Perfil DSS asociado a los servicios web de TS@

TS@ 3.1.3

Documento nº:	TSA-XMLSOAP_PROFILE_DSS
Revisión:	005
Fecha:	21-03-2018

CONTROL DE MODIFICACIONES

Documento nº:	TSA-XMLSOAP_PROFILE_DSS
Revisión:	005
Fecha:	21-03-2018

Rev.	001
Fecha	14-10-2014
Descripción	Documento inicial

Rev.	002
Fecha	13-08-2015
Descripción	Se modifica la fuente Frutiger por Calibri. Se añade un nuevo ResultMajor (warning). Se añade un elemento opcional para la petición de validación de sello de tiempo (dss:ReturnProcessingDetails). Se añaden dos elementos para la respuesta de validación de sello de tiempo (dss:SigningTimeInfo y dss:ProcessingDetails). Se añaden los ResultMinor asociados a las tareas de verificación para la validación de sellos de tiempo.

Rev.	003
Fecha	07-07-2017
Descripción	Se actualiza la información de versión a la 3.1.3.

Rev.	004
Fecha	02-01-2018
Descripción	Se incluye el anexo A.4 en el que se informa de la necesidad de revisar la Guía 807 del Esquema Nacional de Seguridad.

Rev.	005
Fecha	21-03-2018
Descripción	Se marcan como deprecados los servicios de validación y renovación de sellos de tiempo.

CONTROL DE DISTRIBUCIÓN

Documento nº:	TSA-XMLSOAP_PROFILE_DSS
Revisión:	005
Fecha:	21-03-2018

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

Distribución en Papel:

Nombre o Cargo y Organización	Nº de Ejemplares	Referencia de la carta de transmisión y fecha

Índice

1 Objeto 5

2 Siglas y Acrónimos 6

3 Documentos de Referencia 7

4 Introducción 8

5 Espacio de Nombres 9

6 Servicios DSS de TS@ 10

6.1 Servicio de Creación de Sello de Tiempo 10

6.1.1 Mensaje XML de Petición 10

6.1.2 Mensaje XML de Respuesta 20

6.2 Servicio de Validación de Sello de Tiempo. Servicio discontinuado (deprecated). 24

6.2.1 Mensaje XML de Petición 24

6.2.2 Mensaje XML de Respuesta 35

6.3 Servicio de Renovación de Sello de Tiempo. Servicio discontinuado (deprecated). 44

6.3.1 Mensaje XML de Petición 45

6.3.2 Mensaje XML de Respuesta 56

A.1 Descripción de los Elementos utilizados en los Diagramas 61

A.2 Identificadores 64

A.2.1 Identificadores de Tipo de Sello de Tiempo 64

A.2.2 Identificadores de resultado del proceso 64

A.2.3 Identificadores de tareas de verificación 66

A.3 Ejemplos de Peticiones y Respuesta 69

A.3.1 Ejemplos de Generación de Sello de Tiempo 69

A.3.2 Ejemplos de Validación de Sello de Tiempo 86

A.3.3 Ejemplos de Renovación de Sello de Tiempo 99

A.4 Guía 807 del Esquema Nacional de Seguridad (ENS). 127

1 Objeto

El presente documento describe los perfiles utilizados por los servicios web de la plataforma TS@ según las especificaciones definidas por la organización OASIS para los servicios de sello de tiempo DSS.

2 Siglas y Acrónimos

DSS	Digital Signature Service
XML	eXtensible Markuap Language
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
ASN.1	Abstract Syntax Notation One

3 Documentos de Referencia

[DSS_CORE]	Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0
[XMLDSIG]	XML Signature Syntax and Processing W3C Recommendation 12 February 2002
[TST_PROFILE]	XML Timestamping Profile of the OASIS Digital Signature Services Version 1.0
[WS_SECURITY]	Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) OASIS Standard 200401, March 2004
[USERNAME_TOKEN]	Web Services Security UsernameToken Profile 1.0 OASIS Standard 200401, March 2004
[CERTIFICATE_TOKEN]	Web Services Security X.509 Certificate Token Profile OASIS Standard 200401, March 2004
[SAML_TOKEN]	Web Services Security: SAML Token Profile OASIS STANDARD, 01 Dec. 2004
[DSS_XSS]	eXtended Signature Services (XSS) Profile of the OASIS Digital Signature Service (DSS), Working Draft 07, 24 March 2006
[SAML_CORE]	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 OASIS Standard, 15 March 2005

4 Introducción

El estándar Digital Signature Service de OASIS define, entre otros, protocolos de sello de tiempo basados en interfaces XML. El perfil DSS en el que se basa este documento se refiere a XML Timestamping, asociado a los servicios de sello de tiempo, validación de sello de tiempo, y renovación de sello de tiempo (re-sellado), estando estos dos últimos discontinuados (deprecated) en la versión actual. En apartados posteriores se describirán los elementos relacionados con el perfil indicado.

5 Espacio de Nombres

Los prefijos utilizados en están implementación están asociados a los siguientes espacios de nombres:

- **dss**: Espacio de nombres definido en [DDS_CORE].
- **ds**: Espacio de nombres definido en [XMLDSIG].
- **dst**: Espacio de nombres definido en [TST_PROFILE].
- **xss**: Espacio de nombres definido en [DSS_XSS].
- **saml**: Espacio de nombres definido en [SAML_CORE].
- **wsse**: Espacio de nombres definido en [WS_SECURITY].
- **wsu**: Espacio de nombres definido en [WS_SECURITY].

6 Servicios DSS de TS@

Los Servicios Web que publica la plataforma TS@ son:

- ***CreateTimeStampWS*.** Servicio de creación de sello de tiempo.
- ***VerifyTimeStampWS*.** Servicio de validación de sello de tiempo. Servicio descontinuado (deprecated).
- ***RenewTimeStampWS.*** Servicio de renovación de sello de tiempo (deprecated). Servicio descontinuado (deprecated).

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

6.1 Servicio de Creación de Sello de Tiempo

El servicio de creación de sello de tiempo (CreateTimeStampWS) permite la generación de sellos de tiempo a partir de un certificado alojado en la plataforma.

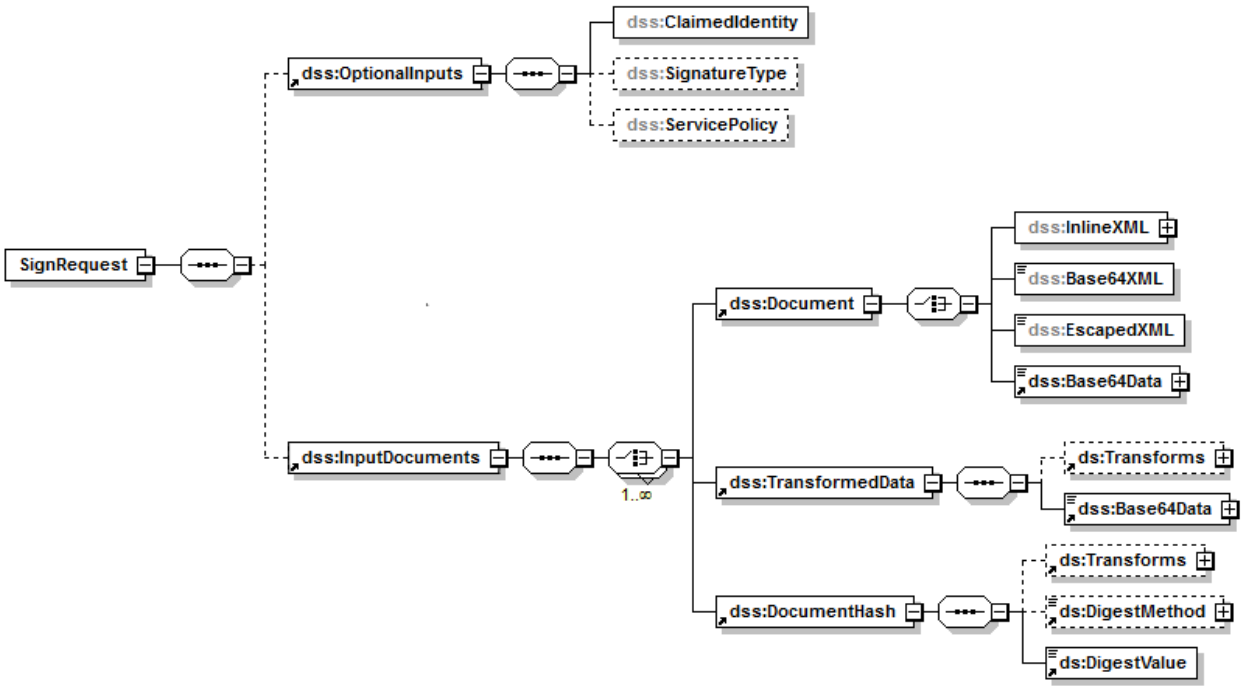
OASIS en sus especificaciones para servicio de firma digital (DSS) define diferentes elementos para soportar las peticiones de generación de sellos de tiempo y las respuestas del proceso. Estos elementos son:

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

A continuación se detalla la definición de dichos elementos.

6.1.1 Mensaje XML de Petición

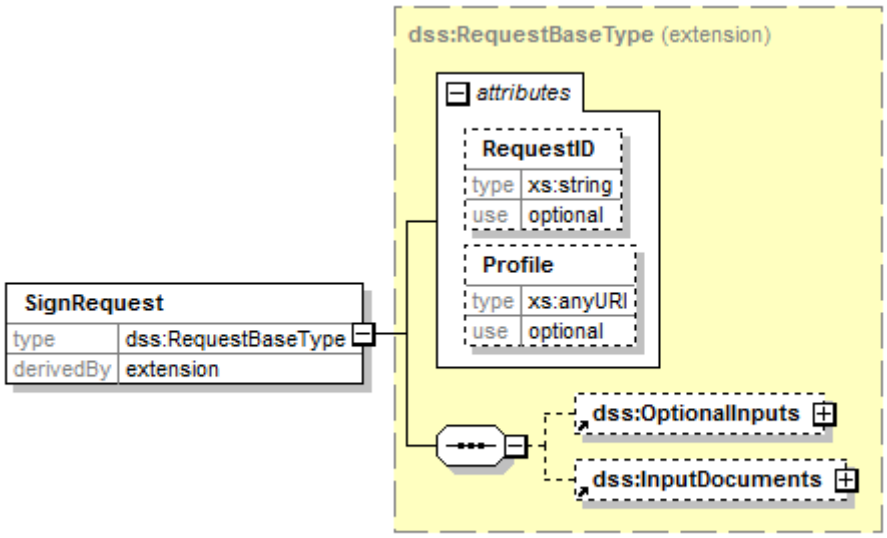
En la siguiente figura podemos observar los distintos componentes que pueden formar una petición de sello de tiempo:



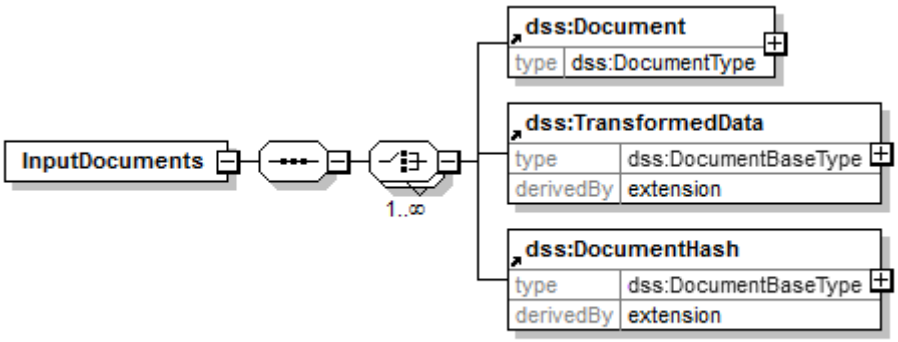
Como se observa en la anterior figura la petición de firma dss:SignRequest esta compuesta por dos elementos diferenciados:

- *dss:InputDocument*. Elemento que recoge el documento a ser sellado, o una referencia al mismo. La información de los datos a ser firmados puede incluirse de las siguientes formas:
    - Incluyendo el documento en un elemento *dss:Document*.
    - Incluyendo el documento en un elemento *dss:TransformedData*.
    - Incluyendo el documento en un elemento *dss:DocumentHash*.
- *dss:OptionalInput.* Elemento que incluye la información necesaria para que el servidor pueda realizar el sellado de los datos pasados en el anterior componente, para esta implementación del perfil el único paramétro obligatorio es el identificador de aplicación (contenido en el componente *dss:ClaimedIdentity*). Adicionalmente este componente permite incluir parámetros adicionales como son el tipo de sello de tiempo a generar (componente *dss:SignatureType*), y la política de sello de tiempo (componente *dss:ServicePolicy*).

