualizar no es valida.
COD_160	No se ha suministrado el formato al que actualizar la firma.
COD_162	No se detectó el formato de la firma entrante al ser nula.
COD_163	No se puede crear un detector PDF para la firma de entrada. Debe contener objetos PdfPKCS7.
COD_164	No se puede crear un detector ODF para la firma de entrada. Debe contener firmas XMLDSIG.
COD_165	No se puede crear un detector ASN.1 para la firma de entrada. Debe ser un objeto ASN.1.
COD_166	No se puede crear un detector XML para la firma de entrada. Debe ser un documento XML.
COD_167	No se puede crear un detector S/MIME para la firma de entrada. Debe ser un mensaje MIME.
COD_168	Error de lectura en la firma de entrada para crear el detector.
COD_169	No se puede crear un detector de formatos específico. Tipo de firma no reconocido.
COD_170	Error creando un detector explícitamente. El tipo de firma no puede ser nulo.

COD_171	Error creando un detector ESPECÍFICO. La firma de entrada no es del tipo ESPECÍFICO.
COD_172	No se puede crear un detector para el tipo de firma ESPECÍFICO. No es un tipo de firma soportado.

Custodia

COD_076	Error al almacenar una CRL.
COD_106	Error almacenando la información del documento en Custodia.
COD_107	Error eliminando en contenido del documento en Custodia.
COD_108	Error obteniendo el identificador del documento de Custodia.
COD_109	Error obteniendo el contenido del documento de Custodia a partir de su identificador.
COD_110	Error obteniendo el contenido del documento de Custodia a partir del identificador de transacción.
COD_111	Error actualizando la firma almacenada en Custodia.
COD_112	Error actualizando el hash de un documento en Custodia.
COD_113	Error obteniendo el hash de un documento de Custodia.
COD_114	Error obteniendo una firma de Custodia.
COD_115	Error obteniendo la Firma Electrónica de Custodia de una aplicación concreta.
COD_116	Error obteniendo el formato de la firma.
COD_118	Error almacenando una firma electrónica.
COD_158	Error al custodiar la firma en procesos upgrade.
COD_178	Error leyendo o escribiendo en el esquema de eventos de alarmas.

Almacenes de Claves

COD_190	No se ha podido acceder al caché de keystores.

Políticas de Firma

COD_181	No se ha podido acceder al caché de políticas de firma.

Tareas

COD_184	Error gestionando un scheduler.
COD_185	Error gestionando una tarea.

Administración Delegada

COD_188	Error mientras se realizaban operaciones relacionadas con la administración delegada.

SNI

COD_192	Error al realizar la conexión SSL + SNI.

A.3 Integración con la plataforma mediante de Web Services – WSS

@firma incorpora el estándar de OASIS Web Service Security v1.1 de 1 de Febrero de 2006. Esta especificación permite incorporar mecanismos de protección a la mensajería de servicios web. Algunas de las amenazas implícitas en los servicios web podrían ser:

- El contenido de los mensajes podría ser interceptado, leído y modificado en tránsito por un tercero.
- Se podrían enviar mensajes a un servicio, suplantando la identidad de un tercero, en aquellos casos en los que el servicio carezca de determinadas medidas de seguridad referentes a la autenticación de las partes.

WSS define un formato de mensajería basado en SOAP que permite reducir considerablemente estas amenazas mediante el uso de tokens de seguridad combinados con firmas digitales para proteger y autenticar los mensajes SOAP.

Se remite al lector a la especificación de OASIS-WSS para más información:

> http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

Las aplicaciones dadas de alta en la plataforma tienen configurado un nivel de securización que deberán cumplir en cada una de las peticiones realizadas. Este podrá ser:

- Sin securizar, para el cual las peticiones XMLSOAP se definen sin ningún tipo de cabecera de seguridad.
- Securizadas mediante usuario/password. Dicho usuario tendrá que estar dado de alta en la plataforma para esa aplicación. En la petición XMLSOAP se tendrá que usar la cabecera de seguridad UsernameToken, pudiendo la password estar o no hasheada.

  Este token de seguridad permite la incorporación de dos parámetros wsse:Nonce, que especifica un número aleatorio generado por el cliente, y wsu:Created, que indica cuando fue creada la petición. Ambos parámetros facilitan la identificación del mensaje SOAP en un posible ataque por repetición.
- Securizadas mediante Firma Electrónica XMLDSIG. La petición XMLSOAP deberá estar firmada con un certificado dado en la plataforma para dicha aplicación.

Este procedimiento exige la incorporación de dos elementos dentro del ítem wsse:Security. Estos elementos son:

- BinarySecurityToken. Incorpora información relacionada con el firmante de la petición SOAP. En concreto se incluirá el certificado X.509v3 codificado en Base64. El certificado se usará para la identificación de la aplicación cliente, por lo que se considera obligatorio su inclusión para peticiones securizadas mediante firma electrónica. Este elemento posee 3 atributos:
  - wsu:Id. Cadena de texto que identifica el BinarySecurityToken y que posteriormente permitirá su referencia dentro de la firma electrónica de la petición.
  - EncodingType. Se identificará la codificación del certificado incluido en el objeto. En nuestro caso será Base64 por lo que se incluirá la referencia *http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary*.
  - ValueType. Especifica el tipo de certificado incluido. @Firma sólo acepta la inclusión de certificados X.509v3 por lo que se incluirá la referencia *http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3*
- Signature. Incluye la firma electrónica en formato XMLDSIG de la petición. Dicha firma electrónica deberá incluir obligatoriamenteen sus referencias el cuerpo de la petición (elemento Body), siendo recomendado incluir también una referencia al certificado firmante, bien a partir del KeyInfo o bien directamente desde el BinarySecurityToken.

  WS-Security permite varios modos para referenciar el certificado firmante en la firma electrónica, quedando a criterio de la aplicación cliente la elección de uno específico.

Además, WSS permite la inclusión de los sellos de tiempo que mitigan el riesgo de replicar un mensaje enviado por un usuario malintencionado. De esta forma **se recomienda incluir en el tag Security el elemento Timestamp** para permitir especificar los elementos:

- ***Created***. Cúando fue creado la petición web.
- ***Expires***. Tiempo máximo de vida (caducidad) en la que se podrá atender a dicha petición. Altamente recomendado.

La presencia del elemento Timestamp y Expires, garantiza que la plataforma no aceptará peticiones securizadas en un momento posterior a su caducidad.

A continuación, mostramos un ejemplo de petición XMLSOAP securizadas mediante usuario/password y mediante Firma Electrónica XMLDSIG, respectivamente.

Ejemplo de securización mediante Usuario/Password.

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Header>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">

    <wsse:UsernameToken wsu:Id="UsernameToken-6330713" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    <wsse:Username>prueba</wsse:Username>

        <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-
1.0#PasswordDigest">          LiP3J84wKHpA6sMOu2BVVZRGYSY=

        </wsse:Password>

        <wsse:Nonce>lckJBnhGHAj4EGG3YuGXmg==</wsse:Nonce>

        <wsu:Created>2006-07-26T15:16:00.925Z</wsu:Created>

    </wsse:UsernameToken>

</wsse:Security>

</soapenv:Header>

<soapenv:Body>

    <ValidateCertificate xmlns="http://soapinterop.org/">

    < ValidateCertificate Request xsi:type="xsd:string" xmlns="">

        [XML de entrada]