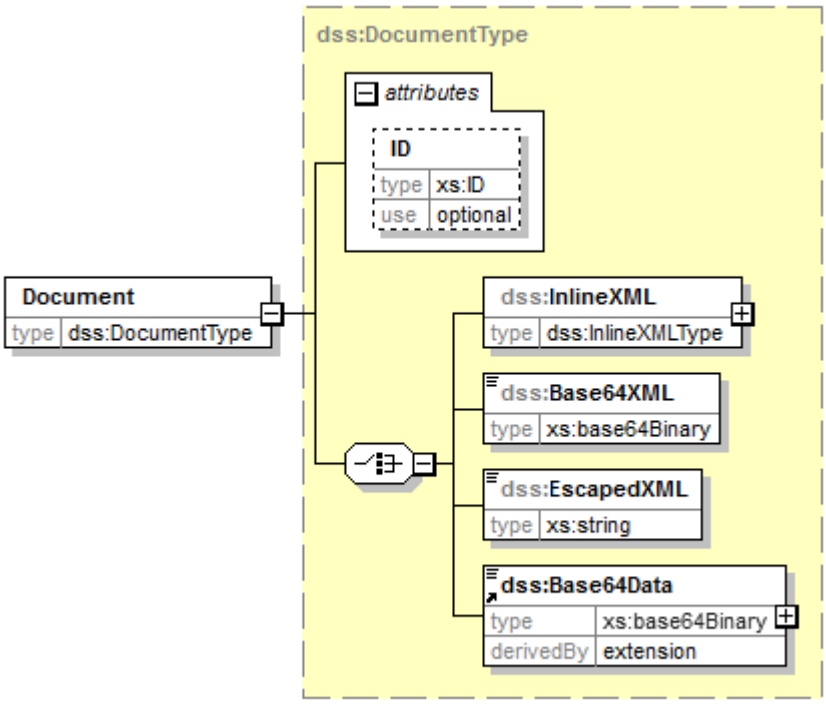
6.1.1.1 dss:SignRequest

SignRequest		
Diagrama		
Descripción	Componente introducido en las especificaciones [DSS_CORE] y que constituye el elemento raíz de una petición de generación de sello de tiempo.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:InputDocuments.* Este componente se describe en el apartado 6.1.1.2. • *dss:OptionalInputs.* Este componente se describe en el apartado 6.1.1.10.	
Atributos	**Nombre**	**Descripción**
	Profile	Identificador del perfil soportado por el servicio. Para peticiones de generación de sello de tiempo a la plataforma, el valor de este atributo será: **urn:oasis:names:tc:dss:1.0:profiles:timestamping.** Esta URI identifica al perfil Timestamping de OASIS.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma.

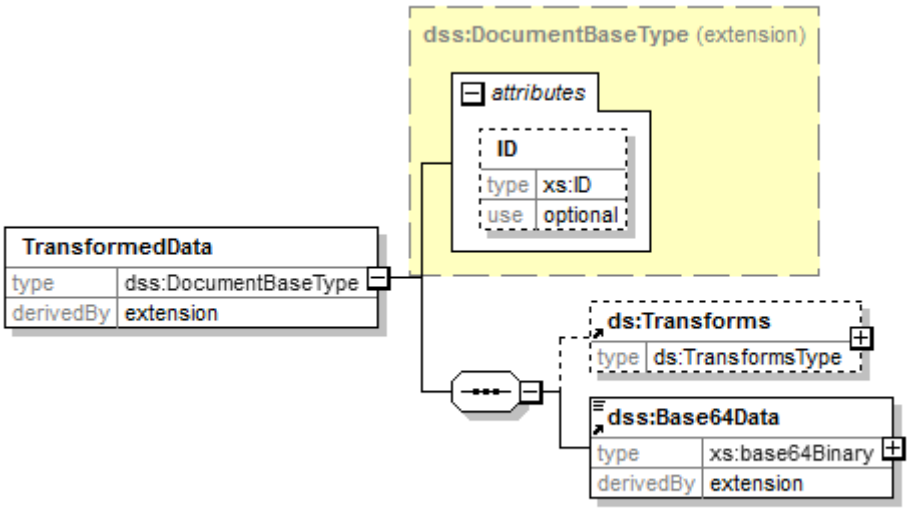
6.1.1.2 dss:InputDocuments

InputDocuments	
Diagrama	
Descripción	Este elemento contendrá el documento o datos que van a ser sellados.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:Document*. Este elemento se describe en el apartado 6.1.1.3. • *dss:TransformedData*. Este elemento se describe en el apartado 6.1.1.4. • *dss:DocumentHash.* Este elemento se describe en el apartado 6.1.1.5.

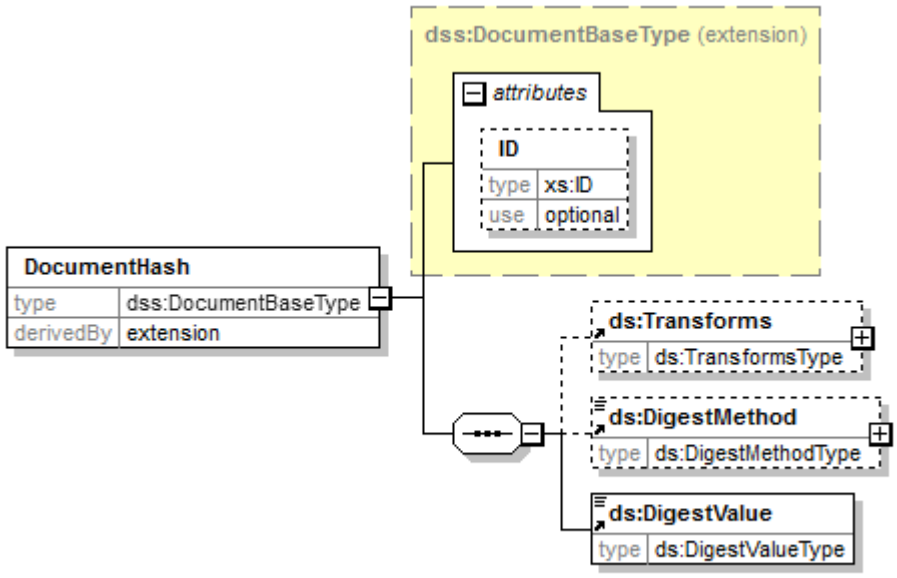
6.1.1.3 dss:Document

Document		
Diagrama		
Descripción	Este elemento contendrá los datos a sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Base64Data*. Este elemento se describe en el apartado 6.1.1.6. • *dss:Base64XML*. Este elemento se describe en el apartado 6.1.1.7. • *dss:InlineXML*. Este elemento se describe en el apartado 6.1.1.8. • *dss:EscapedXML*. Este elemento se describe en el apartado 6.1.1.9.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

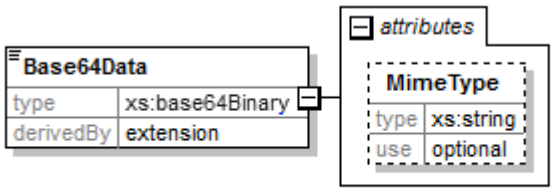
6.1.1.4 dss:TransformedData

TransformedData		
Diagrama		
Descripción	Este elemento contendrá los datos a sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *ds:Transforms*. Elemento que contiene la lista de transformadas aplicadas sobre los datos. • *dss:Base64Data*. Este elemento se describe en el apartado 6.1.1.6.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

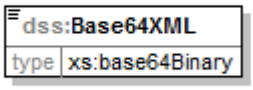
6.1.1.5 dss:DocumentHash

DocumentHash		
Diagrama		
Descripción	Este elemento contendrá los datos a sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *ds:Transforms*. Elemento que contiene la lista de transformadas aplicadas sobre los datos. • *ds:DigestMethod*. Elemento que especifica el algoritmo de resumen usado para calcular el resumen de los datos canonicalizados en base a las transformadas indicadas por el elemento anterior. • *ds:DigestValue*. Elemento que especifica el valor del resumen de los datos canonicalizados.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

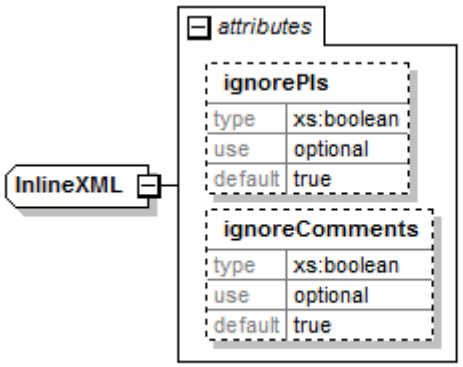
6.1.1.6 dss:Base64Data

Base64Data		
Diagrama		
Descripción	Este elemento contendrá datos, en formato diferente a XML, codificados en Base64.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	**Nombre**	**Descripción**
	MimeTye	Indicador del tipo de datos contenidos.

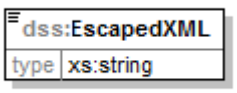
6.1.1.7 dss:Base64XML

Base64XML	
Diagrama	
Descripción	Este elemento contendrá datos, en formato XML, codificados en Base64.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

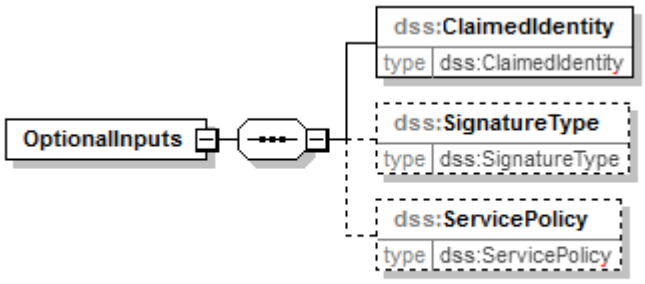
6.1.1.8 dss:InlineXML

InlineXML		
Diagrama		
Descripción	Este elemento contendrá un documento completo en formato XML, pero sin saltos de línea ni retornos de carro.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	**Nombre**	**Descripción**
	IgnoresPIs	Indicador para ignorar, o no, las instrucciones de procesamiento del documento XML completo.
	IgnoreComments	Indicador para ignorar, o no, los comentarios en el documento XML completo.

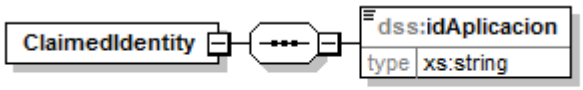
6.1.1.9 dss:EscapedXML

EscapedXML	
Diagrama	
Descripción	Este elemento contendrá datos en formato XML escapados.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

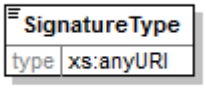
6.1.1.10 dss:OptionalInputs

OptionalInputs	
Diagrama	
Descripción	Este elemento contendrá parámetros adicionales de la petición.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:ClaimedIdentity*. Este elemento se describe en el apartado 6.1.1.11. • *dss:SignatureType*. Este elemento se describe en el apartado 6.1.1.12. • *dss:ServicePolicy*. Este elemento se describe en el apartado 6.1.1.13.

6.1.1.11 dss:ClaimedIdentity

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

6.1.1.12 dss:SignatureType

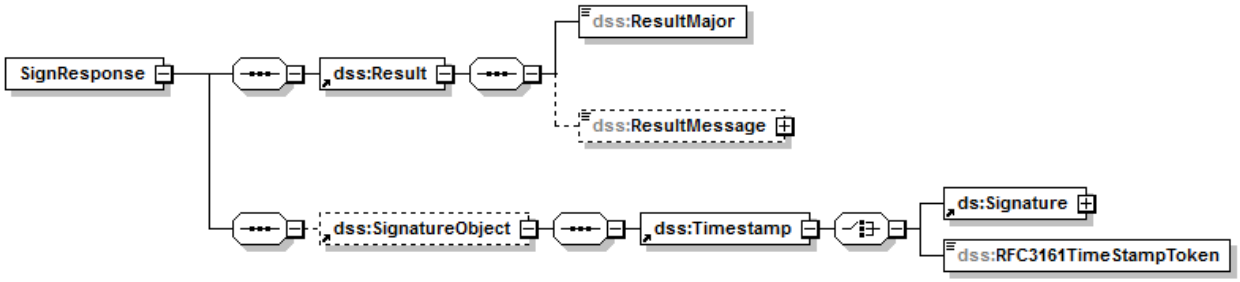
SignatureType	
Diagrama	
Descripción	Este elemento permite identificar el tipo de sello de tiempo a generar mediante su URI. Su inclusión es opcional, si bien, en caso de no incluirse, se procederá a generar un sello de tiempo de tipo XML. En el anexo se detallan las URI aceptadas en la versión actual del perfil.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

6.1.1.13 dss:ServicePolicy

ServicePolicy	
Diagrama	
Descripción	Este elemento permite identificar la política de sello de tiempo a utilizar en la generación del sello de tiempo por medio de la inclusión de su URI, establecida en el proceso de alta de la política de sello de tiempo en el sistema. Su inclusión es opcional.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

6.1.2 Mensaje XML de Respuesta

En la siguiente figura podemos observar los distintos componentes que pueden formar una respuesta de sello de tiempo:

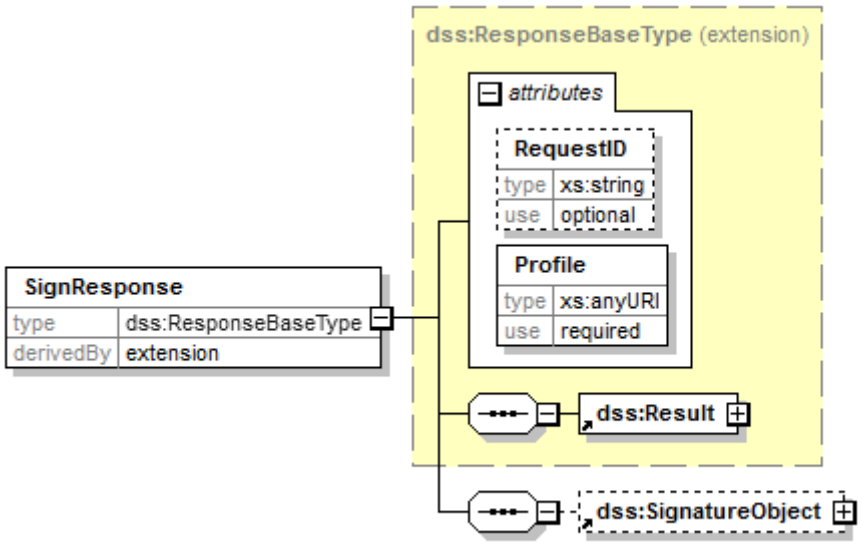


Como se observa en la anterior figura la respuesta de sello de tiempo *dss:SignResponse* está compuesta por dos elementos diferenciados:

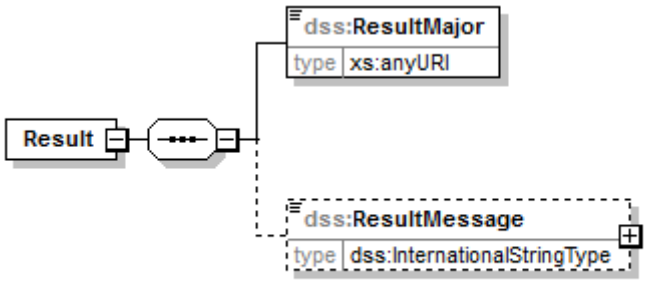
- *dss:Result.* Componente que recoge el resultado final del proceso.
- *dss: SignatureObject.* Componente que contiene el sello de tiempo generado.