    </V ValidateCertificate Request>
```

```
    </ ValidateCertificate >

</soapenv:Body>

</soapenv:Envelope>
```

Ejemplo de securización mediante Firma Electrónica

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

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<soapenv:Header>

    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">

        <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary"      ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3" wsu:Id="CertId-64011711"      xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
    MIIHKDCCBhCgAwIBAgIQNBvNb3XUFW1DaeCVPLrlPDANBgkqhkiG9w0BAQUFADCB1jELMAkGA1UEBhMCRVMxD
zANBgNVBAcTBk1hZHJpZDEgMB4GCSqGSIb3
    DQEJARYRYWNAYWNhYm9nYWNpYS5vcmcxNjA0BgNVBAoTLUNvbnNlam8gR2VuZXJhbCBkZSBsYSBBYm9nYWNp
YSBOSUY6US0yODYzMDA2STEyMDAGA
    1UECxMpQXV0b3JpZGFkIGRlIENlcnRpZmljYWNpb24gZGUgbGEgQWJvZ2FjaWExKDAmBgNVBAMTH0FDQSAtIENlc
nRpZmljYWRvcyBDb3Jwb3JhdGl2b3MwHhcN
    MDUxMTAzMDk1NTI2WhcNMDgxMTAzMDk1NTI2WjCCAQoxEjAQBgNVBAUTCTEyMzQ1Njc4WjEQMA4GA1UEDB
MHQWJvZ2FkbzEPMA0GA1UECBMGTWFkcmlkMQ
    swCQYDVQQGEwJFUzE+MDwGA1UEChQ1Q29uc2VqbyBHZW5lcmFsIGRlIGxhIEFib2dhY+
    1hIEVzcGHxb2xhIC8gQ0dBRSAvIDIwMDAxGDAWBgNVBAsTDzI4MDA0IC8gOTk5OTk5OTE3MDUGA1UEAxQuTk9N
QlJFIFBS2kVCQSBQUlVF0UEgQ09MRUdJQUR
    PIC0gTklGIDEyMzQ1Njc4WjExMC8GCSqGSIb3DQEJARYiZGVtby5lbXBsZWFkb0BjZ2FlLnJlZGFib2dhY2lhLm9yZzCBnz
ANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgY
    EAr+9Yys77Kj2nSTzbKIGddNvH2gI5REWD4mP4CIzdGu/y5dCcaFA/4jk759dLxQ/BgJK4dovjScdriV358PRNmnLwz87
FgXKEQkp1Z6ViGjNp+QvMegOENrrX+
    4VKbBejFxWk/LVdL9252cpcYGrUygTHa3qwBjuKzv9zeZxrxDECAwEAAaOCAz0wggM5MDcGA1UdEgQwMC6BEWFj
QGFjYWJvZ2FjaWEub3JnhhlodHRwOi8vd3
    d3LmFjYWJvZ2FjaWEub3JnMC0GA1UdEQQmMCSBImRlbW8uZW1wbGVhZG9AY2dhZS5yZWRhYm9nYWNpYS5vc
mcwDAYDVR0TAQH/BAIwADAOBgNVHQ8B
    Af8EBAMCA/gwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMBEGCWCGSAGG+EIBAQQEAwIFoDAsBgl
ghkgBhvhCAQgEHxYdaHR0cDovL3d3dy5
```

hY2Fib2dhY2lhLm9yZy9kb2MwYgYJYIZIAYb4QgENBFUWU0VzdGUgZXMgdW4gY2VydGlmaWNhZG8gcGVyc29uYWwgcmVjb25vY2lkby4gQ29uc3VsdGUgIGh
0dHA6Ly93d3cuYWNhYm9nYWNpYS5vcmcvZG9jMB0GA1UdDgQWBBTMEMwjtUi13eRrb/8nZawkq7wlXTAfBgNVHSMEGDAWgBRaeUyhDPwIFizChUVPMqvnK0
XAETCBrAYDVR0gBIGkMIGhMIGeBgsrBgEEAYGBFQoCATCBjjApBggrBgEFBQcCARYdaHR0cDovL3d3dy5hY2Fib2dhY2lhLm9yZy9kb2MwYQYIKwYBBQUHAgIw
VRpTRXN0ZSBlcyB1biBjZXJ0aWZpY2FkbyBwZXJzb25hbCByZWNvbm9jaWRvLiBDb25zdWx0ZSAgaHR0cDovL3d3dy5hY2Fib2dhY2lhLm9yZy9kb2MwVgYIKwY
BBQUHAQEESjBIMEYGCCsGAQUFBzAChjpodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2NlcnRpZmljYWRvcy9BQ0Fjb3Jwb3JhdGl2b3MuY3J0MC8GCCsGAQUFB
wEDBCMwITAIBgYEAI5GAQEwFQYGBACORgECMAsTA0VVUgIBBgIBBDB1BgNVHR8EbjBsMGqgaKBmhjFodHRwOi8vd3d3LmFjYWJvZ2FjaWEub3JnL2NybC9BQ
0Fjb3Jwb3JhdGl2b3MuY3JshjFodHRwOi8vY3JsLmFjYWJvZ2FjaWEub3JnL2NybC9BQ0Fjb3Jwb3JhdGl2b3MuY3JsMA0GCSqGSIb3DQEBBQUAA4IBAQAuh0A4tK/
AWEOaA3WwOyMPA8RNqlSV3HbXt2ghc4CsxRLQXa0R4Fz8o2qG+Euv+3PBlVWwnWXe3
+v1MGyajLD8m5Ce+P9wEA5KZVLUQzE9Z89Ugqj9dTeghpnWtqzKbbQG+IEgh9jzneQxDWnFYxG8IGrcoefB9Bg2S7I
HfnMHOitEm5Up1KdaCnYYBsOYZ+KdE/u/SrR
EhAzBZns1OaLWpHgFrG50IwAN34ODWi3kjlavNxpn4wlEBERCSlcE12IRYNLb9M0iYLJj5qTHuFfojW5
+ZA6HAX2swUK76iqxbwXOdduN6eF8lyTUxJBN6ZsM3UCctknvWYk615Y7Y3CF

```
        </wsse:BinarySecurityToken>

        <ds:Signature Id="Signature-11733267" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

            <ds:SignedInfo>

            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

            <ds:Reference URI="#id-31637242">

                <ds:Transforms>

                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

                </ds:Transforms>

                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

                <ds:DigestValue>W3KSrZ2+zMXRSTpiKiqb9LeerMw=</ds:DigestValue>

            </ds:Reference>
```

```
            </ds:SignedInfo>

            <ds:SignatureValue>

            m+XwtcTVDG+HquLNZC4w0kADjuzzZoY8MFm8iYNBSpOEG5YK+lzywfhKyL+VapXuSS3twmtX8bgK

            dKFEry+tCNnlvYJFjNWKRvHgnia0SPKCFrn96R6Kc1HPbkLAOdTi7q3RyWuvzruJa8opvJtIzXgc

            fegSET4ya35zJEjWXgY=

            </ds:SignatureValue>

            <ds:KeyInfo Id="KeyId-1635615">

                <wsse:SecurityTokenReference wsu:Id="STRId-8703610" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-  utility-  1.0.xsd">

                    <wsse:Reference URI="#CertId-64011711" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0       #X509v3"/>
    </wsse:SecurityTokenReference>

            </ds:KeyInfo>

        </ds:Signature>

    </wsse:Security>

    </soapenv:Header>

        <soapenv:Body>

        <ValidateCertificate xmlns="http://soapinterop.org/">

            <ValidateCertificateRequest xsi:type="xsd:string" xmlns="">

                [XML Entrada]

            </ ValidateCertificateRequest>

        </ ValidateCertificate>

    </soapenv:Body>

</soapenv:Envelope>
```