A continuación se detalla cada elemento.

6.1.2.1 dss:SignResponse

SignResponse		
Diagrama		
Descripción	Elemento raíz de la respuesta a una petición de sello de tiempo.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Result.* Este componente se describe en el apartado 6.1.2.2. • *dss:SignatureObject.* Este componente se describe en el apartado 6.1.2.3.	
Atributos	**Nombre**	**Descripción**
	Profile	URI que indica el perfil que implementa el servidor. En este caso, el valor del atributo siempre será **urn:oasis:names:tc:dss:1.0:profiles:timestamping**.
	RequestID	Identificador de la petición origen. En caso de haberse especificado un identificador en la petición, se devolverá el mismo valor.

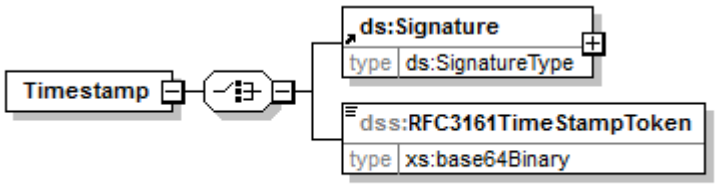
6.1.2.2 dss:Result

Result	
Diagrama	
Descripción	Elemento que contiene el resultado del proceso de generación de sello de tiempo.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:ResultMajor.* Componente que indica, mediante una URI, el resultado global del proceso. En el anexo se detallan los distintos valores que puede tomar. • *dss:ResultMessage*. Componente que presenta un mensaje descriptivo del resultado del proceso.

6.1.2.3 dss:SignatureObject

SignatureObject	
Diagrama	
Descripción	Elemento que contiene el sello de tiempo generado.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	▪ *dss:Timestamp.* Este elemento se describe en el apartado 6.1.2.4.

6.1.2.4 dss:Timestamp

Timestamp	
Diagrama	
Descripción	Elemento que representa el sello de tiempo generado.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	▪ *ds:Signature.* Este elemento se corresponde con el sello de tiempo en formato XML. Para más información acerca de este elemento se recomienda acudir a los documentos [DSS_CORE] y [XML_TIMESTAMP]. ▪ *dss:RFC3161TimeStampToken*. Este elemento se corresponde con el sello de tiempo ASN.1 codificado en Base64, según define [RFC3161].

6.2 Servicio de Validación de Sello de Tiempo. Servicio discontinuado (deprecated).

El servicio de validación de sello de tiempo (VerifyTimeStampWS) permite la validación de sellos de tiempo.

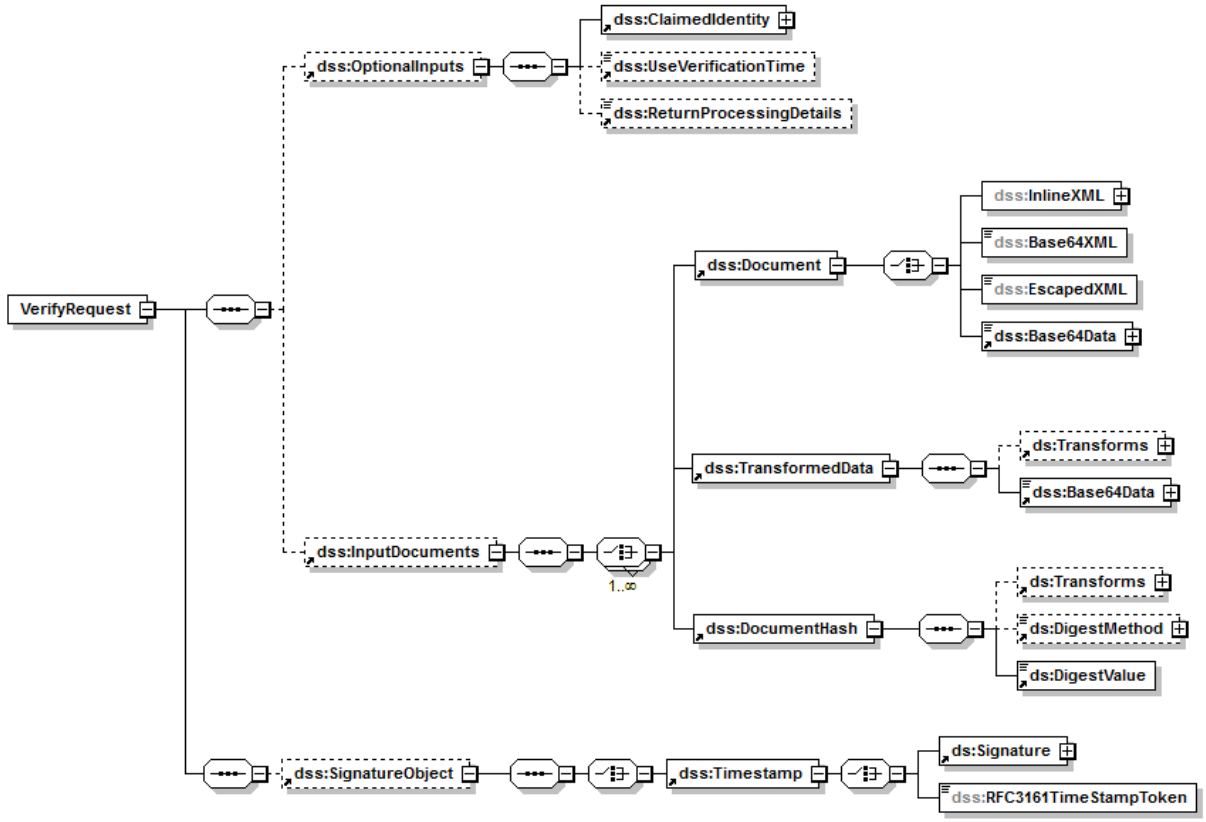
OASIS en sus especificaciones para servicio de firma digital (DSS) define diferentes elementos para soportar las peticiones de validación de sellos de tiempo y las respuestas del proceso. Estos elementos son:

- ***dss:VerifyRequest***: Elemento XML de petición de validación.
- ***dss:VerifyResponse***: Elemento XML de respuesta de validación.

A continuación se detalla la definición de dichos elementos.

6.2.1 Mensaje XML de Petición

En la siguiente figura podemos observar los distintos componentes que pueden formar una petición de validación de sello de tiempo:



Como se observa en la anterior figura la petición de validación *dss:VerifyRequest* esta compuesta por tres elementos diferenciados:

- *dss:InputDocument.* Elemento que recoge el documento que fue sellado por el sello de tiempo a validar, o una referencia al mismo. La información de los datos originales puede incluirse de las siguientes formas:
    - Incluyendo el documento en un elemento *dss:Document*.
    - Incluyendo el documento en un elemento *dss:TransformedData*.
    - Incluyendo el documento en un elemento *dss:DocumentHash*.
- *dss:SignatureObject.* Elemento que incluye el sello de tiempo a validar.
- *dss:OptionalInput.* Elemento que incluye la información necesaria para que el servidor pueda realizar la validación del sello de tiempo. Para esta implementación del perfil el único paramétro obligatorio es el identificador de aplicación (contenido en el componente *dss:ClaimedIdentity*). Adicionalmente, este componente permite incluir dos elementos opcionales:
    - *dss:UseVerificationTime.* Elemento que establece la fecha respecto a la cual se debe determinar la validez de la firma del sello de tiempo.

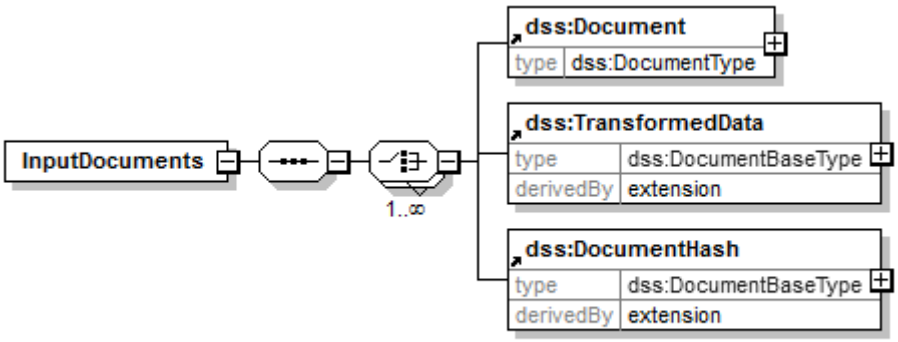
- *dss:ReturnProcessingDetails.* Elemento que permite obtener el resultado de cada tarea de verificación que constituye el proceso de validación de un sello de tiempo.

A continuación se detalla cada elemento.

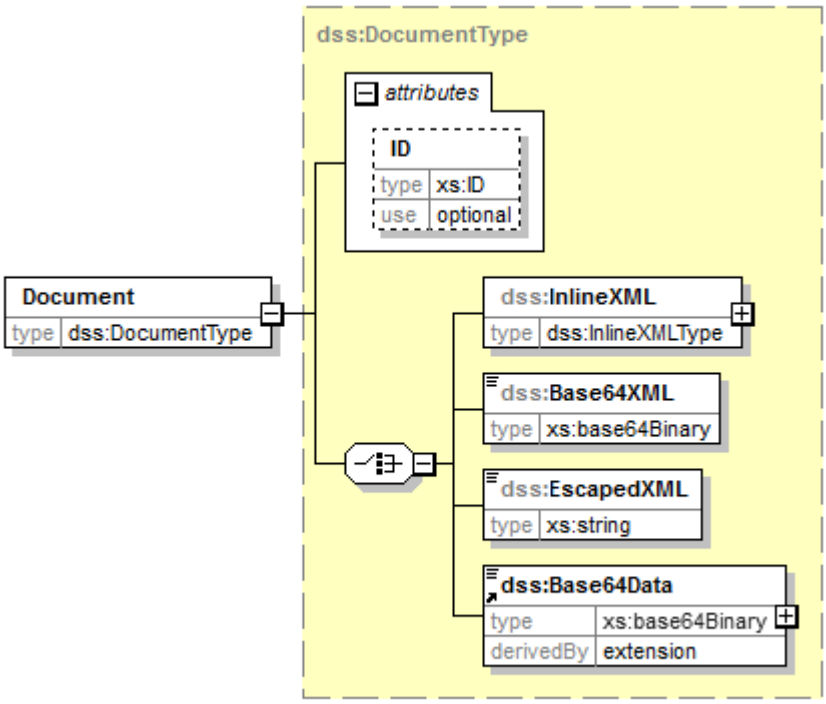
6.2.1.1 dss:VerifyRequest

VerifyRequest		
Diagrama		
Descripción	Componente introducido en las especificaciones [DSS_CORE] y que constituye el elemento raíz de una petición de validación de sello de tiempo.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:OptionalInputs.* Este componente se describe en el apartado 6.2.1.12. • *dss:SignatureObject.* Este componente se describe en el apartado 6.2.1.10. • *dss:InputDocuments.* Este componente se describe en el apartado 6.2.1.2.	
Atributos	**Nombre**	**Descripción**
	Profile	Identificador del perfil soportado por el servicio. Para peticiones de validación de sello de tiempo a la plataforma, el valor de este atributo será: **urn:oasis:names:tc:dss:1.0:profiles:timestamping.** Esta URI identifica al perfil Timestamping de OASIS.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma.

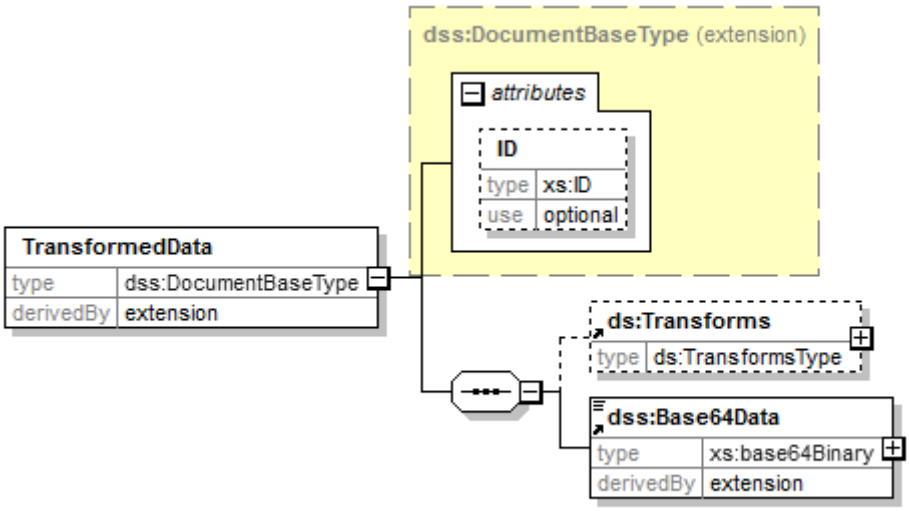
6.2.1.2 dss:InputDocuments

InputDocuments	
Diagrama	
Descripción	Este elemento contendrá el documento o datos que fueron sellados por el sello de tiempo a validar.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:Document*. Este elemento se describe en el apartado 6.2.1.3. • *dss:TransformedData*. Este elemento se describe en el apartado 6.2.1.4. • *dss:DocumentHash.* Este elemento se describe en el apartado 6.2.1.5.

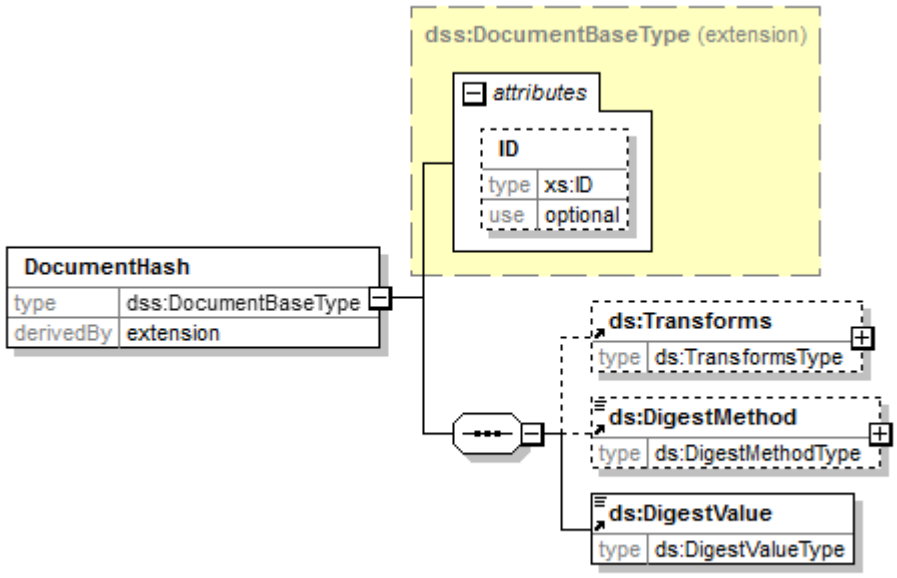
6.2.1.3 dss:Document

Document		
Diagrama		
Descripción	Este elemento contendrá los datos originales sin sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Base64Data*. Este elemento se describe en el apartado 6.2.1.6. • *dss:Base64XML*. Este elemento se describe en el apartado 6.2.1.7. • *dss:InlineXML*. Este elemento se describe en el apartado 6.2.1.8. • *dss:EscapedXML*. Este elemento se describe en el apartado 6.2.1.9.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

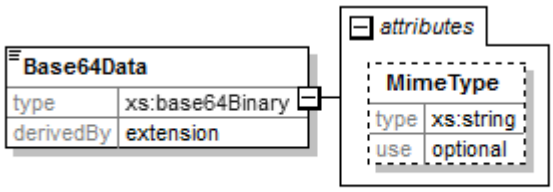
6.2.1.4 dss:TransformedData

TransformedData		
Diagrama		
Descripción	Este elemento contendrá los datos originales sin sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *ds:Transforms*. Elemento que contiene la lista de transformadas aplicadas sobre los datos. • *dss:Base64Data*. Este elemento se describe en el apartado 6.2.1.6.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

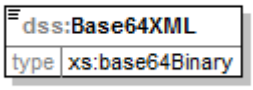
6.2.1.5 dss:DocumentHash

DocumentHash		
Diagrama		
Descripción	Este elemento contendrá los datos originales sin sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *ds:Transforms*. Elemento que contiene la lista de transformadas aplicadas sobre los datos. • *ds:DigestMethod*. Elemento que especifica el algoritmo de resumen usado para calcular el resumen de los datos canonicalizados en base a las transformadas indicadas por el elemento anterior. • *ds:DigestValue*. Elemento que especifica el valor del resumen de los datos canonicalizados.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

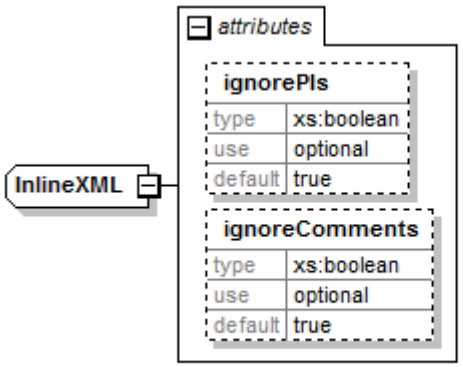
6.2.1.6 dss:Base64Data

Base64Data		
Diagrama		
Descripción	Este elemento contendrá datos, en formato diferente a XML, codificados en Base64.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	**Nombre**	**Descripción**
	MimeTye	Indicador del tipo de datos contenidos.

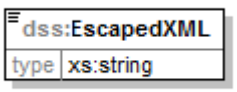
6.2.1.7 dss:Base64XML

Base64XML	
Diagrama	
Descripción	Este elemento contendrá datos, en formato XML, codificados en Base64.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

6.2.1.8 dss:InlineXML

InlineXML		
Diagrama		
Descripción	Este elemento contendrá un documento completo en formato XML, pero sin saltos de línea ni retornos de carro.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	**Nombre**	**Descripción**
	IgnoresPIs	Indicador para ignorar, o no, las instrucciones de procesamiento del documento XML completo.
	IgnoreComments	Indicador para ignorar, o no, los comentarios en el documento XML completo.

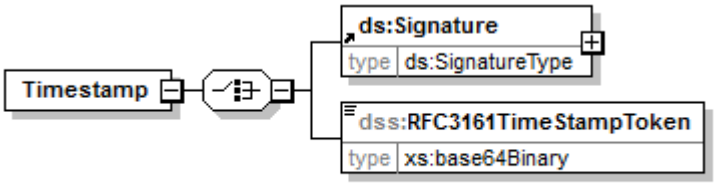
6.2.1.9 dss:EscapedXML

EscapedXML	
Diagrama	
Descripción	Este elemento contendrá datos en formato XML escapados.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

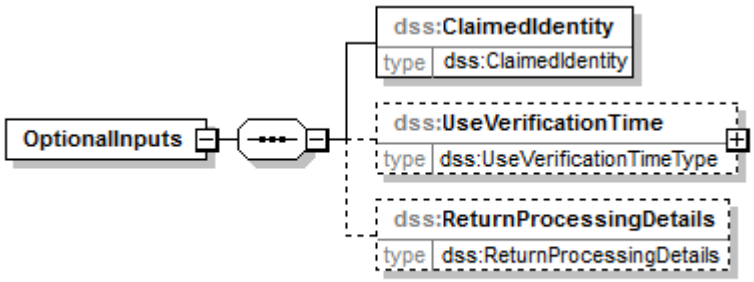
6.2.1.10 dss:SignatureObject

SignatureObject	
Diagrama	
Descripción	Elemento que contiene el sello de tiempo a validar.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	▪ *dss:Timestamp.* Este elemento se describe en el apartado 6.2.1.11.

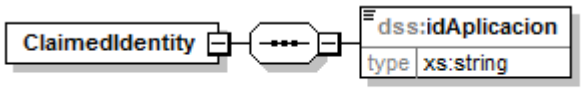
6.2.1.11 dss:Timestamp

Timestamp	
Diagrama	
Descripción	Elemento que representa el sello de tiempo a validar.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	▪ *ds:Signature.* Este elemento se corresponde con el sello de tiempo en formato XML. Para más información acerca de este elemento se recomienda acudir a los documentos [DSS_CORE] y [XML_TIMESTAMP]. ▪ *dss:RFC3161TimeStampToken*. Este elemento se corresponde con el sello de tiempo ASN.1 codificado en Base64, según define [RFC3161].

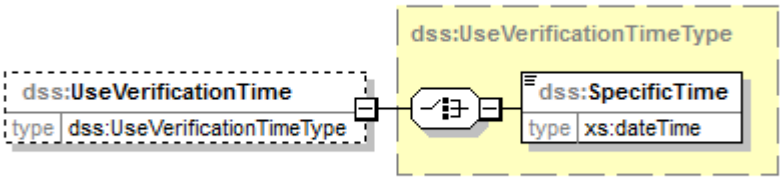
6.2.1.12 dss:OptionalInputs

OptionalInputs	
Diagrama	
Descripción	Este elemento contendrá parámetros adicionales de la petición.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:ClaimedIdentity*. Este elemento se describe en el apartado 6.2.1.13. • *dss:UseVerificationTime*. Este elemento se describe en el apartado 6.2.1.14. • *dss:ReturnProcessingDetails.* Este elemento se describe en el apartado 6.2.1.15.

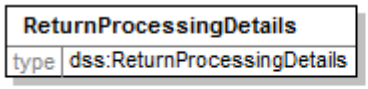
6.2.1.13 dss:ClaimedIdentity

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

6.2.1.14 dss:UseVerificationTime

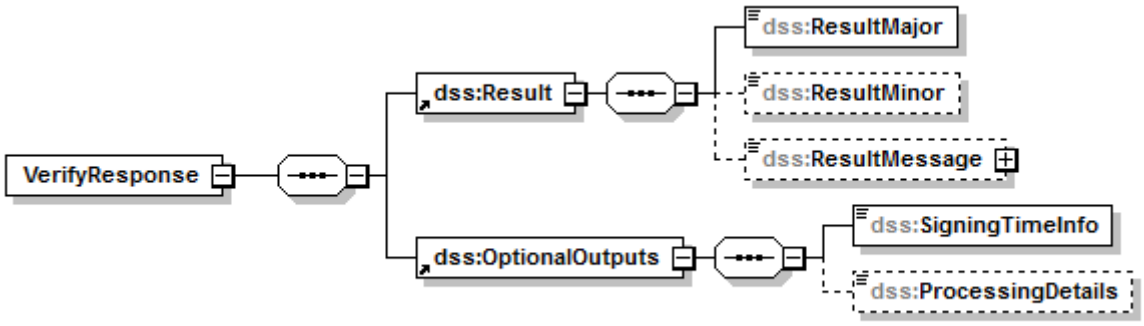
UseVerificationTime	
Diagrama	
Descripción	Este elemento opcional indica al servidor la fecha concreta a utilizar para determinar la validez de la firma del sello de tiempo, en lugar de utilizar la fecha actual en el momento de la recepción de la petición en el servidor.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:SpecificTime*. Este elemento indica la fecha a utilizar para la validación de la firma del sello de tiempo expresada en formato UTC.

6.2.1.15 dss:ReturnProcessingDetails

ReturnProcessingDetails	
Diagrama	
Descripción	Este elemento opcional indica al servidor que el cliente desea obtener el resultado de cada tarea de verificación que constituye el proceso de validación de un sello de tiempo.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

6.2.2 Mensaje XML de Respuesta

En la siguiente figura podemos observar los distintos componentes que pueden formar una respuesta de validación de sello de tiempo:

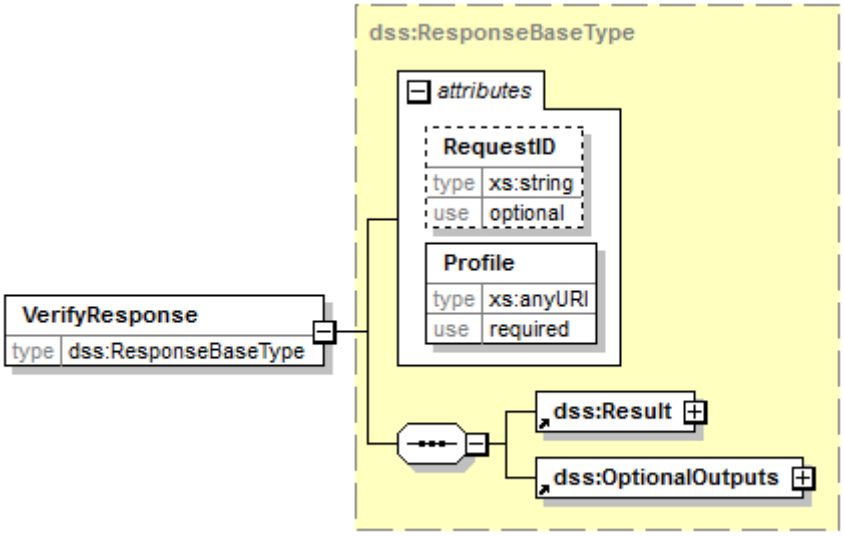


Como se observa en la anterior figura la respuesta de validación de sello de tiempo *dss:VerifyResponse* esta compuesta por dos elementos:

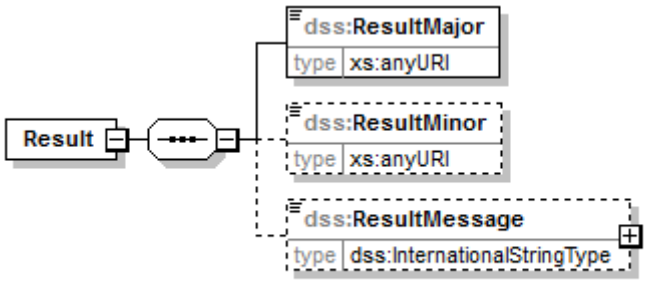
- *dss:Result.* Componente que recoge el resultado final del proceso.
- *dss:OptionalOutputs.* Componente que recoge elementos opcionales, en concreto:
    - *dss:SigningTimeInfo.* Elemento que incluye la fecha de generación del sello de tiempo y su posible desviación.
    - *dss:ProcessingDetails.* Elemento que recoge el resultado detallado sobre cada una de las validaciones realizadas en el proceso de validación del sello de tiempo.