A continuación mostramos un ejemplo de cliente Web Service con axis, que invocará al servicio web indicado en el point, haciendo uso del nivel de securización indicado en la constante **security.mode** del fichero securityConfiguration.properties.

TestClient.java

```
/**
 * <p>Fichero: TestClient.java</p>
 * <p>Descripción: </p>
 * <p>Empresa: Telvent Interactiva </p>
 * <p>Fecha creación: 26-jul-2006</p>
 * @author SERYS
 * @version 1.0
*/

import java.io.BufferedReader;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileReader;
import java.io.IOException;
import java.net.URL;
import java.util.Properties;

import javax.xml.namespace.QName;

import org.apache.axis.client.Call;
```

```
import org.apache.axis.client.Service;

import org.apache.axis.constants.Use;

import org.apache.log4j.Logger;



import com.telventi.afirma.Excepcion;

import com.telventi.afirma.IExcepcion;



import wss4j.ClientHandler;



public class TestClient

{

  private static final Logger logger= Logger.getLogger(TestClient.class);



  private static final String CABECERA_ERROR="[TestClient]:";



  //Ruta donde se encuentran los ficheros de entrada a los servicios web

  private static final String RUTA_XML_ENTRADA= "webservices.rutaXml";



  //Fichero xml de entrada para el servicio web GetInfoCertificate

  private static final String XML_ENTRADA_GETINFOCERTIFICATE= "webservices.GetInfoCertificate";



  //Fichero xml de entrada para el servicio web ValidarCertificado

  private static final String XML_ENTRADA_VALIDARCERTIFICADO= "webservices.ValidateCertificate";
```

```
// Timeout configurado para las llamadas a los servicios Web
private static int TIMER;

private static Properties configuration = null;

private static Properties prop = null;

static
{
    // Carga del fichero de configuración
    configuration = new Properties();
    try
    {
        URL url =  ClassLoader.getSystemResource("securityConfiguration.properties");
        configuration.load(new FileInputStream(new File(url.getFile())));
        TIMER = Integer.parseInt(configuration.getProperty("timer"));
    }
    catch (Exception e)
    {
        System.err.println("Error cargando el fichero de properties securityConfiguration.properties");
        System.exit(-1);
    }
    prop = new Properties();
    try {
```

```
                prop.load(TestClient.class.getResourceAsStream("webservices.properties"));
        } catch(IOException e){
                System.err.println("Error cargando el fichero de properties webServices.properties");
                System.exit(-1);
        }
    }
public static void main(String [] args) {
    ClientHandler sender = null;
    try {
        String ruta_trusted_cacerts= "c:/truststoreWS.jks";

        System.setProperty("javax.net.ssl.trustStore",ruta_trusted_cacerts);

        //se pasará como argumentos el nombre del servicio web a invocar.
        String webService = args[0];
        String endpoint =”https://localhost/afirmaws/services/“ + webService;

        // Creacion del manejador que securizará la petición SOAP
        sender = new ClientHandler(configuration);

        Service  service = new Service();
        Call     call    = (Call) service.createCall();

        call.setTargetEndpointAddress( new java.net.URL(endpoint) );
```

```
call.setOperationName(new QName("http://soapinterop.org/", webService) );

call.setOperationUse(Use.LITERAL);

call.setTimeout(new Integer(TIMER));

call.setClientHandlers(sender, null);


long requestTime = System.currentTimeMillis();


String rutaXML= prop.getProperty(TestClient.RUTA_XML_ENTRADA);

String xmlEntrada=null;


if (webService.equals("GetInfoCertificate"))

        xmlEntrada= prop.getProperty(TestClient.XML_ENTRADA_GETINFOCERTIFICATE);

else if (webService.equals("ValidateCertificate"))

        xmlEntrada= prop.getProperty(TestClient.XML_ENTRADA_VALIDATECERTIFICATE);


String paramIn = leeFichero(rutaXML + "/" + xmlEntrada);

logger.info(TestClient.CABECERA_ERROR + paramIn.toString());


String param = webService + "Request";

call.addParameter(param, org.apache.axis.Constants.XSD_STRING, javax.xml.rpc.ParameterMode.IN);

call.setReturnType(org.apache.axis.Constants.XSD_STRING);


String ret = (String) call.invoke( new Object[] { paramIn } );

long tiempoRespuesta = System.currentTimeMillis();
```

```
            long resultado = tiempoRespuesta - requestTime;



            System.out.println("Tiempo de Respuesta ["+resultado+"]");

            logger.error(TestClient.CABECERA_ERROR + " resultado" + ret );

    } catch (Exception e) {

      logger.error(TestClient.CABECERA_ERROR + e.toString());

    }

}//main



    public static String leeFichero(String urlFichero) {

    try{

                BufferedReader in  = new BufferedReader(new FileReader(urlFichero));

                String leidoAux = "";

                String fichero = "";



                leidoAux = in.readLine();

                while(leidoAux != null)

                {

                        fichero += leidoAux;

                        leidoAux = in.readLine();

                }



                if(fichero != null && fichero.trim().length()>0)

                {
```

```
                    return fichero.toString();

                }

        }catch(Exception e)

        {}

      return null;

   }//leeFichero

}
```