A continuación se detalla dicho elemento.

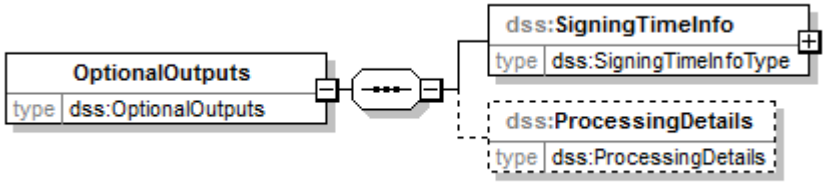
6.2.2.1 dss:VerifyResponse

VerifyResponse		
Diagrama		
Descripción	Elemento raíz de la respuesta a una petición de validación de sello de tiempo.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Result.* Este componente se describe en el apartado 6.2.2.2. • *dss:OptionalOutpus.* Este componente se describe en el apartado 6.2.2.3.	
Atributos	**Nombre**	**Descripción**
	Profile	URI que indica el perfil que implementa el servidor. En este caso, el valor del atributo siempre será **urn:oasis:names:tc:dss:1.0:profiles:timestamping**.
	RequestID	Identificador de la petición origen. En caso de haberse especificado un identificador en la petición, se devolverá el mismo valor.

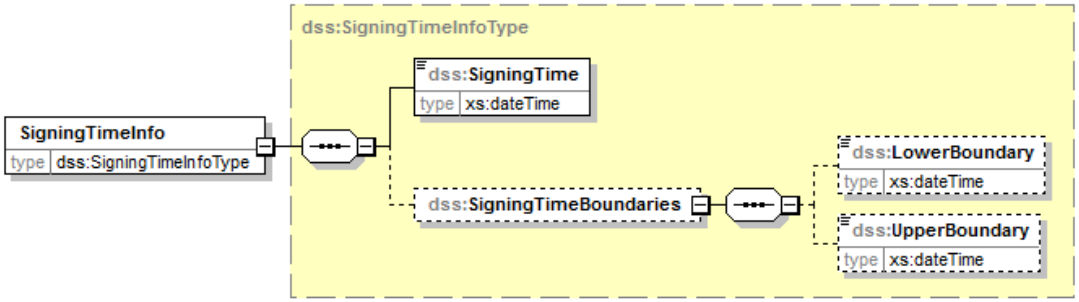
6.2.2.2 dss:Result

Result	
Diagrama	
Descripción	Elemento que contiene el resultado del proceso de validación del sello de tiempo.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:ResultMajor.* Componente que indica, mediante una URI, el resultado global del proceso. En el anexo A.2.2 se detallan los distintos valores que puede tomar. • *dss:ResultMinor.* Elemento que especifica mediante una URI el resultado indicado en el componente anterior. En el anexo A.2.2 se detallan los distintos valores que puede tomar. • *dss:ResultMessage*. Componente que presenta un mensaje descriptivo del resultado del proceso.

6.2.2.3 dss:OptionalOutputs

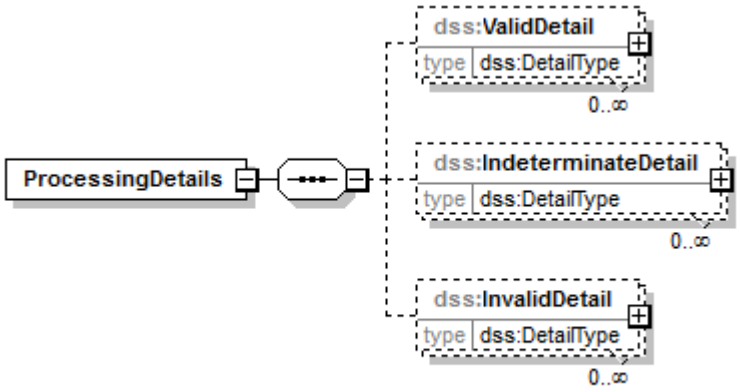
OptionalOutputs	
Diagrama	
Descripción	Elemento que contiene parámetros adicionales de la respuesta definidos en [DSS_CORE].
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:SigningTimeInfo.* Componente que informa sobre la fecha de generación del sello de tiempo y su posible desviación. Este componente se describe en el apartado 6.2.2.4. • *dss:ProcessingDetails.* Elemento que recoge el resultado detallado sobre cada una de las validaciones realizadas en el proceso de validación del sello de tiempo. Este componente se describe en el apartado 6.2.2.5.

6.2.2.4 dss:SigningTimeInfo

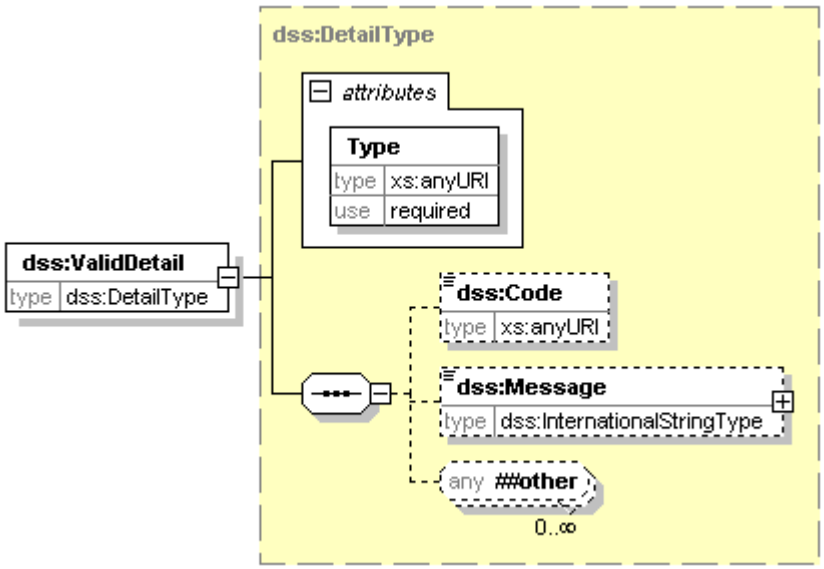
OptionalOutputs	
Diagrama	
Descripción	Elemento que contiene información acerca de la fecha de generación del sello de tiempo y su posible desviación.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

Hijos	• *dss:SigningTime.* Componente que contiene la fecha de generación del sello de tiempo.
	• *dss:SigningTimeBoundaries.* Componente que incluye información sobre la desviación admitida para la fecha de generación del sello de tiempo. Como hijos posee dos elementos:
	  ○ *dss:LowerBoundary.* Elemento que establece el límite inferior en la desviación.
	  ○ *dss:UppderBoundary.* Elemento que establece el límite superior en la desviación.

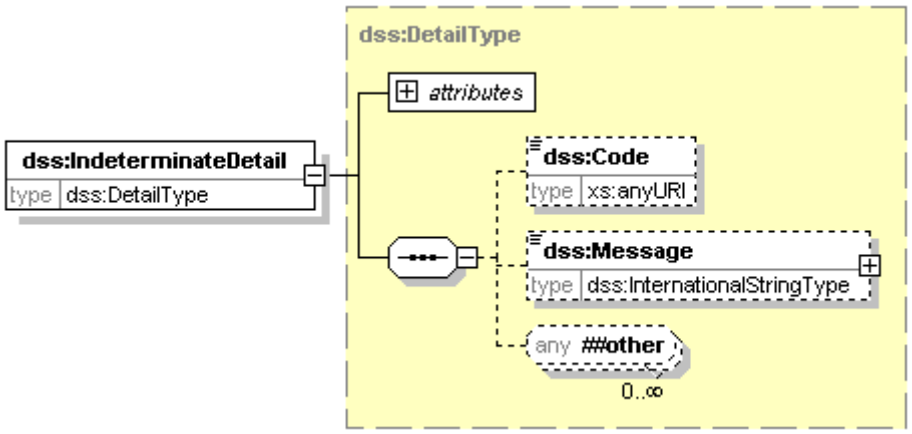
6.2.2.5 dss:ProcessingDetails

ProcessingDetails	
Diagrama	
Descripción	Elemento que contiene el resultado de los distintos pasos que forman el proceso de verificación de un sello de tiempo.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:ValidDetail.* Componente que contiene una tarea de validación que ha arrojado un resultado satisfactorio. Este componente se describe en el apartado 6.2.2.6. • *dss:IndeterminateDetail.* Componente que contiene una tarea de validación que ha arrojado un resultado indeterminado. Este componente se describe en el apartado 6.2.2.7. • *Dss:InvalidDetail.* Componente que contiene una tarea de validación que ha arrojado un resultado no satisfactorio. Este componente se describe en el apartado 6.2.2.8.

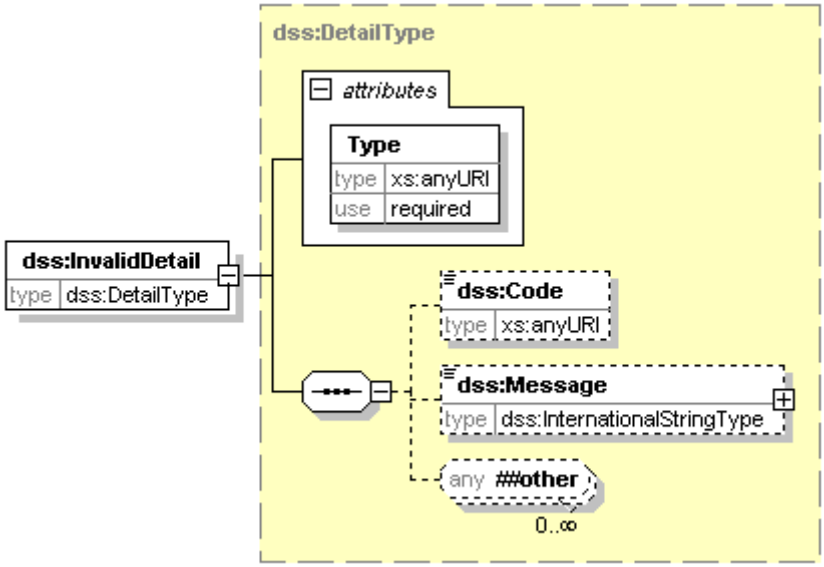
6.2.2.6 dss:ValidDetail

ValidDetail		
Diagrama		
Descripción	Elemento que contiene la información asociada a una tarea de validación que arroja un resultado satisfactorio.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Code.* URI que especifica el resultado anterior. En este perfil no se especifican valores para los casos de validación satisfactoria. • *dss:Message.* Cadena literal con un mensaje descriptivo del resultado del proceso.	
Atributos	**Nombre**	**Descripción**
	Type	URI que identifica la tarea de validación ejecutada. En el anexo se detallan los valores posible para este atributo

6.2.2.7 dss:IndeterminateDetail

IndeterminateDetail		
Diagrama		
Descripción	Componente que contiene información sobre la ejecución de una tarea de validación que arroja un resultado indefinido.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Code.* URI que especifica el resultado anterior. En el anexo A.2.3 se detallan las URI´s que puede tomar como valor este elemento. • *dss:Message.* Cadena literal con un mensaje descriptivo del resultado del proceso.	
Atributos	**Nombre**	**Descripción**
	Type	URI que identifica la tarea de validación ejecutada. En el anexo se detallan los valores posible para este atributo

6.2.2.8 dss:InvalidDetail

InvalidDetail		
Diagrama		
Descripción	Elemento que contiene la información asociada a una tarea de validación que arroja un resultado no satisfactorio.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Code.* URI que especifica el resultado anterior. En el anexo A.2.3 se detallan las URI´s que puede tomar como valor este elemento. • *dss:Message.* Cadena literal con un mensaje descriptivo del resultado del proceso.	
Atributos	**Nombre**	**Descripción**
	Type	URI que identifica la tarea de validación ejecutada. En el anexo se detallan los valores posibles para este atributo.

6.3 Servicio de Renovación de Sello de Tiempo. Servicio discontinuado (deprecated).

El servicio de re-sellado (RenewTimeStampWS) permite la renovación de un sello de tiempo existente mediante un certificado alojado en la plataforma, en este caso el cliente delega el proceso de firma a la plataforma.

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

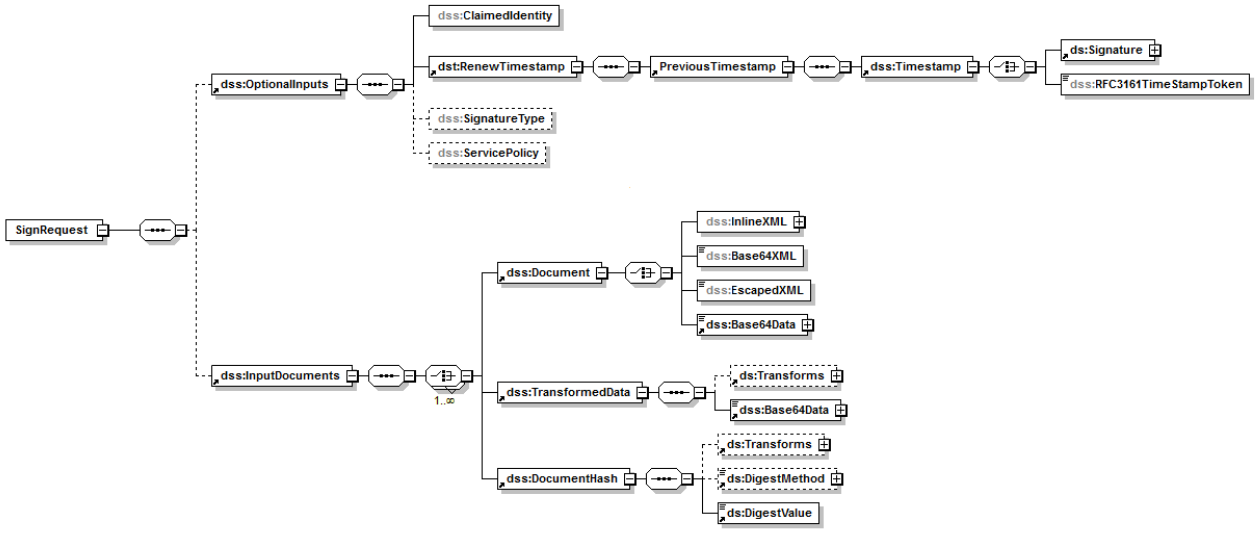
- ***dss:SignRequest***: Elemento XML de petición de renovación de sello de tiempo.

- ***dss:SignResponse***: Elemento XML de respuesta de renovación de sello de tiempo.

A continuación se detalla la definición de dichos elementos.

6.3.1 Mensaje XML de Petición

En la siguiente figura podemos observar los distintos componentes que pueden formar una petición de renovación de sello de tiempo:



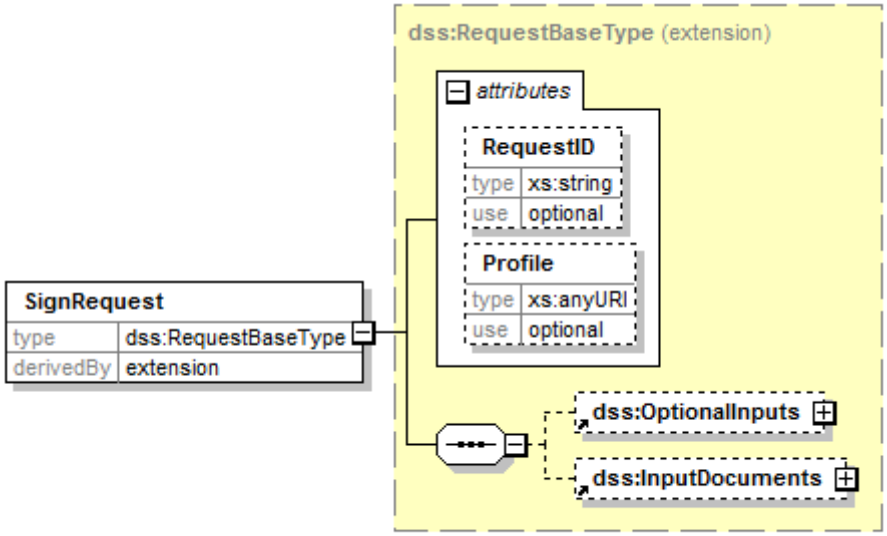
Como se observa en la anterior figura la petición de firma *dss:SignRequest* esta compuesta por dos elementos diferenciados:

- *dss:InputDocument.* Elemento que recoge el documento a ser sellado, o una referencia al mismo. La información de los datos a ser firmados puede incluirse de las siguientes formas:
    - Incluyendo el documento en un elemento *dss:Document*.
    - Incluyendo el documento en un elemento *dss:TransformedData*.
    - Incluyendo el documento en un elemento *dss:DocumentHash*.
- *dss:OptionalInput.* Elemento que incluye la información necesaria para que el servidor pueda realizar el sellado de los datos pasados en el anterior componente, para esta implementación

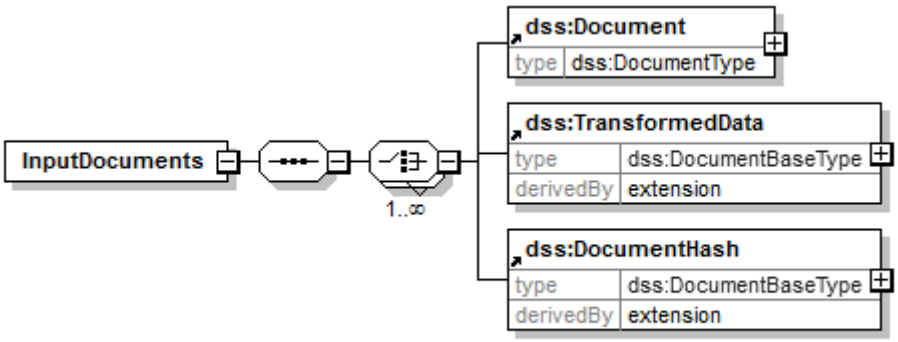
del perfil existen dos parámetros obligatorios, caso del identificador de aplicación (contenido en el componente *dss:ClaimedIdentity*) y del sello de tiempo anterior (contenido en el componente *dst:RenewTimeStamp*). Adicionalmente este componente permite incluir parámetros adicionales como son el tipo de sello de tiempo a generar (componente *dss:SignatureType*), y la política de sello de tiempo (componente *dss:ServicePolicy*).

A continuación se detalla cada elemento.

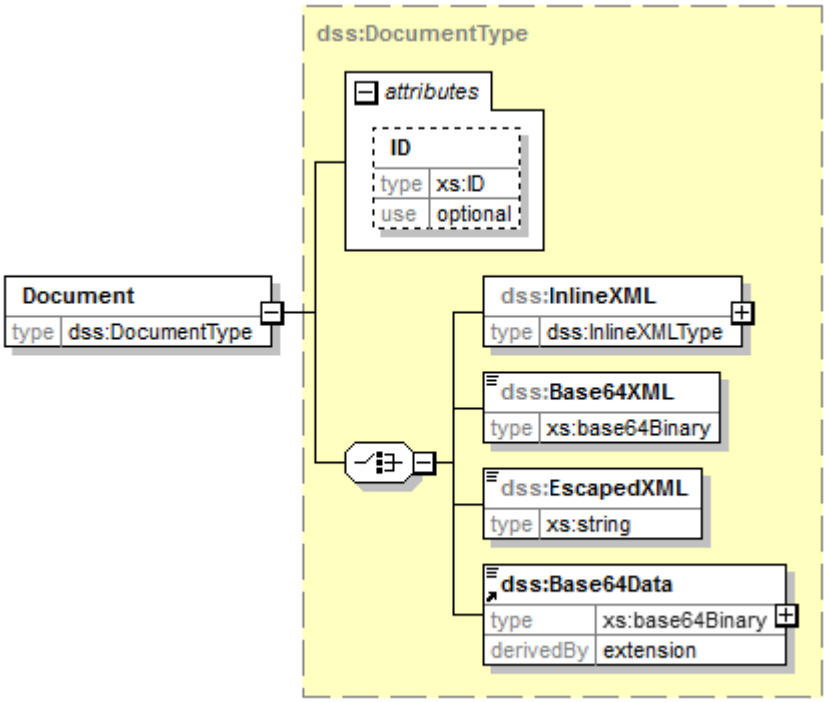
6.3.1.1 dss:SignRequest

SignRequest		
Diagrama		
Descripción	Componente introducido en las especificaciones [DSS_CORE] y que constituye el elemento raíz de una petición de re-sellado.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:OptionalInputs.* Este componente se describe en el apartado 6.3.1.10. • *dss:InputDocuments.* Este componente se describe en el apartado 6.3.1.2.	
Atributos	**Nombre**	**Descripción**
	Profile	Identificador del perfil soportado por el servicio. Para peticiones de re-sellado a la plataforma, el valor de este atributo será: **urn:oasis:names:tc:dss:1.0:profiles:timestamping.** Esta URI identifica al perfil Timestamping de OASIS.
	RequestID	Identificador alfanumérico que permite relacionar la petición con la respuesta asociada a la misma.

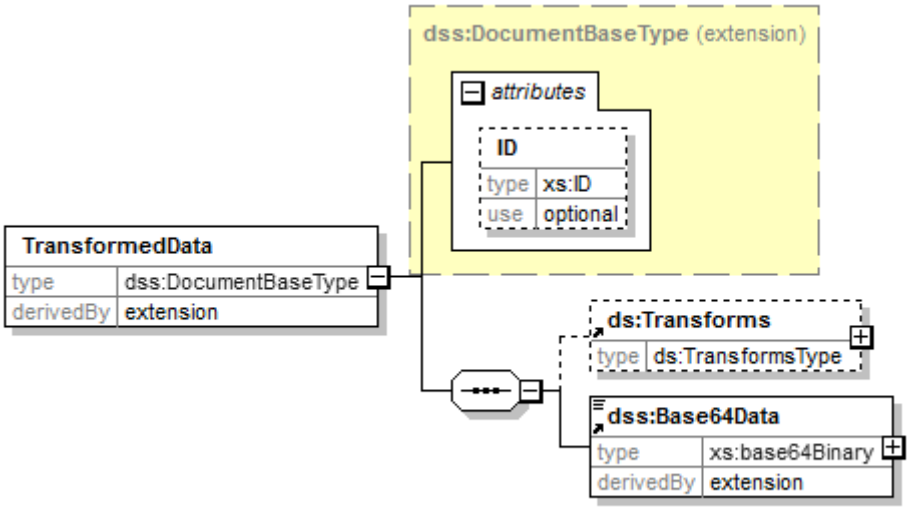
6.3.1.2 dss:InputDocuments

InputDocuments	
Diagrama	
Descripción	Este elemento contendrá el documento o datos que van a ser re-sellados. Dicho documento, o datos, deben ser los mismos que fueron sellados por el sello de tiempo previamente existente.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:Document*. Este elemento se describe en el apartado 6.3.1.3. • *dss:TransformedData*. Este elemento se describe en el apartado 6.3.1.4. • *dss:DocumentHash.* Este elemento se describe en el apartado 6.3.1.5.

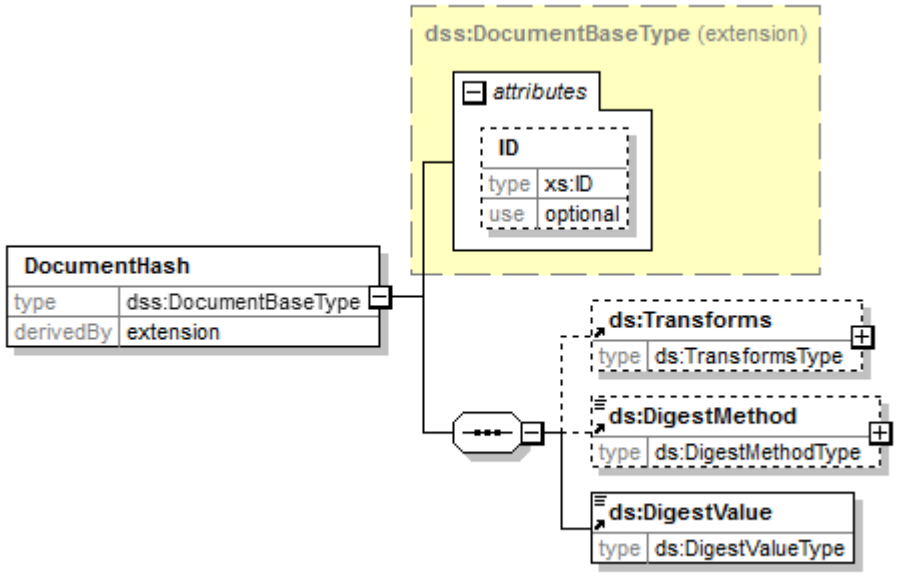
6.3.1.3 dss:Document

Document		
Diagrama		
Descripción	Este elemento contendrá los datos a re-sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Base64Data*. Este elemento se describe en el apartado 6.3.1.6. • *dss:Base64XML*. Este elemento se describe en el apartado 6.3.1.7. • *dss:InlineXML*. Este elemento se describe en el apartado 6.3.1.8. • *dss:EscapedXML*. Este elemento se describe en el apartado 6.3.1.9.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

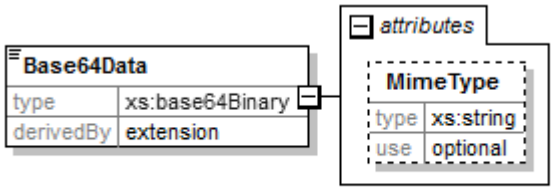
6.3.1.4 dss:TransformedData

TransformedData		
Diagrama		
Descripción	Este elemento contendrá los datos a re-sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *ds:Transforms*. Elemento que contiene la lista de transformadas aplicadas sobre los datos. • *dss:Base64Data*. Este elemento se describe en el apartado 6.3.1.6.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

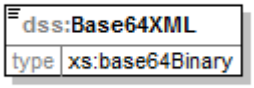
6.3.1.5 dss:DocumentHash

DocumentHash		
Diagrama		
Descripción	Este elemento contendrá los datos a re-sellar.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *ds:Transforms*. Elemento que contiene la lista de transformadas aplicadas sobre los datos. • *ds:DigestMethod*. Elemento que especifica el algoritmo de resumen usado para calcular el resumen de los datos canonicalizados en base a las transformadas indicadas por el elemento anterior. • *ds:DigestValue*. Elemento que especifica el valor del resumen de los datos canonicalizados.	
Atributos	**Nombre**	**Descripción**
	ID	Identificador único dentro del XML que permitiría ser referenciado desde otro elemento de la petición.