ClientHandler.java

```
package wss4j;



import java.io.ByteArrayInputStream;

import java.io.ByteArrayOutputStream;

import java.util.Properties;



import javax.xml.soap.MessageFactory;

import javax.xml.soap.SOAPMessage;

import javax.xml.transform.TransformerFactory;

import javax.xml.transform.dom.DOMSource;

import javax.xml.transform.stream.StreamResult;



import org.apache.axis.AxisFault;
```

```
import org.apache.axis.MessageContext;

import org.apache.axis.SOAPPart;

import org.apache.axis.handlers.BasicHandler;

import org.apache.ws.security.WSConstants;

import org.apache.ws.security.components.crypto.Crypto;

import org.apache.ws.security.components.crypto.CryptoFactory;

import org.apache.ws.security.message.WSSecHeader;

import org.apache.ws.security.message.WSSecSignature;

import org.apache.ws.security.message.WSSecUsernameToken;

import org.w3c.dom.Document;

import org.w3c.dom.Element;



/**

 * Clase encargada de securizar los mensajes SOAP de petición realizados desde un cliente.

 * @author SEPAOT

 *

 */

public class ClientHandler extends BasicHandler

{

	private static final long serialVersionUID = 1L;



	// Opciones de seguridad



	// Seguridad UserNameToken
```

```
public static final String USERNAMEOPTION = WSConstants.USERNAME_TOKEN_LN;

// Seguridad BinarySecurityToken

public static final String CERTIFICATEOPTION = WSConstants.BINARY_TOKEN_LN;

// Sin seguridad

public static final String NONEOPTION = "None";



// Opción de seguridad del objeto actual

private String securityOption = null;



// Usuario para el token de seguridad UserNameToken.

private String userTokenUserName = null;



// Password para el token de seguridad UserNameToken

private String userTokenUserPassword = null;



// Tipo de password para el UserNameTokenPassword

private String userTokenUserPasswordType = null;



// Localización del keystore con certificado y clave privada de usuario

private String keystoreLocation = null;



// Tipo de keystore

private String keystoreType = null;
```

```
        // Clave del keystore
        private String keystorePassword = null;

        // Alias del certificado usado para firmar el tag soapBody de la petición y que será alojado en el token BinarySecurityToken
        private String keystoreCertAlias = null;

        // Password del certificado usado para firmar el tag soapBody de la petición y que será alojado en el token BinarySecurityToken
        private String keystoreCertPassword = null;

        /**
         * Constructor que inicializa el atributo securityOption
         *
         * @param securityOption opción de seguridad.
         * @throws Exception
         */
        public ClientHandler(Properties config)
        {
            if(config == null)
            {
                    System.err.println("Fichero de configuracion de propiedades nulo");
                    System.exit(-1);
            }
```

```
		try
		{
			securityOption = config.getProperty("security.mode");
			userTokenUserName = config.getProperty("security.usertoken.user");
			userTokenUserPassword = config.getProperty("security.usertoken.password");
			userTokenUserPasswordType = config.getProperty("security.usertoken.passwordType");
			keystoreLocation = config.getProperty("security.keystore.location");
			keystoreType = config.getProperty("security.keystore.type");
			keystorePassword = config.getProperty("security.keystore.password");
			keystoreCertAlias = config.getProperty("security.keystore.cert.alias");
			keystoreCertPassword = config.getProperty("security.keystore.cert.password");
		}
		catch (Exception e)
		{
			System.err.println("Error leyendo el fichero de configuración de securización");
			System.exit(-1);
		}

		if(!securityOption.equals(USERNAMEOPTION) && !securityOption.equals(CERTIFICATEOPTION) &&
!securityOption.equals(NONEOPTION))
		{
			System.err.println("Opcion de seguridad no valida: " + securityOption);
			System.exit(-1);
		}
```

```
}

public void invoke(MessageContext msgContext) throws AxisFault
{
    SOAPMessage msg,secMsg;
    Document doc = null;

    secMsg = null;

    try
    {
        //Obtención del documento XML que representa la petición SOAP
        msg = msgContext.getCurrentMessage();

        doc = ((org.apache.axis.message.SOAPEnvelope) msg.getSOAPPart().getEnvelope()).getAsDocument();

        //Securización de la petición SOAP según la opcion de seguridad configurada
        if(this.securityOption.equals(USERNAMEOPTION))
            secMsg = this.createUserNameToken(doc);
        else if(this.securityOption.equals(CERTIFICATEOPTION))
            secMsg = this.createBinarySecurityToken(doc);
        else
            secMsg = msg;
```

```
                //Modificación de la petición SOAP
                ((SOAPPart) msgContext.getRequestMessage().getSOAPPart()).
                setCurrentMessage(secMsg.getSOAPPart().getEnvelope(), SOAPPart.FORM_SOAPENVELOPE);
        }
        catch (Exception e)
        {
                System.err.println(e.getMessage());
                System.exit(-1);
        }
}

/**
 * Securiza, mediante el tag userNameToken, una petición SOAP no securizada.
 *
 * @param soapRequest Documento xml que representa la petición SOAP sin securizar.
 * @return Un mensaje SOAP que contiene la petición SOAP de entrada securizada
 * mediante el tag userNameToken.
 */
private SOAPMessage createUserNameToken(Document soapEnvelopeRequest)
{
        ByteArrayOutputStream baos;
        Document secSOAPReqDoc;