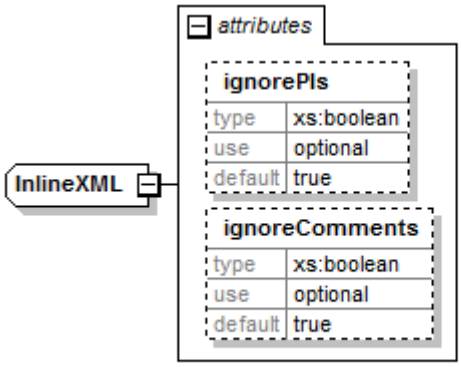
6.3.1.6 dss:Base64Data

Base64Data		
Diagrama		
Descripción	Este elemento contendrá datos, en formato diferente a XML, codificados en Base64.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	**Nombre**	**Descripción**
	MimeTye	Indicador del tipo de datos contenidos.

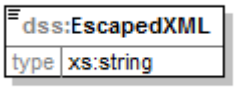
6.3.1.7 dss:Base64XML

Base64XML	
Diagrama	
Descripción	Este elemento contendrá datos, en formato XML, codificados en Base64.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

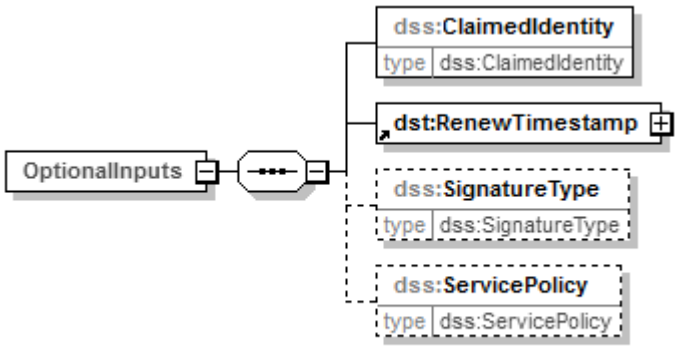
6.3.1.8 dss:InlineXML

InlineXML		
Diagrama		
Descripción	Este elemento contendrá un documento completo en formato XML, pero sin saltos de línea ni retornos de carro.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Atributos	**Nombre**	**Descripción**
	IgnoresPIs	Indicador para ignorar, o no, las instrucciones de procesamiento del documento XML completo.
	IgnoreComments	Indicador para ignorar, o no, los comentarios en el documento XML completo.

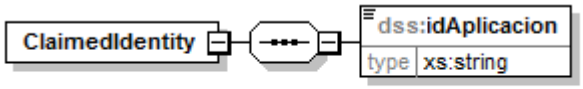
6.3.1.9 dss:EscapedXML

EscapedXML	
Diagrama	
Descripción	Este elemento contendrá datos en formato XML escapados.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

6.3.1.10 dss:OptionalInputs

OptionalInputs	
Diagrama	
Descripción	Este elemento contendrá parámetros adicionales de la petición.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:ClaimedIdentity*. Este elemento se describe en el apartado 6.3.1.11. • *dst:RenewTimestamp.* Este elemento se describe en el apartado 6.3.1.12. • *dss:SignatureType*. Este elemento se describe en el apartado 6.3.1.13. • *dss:ServicePolicy*. Este elemento se describe en el apartado 6.3.1.14.

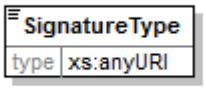
6.3.1.11 dss:ClaimedIdentity

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

6.3.1.12 dss:RenewTimestamp

RenewTimestamp	
Diagrama	
Descripción	Este elemento indica al servidor que la actual petición de sello de tiempo es, efectivamente, una solicitud de renovación de un sello de tiempo (re-sellado) sobre unos datos que fueron sellados en el pasado, por lo que el período de validez del sello de tiempo existente se extiende. Su inclusión es obligatoria, por tanto, por tratarse de una operación de renovación de un sello de tiempo.
Namespace	urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema
Hijos	• *dst:PreviousTimestamp*. Este elemento se describe en el apartado 6.3.1.15.

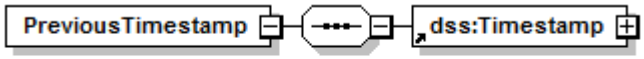
6.3.1.13 dss:SignatureType

SignatureType	
Diagrama	
Descripción	Este elemento permite identificar el tipo de sello de tiempo a generar mediante su URI. Su inclusión es opcional, si bien, en caso de no incluirse, se procederá a generar un sello de tiempo de tipo XML, pues es el único formato de sello de tiempo admitido para el re-sellado. En el anexo se detalla la URI asociada al formato de sello de tiempo XML.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

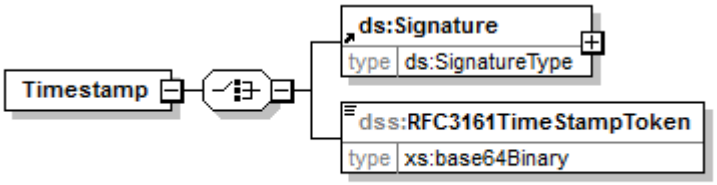
6.3.1.14 dss:ServicePolicy

ServicePolicy	
Diagrama	
Descripción	Este elemento permite identificar la política de sello de tiempo a utilizar en la generación del sello de tiempo por medio de la inclusión de su URI, establecida en el proceso de alta de la política de sello de tiempo en el sistema. Su inclusión es opcional.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema

6.3.1.15 dss:PreviousTimestamp

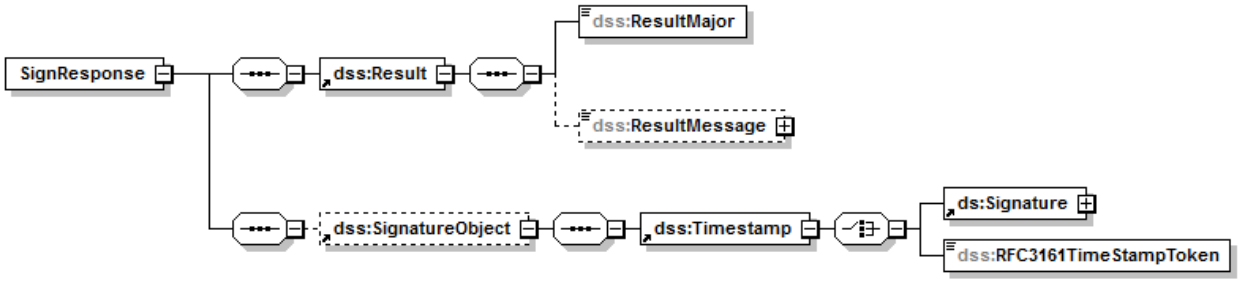
PreviousTimestamp	
Diagrama	
Descripción	Este elemento contiene el sello de tiempo anterior.
Namespace	urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema
Hijos	• *dss:Timestamp*. Este elemento se describe en el apartado 6.3.1.16.

6.3.1.16 dss:Timestamp

Timestamp	
Diagrama	
Descripción	Elemento que representa el sello de tiempo anterior.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	▪ *ds:Signature.* Este elemento se corresponde con el sello de tiempo en formato XML. Para más información acerca de este elemento se recomienda acudir a los documentos [DSS_CORE] y [XML_TIMESTAMP]. ▪ *dss:RFC3161TimeStampToken*. Este elemento se corresponde con el sello de tiempo ASN.1 codificado en Base64, según define [RFC3161].

6.3.2 Mensaje XML de Respuesta

En la siguiente figura podemos observar los distintos componentes que pueden formar una respuesta de renovación de sello de tiempo:

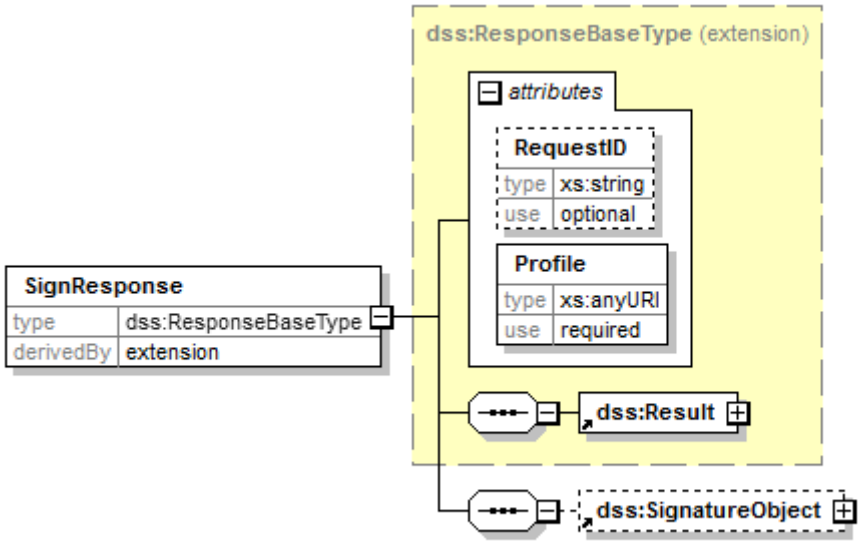


Como se observa en la anterior figura la respuesta de renovación de sello de tiempo *dss:SignResponse* está compuesta por dos elementos diferenciados:

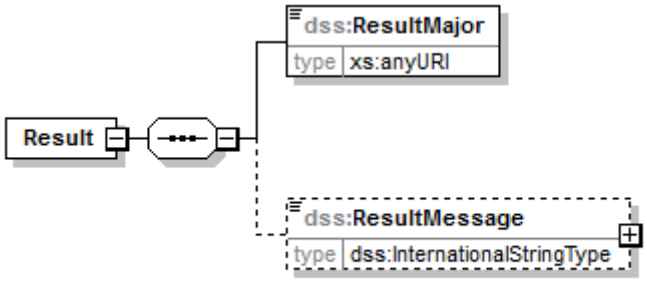
- *dss:Result.* Componente que recoge el resultado final del proceso.
- *dss:SignatureObject.* Componente que contiene el sello de tiempo renovado sobre el sello de tiempo anterior.

A continuación se detalla cada elemento.

6.3.2.1 dss:SignResponse

SignResponse		
Diagrama		
Descripción	Elemento raíz de la respuesta a una petición de re-sellado.	
Namespace	urn:oasis:names:tc:dss:1.0:core:schema	
Hijos	• *dss:Result.* Este componente se describe en el apartado 6.3.2.2. • *dss:SignatureObject.* Este componente se describe en el apartado 6.3.2.3,	
Atributos	**Nombre**	**Descripción**
	Profile	URI que indica el perfil que implementa el servidor. En este caso, el valor del atributo siempre será **urn:oasis:names:tc:dss:1.0:profiles:timestamping**.
	RequestID	Identificador de la petición origen. En caso de haberse especificado un identificador en la petición, se devolverá el mismo valor.

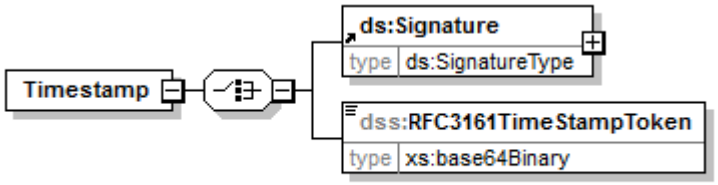
6.3.2.2 dss:Result

Result	
Diagrama	
Descripción	Elemento que contiene el resultado del proceso de generación de sello de tiempo.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	• *dss:ResultMajor.* Componente que indica, mediante una URI, el resultado global del proceso. En el anexo se detallan los distintos valores que puede tomar. • *dss:ResultMessage*. Componente que, en el caso de estar presente, ofrece un mensaje descriptivo del resultado del proceso.

6.3.2.3 dss:SignatureObject

SignatureObject	
Diagrama	
Descripción	Elemento que contiene el sello de tiempo renovado.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	▪ *dss:Timestamp.* Este elemento se describe en el apartado 6.3.2.4.

6.3.2.4 dss:Timestamp

Timestamp	
Diagrama	
Descripción	Elemento que representa el sello de tiempo renovado.
Namespace	urn:oasis:names:tc:dss:1.0:core:schema
Hijos	▪ *ds:Signature.* Este elemento se corresponde con el sello de tiempo en formato XML. Para más información acerca de este elemento se recomienda acudir a los documentos [DSS_CORE] y [XML_TIMESTAMP]. Dado que es un sello de tiempo generado a partir de otro existente, dentro de este elemento se incluye el sello de tiempo anterior.