        DOMSource source;
        Element element;
```

```
SOAPMessage res;
StreamResult streamResult;
String secSOAPReq;
WSSecUsernameToken wsSecUsernameToken;
WSSecHeader wsSecHeader;

try{
    //Inserción del tag wsse:Security y userNameToken
    wsSecHeader = new WSSecHeader(null,false);
    wsSecUsernameToken = new WSSecUsernameToken();
    wsSecUsernameToken.setPasswordType(this.userTokenUserPasswordType);
    wsSecUsernameToken.setUserInfo(this.userTokenUserName, this.userTokenUserPassword);
    wsSecHeader.insertSecurityHeader(soapEnvelopeRequest);
    wsSecUsernameToken.prepare(soapEnvelopeRequest);

    //Añadimos una marca de tiempo inidicando la fecha de creación del tag
    wsSecUsernameToken.addCreated();
    wsSecUsernameToken.addNonce();

    //Modificación de la petición
    secSOAPReqDoc = wsSecUsernameToken.build(soapEnvelopeRequest,wsSecHeader);
    element = secSOAPReqDoc.getDocumentElement();

    //Transformación del elemento DOM a String
```

```
                source = new DOMSource(element);

                baos = new ByteArrayOutputStream();

                streamResult = new StreamResult(baos);

                TransformerFactory.newInstance().newTransformer().transform(source, streamResult);

                secSOAPReq = new String(baos.toByteArray());



                //Creación de un nuevo mensaje SOAP a partir del mensaje SOAP securizado formado

                res = MessageFactory.newInstance().createMessage(null,new
ByteArrayInputStream(secSOAPReq.getBytes()));



                return res;

            }

            catch (Exception e) {

                System.err.println(e.getMessage());

                System.exit(-1);

                return null;

            }

        }



        /**

         * Securiza, mediante el tag BinarySecurityToken y firma una petición SOAP no securizada.

         *

         * @param soapEnvelopeRequest Documento xml que representa la petición SOAP sin securizar.

         * @return Un mensaje SOAP que contiene la petición SOAP de entrada securizada
```

```
         * mediante el tag BinarySecurityToken.
         */
        private SOAPMessage createBinarySecurityToken(Document soapEnvelopeRequest)
        {
            ByteArrayOutputStream baos;
            Crypto crypto;
            Document secSOAPReqDoc;
            DOMSource source;
            Element element;
            StreamResult streamResult;
            String secSOAPReq;
            SOAPMessage res;
            WSSecSignature wsSecSignature;
            WSSecHeader wsSecHeader;

            try
            {
                //Inserción del tag wsse:Security y BinarySecurityToken
                wsSecHeader = new WSSecHeader(null, false);
                wsSecSignature = new WSSecSignature();
                crypto = CryptoFactory.getInstance("org.apache.ws.security.components.crypto.Merlin",
this.initializateCryptoProperties());

                //Indicación para que inserte el tag BinarySecurityToken
```

```
                wsSecSignature.setKeyIdentifierType(WSConstants.BST_DIRECT_REFERENCE);


                //wsSecSignature.setKeyIdentifierType(WSConstants.ISSUER_SERIAL);

                wsSecSignature.setUserInfo(this.keystoreCertAlias, this.keystoreCertPassword);

                wsSecHeader.insertSecurityHeader(soapEnvelopeRequest);

                wsSecSignature.prepare(soapEnvelopeRequest,crypto,wsSecHeader);


                //Modificación y firma de la petición

                secSOAPReqDoc = wsSecSignature.build(soapEnvelopeRequest,crypto,wsSecHeader);

                element = secSOAPReqDoc.getDocumentElement();


                //Transformación del elemento DOM a String

                source = new DOMSource(element);

                baos = new ByteArrayOutputStream();

                streamResult = new StreamResult(baos);

                TransformerFactory.newInstance().newTransformer().transform(source, streamResult);

                secSOAPReq = new String(baos.toByteArray());


                //Creación de un nuevo mensaje SOAP a partir del mensaje SOAP securizado formado

                res = MessageFactory.newInstance().createMessage(null,new
ByteArrayInputStream(secSOAPReq.getBytes()));


                return res;

            }
```

```
        catch (Exception e)
        {
            System.err.println(e.getMessage());
            System.exit(-1);
            return null;
            }
    }

    /**
     * Establece el conjunto de propiedades con el que será inicializado el gestor criptográfico de WSS4J.
     * @return Devuelve el conjunto de propiedades con el que será inicializado el gestor criptográfico de WSS4J.
     */
    private Properties initializateCryptoProperties()
    {
        Properties res = new Properties();
        res.setProperty("org.apache.ws.security.crypto.provider",
                        "org.apache.ws.security.components.crypto.Merlin");
        res.setProperty("org.apache.ws.security.crypto.merlin.keystore.type",this.keystoreType);
        res.setProperty("org.apache.ws.security.crypto.merlin.keystore.password",this.keystorePassword);
        res.setProperty("org.apache.ws.security.crypto.merlin.keystore.alias",this.keystoreCertAlias);
        res.setProperty("org.apache.ws.security.crypto.merlin.alias.password",this.keystoreCertPassword);
        res.setProperty("org.apache.ws.security.crypto.merlin.file",this.keystoreLocation);

        return res;
```

```
        }

}
```

securityConfiguration.properties

```
# Tiempo máximo de espera en la petición al servicio (en ms)

timer=60000



######################################################################

#                              SECURIZACIÓN DE PETICIÓN SOAP DEL CLIENTE       #

######################################################################



# MODO DE SECURIZACION

# Valores posibles: None, UsernameToken, BinarySecurityToken

security.mode=None



# Atributos exclusivos si security.mode es UsernameToken

# - usuario:  usuario dado de alta para la aplicación que realiza la petición

# - password: password correspondiente

# Valores posibles de passwordType: PasswordDigest (la password se envía hasheada) o PasswordText (la password se envía en claro)

security.usertoken.user=prueba

security.usertoken.password=1111

security.usertoken.passwordType=PasswordDigest
```

```
# Atributos exclusivos si security.mode es BinarySecurityToken

# - location:          Ruta al almacén que contiene el certificado y la clave privada con la que firmar la petición WS

# - type:                Tipo de almacén (PKCS12, JKS)

# - password:     password del Almacén

# - cert alias:    Alias del certificado del usuario que está dentro del almacén

# - cert password: Password de la clave privada correspondiente al certificado anterior

security.keystore.location=C:\\colegiado.pfx

security.keystore.type=PKCS12

security.keystore.password=1111

security.keystore.cert.alias=pruebas

security.keystore.cert.password=1111
```

Webservices.properties

```
webservices.rutaXml=C:\\ws\\xml

webservices.GetInfoCertificate=getInfoCertificate.xml

webservices.ValidateCertificate=validateCertificate.xml
```

A.4 Valores de elementos de validación

A.4.1 Elemento proceso

El elemento <proceso> puede tomar uno de los siguientes valores:

- Proceso de verificación de Firma Electrónica completo
- Proceso de verificación de Firma Electrónica incompleto
- Proceso de verificación de Firma Electrónica fallido

A.4.2 Elemento detalle

El elemento <detalle> puede tomar los siguientes valores separados por una barra vertical "|" combinados de múltiples maneras. Como mínimo al menos toma un valor.

- Error en los parámetros de entrada
- Error en el parámetro de entrada
- No se han podido recuperar los hashes de la Firma Electrónica
- El hash no se corresponde con el hash contenido en la Firma Electrónica
- No se dispone de suficiente información para realizar la comprobación del hash recibido
- No se ha podido validar el hash proporcionado
- Firma Digital correcta
- Firma Digital incorrecta
- La Firma Digital no se ha podido verificar
- Firma Electrónica correcta
- Firma Electrónica incorrecta
- La Firma Electrónica no se ha podido verificar completamente
- Los certificados contenidos en la Firma Electrónica son válidos (integridad, periodo de validez, estado de revocación)

- La Firma Electrónica del bloque es correcta
- La Firma Electrónica del bloque es incorrecta
- Las Firmas Electrónicas Servidor contenidas en el bloque son correctas
- La Firma Electrónica del Documento indicado contenido en el bloque es correcta
- No se ha comprobado que la firma se corresponda con el documento o hash proporcionado

Adicionalmente, en el caso de producirse una excepción durante la validación de la firma, o se detecta que la firma es incompleta, podría tomar como valor un texto explicativo de los motivos que ha producido el error.

A.4.3 Elemento conclusión

El elemento <conclusion> puede tomar los siguientes valores:

- Firma Electrónica correcta
- Firma Electrónica incorrecta
- La Firma Electrónica no se ha podido verificar completamente
- La Firma Electrónica del bloque es correcta
- La Firma Electrónica del Documento indicado contenido en el bloque es correcta

A.5 Obtener versión de @firma

Desde la versión 5.5.0_001, se dispone de un método por el que consultar la versión de @firma que se encuentra instalada en el servidor al que se accede. Para ello tan solo habría que introducir en el navegador la siguiente ruta:

```
http://IP_SERVIDOR/afirmaws/version.xml
```

donde IP_SERVIDOR es la dirección IP del servidor donde se encuentra la plataforma en funcionamiento.

El servidor nos devolverá un fichero XML como el que sigue (ejemplo obtenido de la versión 5.5.0_001 de @firma):

```
<?xml version="1.0"?>
<AFIRMA_VERSION>
  <major>5</major>
  <minor>5</minor>
  <build>0</build>
  <revision>001</revision>
</AFIRMA_VERSION>
```

A.6 Guia 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