ANEXO

A.1 Descripción de los Elementos utilizados en los Diagramas

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

- **Elemento Simple Obligatorio.**



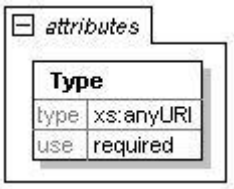
El rectángulo representa un elemento y al ser un rectángulo de borde continuo indica que el elemento es requerido. El nombre de este elemento es <*dss:ResultMayor*> y el tipo es "*xs:anyURI*"

- **Elemento Simple Opcional.**



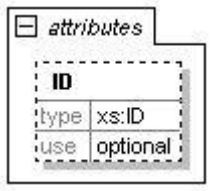
El rectángulo informa que se trata de un elemento y el borde discontinuo que el elemento es opcional. El nombre de este elemento es <*dss:ResultMessage*> y el tipo es "*dss:InternationalStringType*"

- **Atributo Obligatorio.**



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

- **Atributo Opcional.**

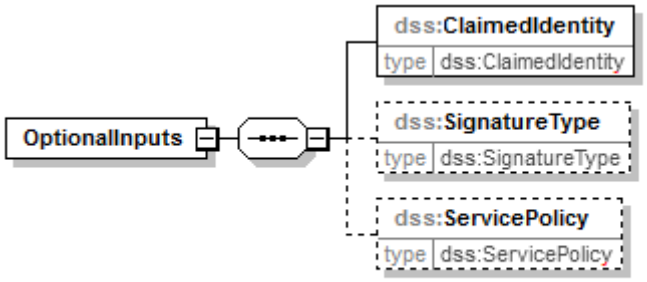


Un rectángulo con la etiqueta "*attributes*" indica que el elemento que contiene es un atributo. Si el rectángulo que describe al atributo tiene los bordes discontinuos el elemento será opcional. El nombre de este atributo es "*ID*" y el tipo es "*xs:ID*"

- **Elementos de Composición.**

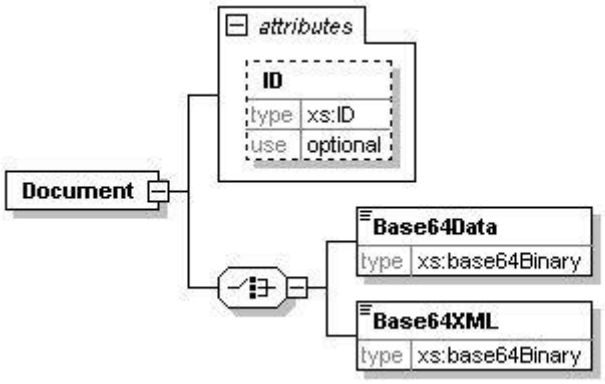
En este documento solamente se utilizan los elementos de composición "*sequence*" y "*choice*" los cuales tienen la representación que se muestra a continuación.

- **Sequence**



El elemento <*OptionalInputs*> está compuesto de la secuencia de elementos <*dss:ClaimedIdentity*>, <*dss:SignatureType*> y <*dss:ServicePolicy*>.

- **Choice**



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

A.2 Identificadores

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

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

A.2.1 Identificadores de Tipo de Sello de Tiempo

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

Formato	Identificador
XML	urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken
ASN.1	urn:ietf:rfc:3161

A.2.2 Identificadores de resultado del proceso

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

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

ResultMajor
urn:oasis:names:tc:dss:1.0:resultmajor:Success
El proceso se ha realizado satisfactoriamente
urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError
La petición no es correcta
urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError
Se ha producido un error al realizar el proceso en el servidor
urn:oasis:names:tc:dss:1.0:resultmajor:Warning
Durante la ejecución del proceso se ha detectado algún evento que debe advertirse al Cliente

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

ResultMinor
urn:oasis:names:tc:dss:1.0:resultminor:invalid:IncorrectSignature
El sello de tiempo no es correcto
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:KeyCompromised
La clave privada del certificado firmante se ha visto comprometida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:NotSupported
El certificado firmante no está soportado por la plataforma de firma y validación @firma
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:NotAllowed
El certificado no se encuentra entre los habilitados para la aplicación cliente definida en la plataforma de firma y validación @firma
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:InvalidSignature
La firma del certificado no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:IncorrectIssuer
El emisor del certificado no es válido
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:NotValidYet
El certificado aún no era válido en el momento de generación del sello de tiempo
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:UnknownStatus
No ha sido posible determinar el estado del certificado
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:InvalidCertificateChain
La cadena de certificación del certificado no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:Revoked
El certificado firmante estaba revocado en el momento de generación del sello de tiempo
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:Expired
El certificado se encontraba caducado en el momento de generación del sello de tiempo
urn:afirma:dss:1.0:profile:XSS:resultminor:SignerCertificate:WithoutTimestampingExtension
El certificado firmante no posee la extensión “id-kp-timeStamping”

urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:InvalidSignature
El núcleo de firma del sello de tiempo no es correcto
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:InvalidReference
La referencia al sello de tiempo no es válida
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:OrphanedReference
Se ha encontrado una referencia hacia un elemento no incluído en el sello de tiempo
urn:afirma:dss:1.0:profile:XSS:resultminor:SignatureCore:MismatchedSignedData
Los datos sellados por el sello de tiempo no coinciden con los datos indicados en la petición
urn:oasis:names:tc:dss:1.0:resultminor:NotSupported
No se permite definir "urn:ietf:rfc:3161" como formato destino en la renovación de sellos de tiempo
urn:oasis:names:tc:dss:1.0:resultminor:GeneralError
Se ha producido un error no categorizado

A.2.3 Identificadores de tareas de verificación

En este anexo se detalla las URI´s utilizadas para identificar las distintas tareas y resultados que forman el proceso de validación de un sello de tiempo.

El proceso de validación de un sello de tiempo se puede dividir en un conjunto de subprocesos que determinarán el estado del mismo. El formato del sello de tiempo determinará qué resultados pueden obtenerse.

En la siguiente tabla se representan las URI's que permiten identificar las tareas mencionadas. En la columna "Identificador" se representan los identificadores de las tareas de verificación, que se corresponden con los que puede tener el atributo "Type" de los elementos "*dss:ValidDetail*", "*dss:InvalidDetail*" o "*dss:IndeterminateDetail*":

Tarea	Identificador[1]	Descripción
Validación Estructural del Sello de Tiempo	SignatureStructure	Consiste en comprobar que el sello de tiempo posee una estructura correcta
Validación del Certificado Firmante	SignerCertificateValidation	Consiste en analizar el certificado firmante del sello de tiempo

[1] Los valores expuestos en la columna deben ir precedidos por la cadena de texto "urn:afirma:dss:1.0:profile:XSS:detail:".

Validación del Núcleo de Firma	SignatureCore	Consiste en analizar el núcleo de la firma que compone el sello de tiempo

Durante la ejecución de una tarea de verificación se puede obtener un resultado no satisfactorio. En la siguiente tabla se representan los errores identificados en este perfil para cada una de las tareas anteriormente expuestas. En la columna "Identificador" se representan los identificadores de resultado para la tarea en cuestión, que se corresponden con los que pueden incluirse en los elementos "*dss:Code*" de los componentes "*dss:InvalidDetail*" o "*dss:IndeterminateDetail*":

Tarea	Identificador[2]	Descripción
Validación Estructural del Sello de Tiempo	code:GeneralError	Se ha producido un error no categorizado
	SignatureStructure:code:InvalidTimestamp	El sello de tiempo está mal formado estructuralmente
Validación del Certificado Firmante	code:GeneralError	Se ha producido un error no categorizado
	Certificate:code:KeyCompromised	La clave privada del certificado firmante se ha visto comprometida
	Certificate:code:NotSupported	El certificado firmante no está soportado por la plataforma de firma y validación @firma
	Certificate:code:NotAllowed	El certificado no se encuentra entre los habilitados para la aplicación cliente definida en la plataforma de firma y validación @firma
	Certificate:code:InvalidSignature	La firma del certificado no es válida
	Certificate:code:IncorrectIssuer	El emisor del certificado no es válido
	Certificate:code:NotValidYet	El certificado aún no era válido en el momento de generación del sello de tiempo
	Certificate:code:UnknownStatus	No ha sido posible determinar el estado del certificado
	Certificate:code:InvalidChain	La cadena de certificación del

[2] Los valores expuestos en la columna deben ir precedidos por la cadena de texto "urn:afirma:dss:1.0:profile:XSS:detail:".

		certificado no es válida
	Certificate:code:Revoked	El certificado firmante estaba revocado en el momento de generación del sello de tiempo
	Certificate:code:Expired	El certificado se encontraba caducado en el momento de generación del sello de tiempo
	Certificate:code:IdKpTimestampingExtensionNotFound	El certificado firmante no posee la extensión "id-kp-timeStamping"
Validación del Núcleo de Firma	code:GeneralError	Se ha producido un error no categorizado
	SignatureCore:code:InvalidSignature	El sello de tiempo se encuentra mal formado
	SignatureCore:code:MismatchedSignedData	Los datos sellados por el sello de tiempo no coinciden con los datos indicados en la petición
	SignatureCore:code:OrphanedReference	Se ha encontrado una referencia hacia un elemento no encontrado
	SignatureCore:code:InvalidReference	La referencia al sello de tiempo no es válida

A.3 Ejemplos de Peticiones y Respuesta

La plataforma TS@ basa su comunicación con las aplicaciones cliente en el protocolo WS-Security (descrito en [WS_SECURITY]). En concreto, para las peticiones SOAP, son 3 los métodos admitidos:

+ **Autenticación por Usuario y Contraseña.** Perfil UsernameToken descrito en [USERNAME_TOKEN].

+ **Autenticación por Certificado.** Perfil X.509 Certificate descrito en [CERTIFICATE_TOKEN]. En este caso, además, las peticiones pueden ir *encriptadas*.

+ **Autenticación por SAML.** Perfil SAML Token descrito en [SAML_TOKEN]. En este caso, además, las peticiones pueden ir *encriptadas*.

Por su parte, la plataforma puede devolver las respuestas de 2 maneras:

- **No Firmadas.**

- **Firmadas.** En este caso, además, las respuestas pueden ir *encriptadas*. Para identificar las maneras en que se puede firmar la respuesta se indica cuál es el "*token de seguridad*" que compone la firma de la respuesta. Las posibilidades son:

    - BinarySecurityToken

    - KeyIdentifier

    - X509IssuerSerial

    - SAMLToken

A continuación se detallan distintos ejemplos de peticiones y respuestas DSS a los servicios detallados en el presente documento, haciendo uso del protocolo WS-Security.

A.3.1 Ejemplos de Generación de Sello de Tiempo

Ejemplo 1. Solicitud de Generación de Sello de Tiempo ASN.1

Petición:

- Securización de la Cabecera SOAP: Usuario y Contraseña

- InputDocument: Document/Base64Data

- Petición Encriptada con Clave Simétrica: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413472481520-1830889046">
```

```
                <wsse:Username>a</wsse:Username>
                <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordDigest">****</wsse:Password>
                <wsse:Nonce EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary">oUg0sviK/CIa1X6MAMADcIoS</wsse:Nonce>
                <wsu:Created>2014-10-16T15:14:41.584Z</wsu:Created>
            </wsse:UsernameToken>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body>
        <dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
            <dss:OptionalInputs>
                <dss:SignatureType>urn:ietf:rfc:3161</dss:SignatureType>
                <dss:ClaimedIdentity>
                    <dss:idAplicacion>appPrueba</dss:idAplicacion>
                </dss:ClaimedIdentity>
            </dss:OptionalInputs>
            <dss:InputDocuments>
                <dss:Document>

<dss:Base64Data>RmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFu
IG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNl
cnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVh
bGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRp
bGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmlj
aGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywg
byBjb3VudGVyLg0KR
```

bGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmlj
aGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywg
byBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFu
IG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNl
cnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVh
bGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRp
bGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmlj
aGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywg
byBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFu
IG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNl
cnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVh
bGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRp
bGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmlj
aGVyby9ldHxwbyBxdWUgc2VhbGl0YmV6YXJ9fGx0YXIgZ2VhbGVzYXIgZ2VhbGVjbHxmb2Jh
bHBvcHwxYXogZ2YwcGZ6ZzGGzGVyBoZ2jZ8GzGzGZ6ZzGjZ8GSzGVyLCB0bSzZ6ZzGjZ6jZ8GzGzGZ6ZzGjZ6jZ8GzGzGZ6ZzGj
PERSMGVyLGwgbXRyZ2jZ8GGzGVyLGwgbXRyZ6jZ8GGzGVyLGwgbXRyZ6jZ8GGzGVyLGwgbXRyZ6jZ8GGzGVyLjVyLGwgbXRyZ6jZ1
PERSMGVyLGwgbXhIGVyLGVyLGwgbXRyZ6jZ8GGzGVyLGwgbXRyZ8GGzGVyLGwgbXRyZ8GSzGVyLGwgbXhIGVyLGwgbXhIGVyLGwgMS
Z1PERSMGVyLGwgbXRyZ6SzGVyLGwgbXhIGVyLGwgbXRyZ8GSzGVyLGwgbXRyZ8GSzGVyLGwgbXhIGVyLGwgMS
PERSMGVyLGwgbXRyZ6SzGVyLGwgbXhIGVyLGwgbXRyZ8GSzGVyLGwgbXRyZ8GSzGVyLGwgbXhIGVyLGwgMS
PERSMGVyLGwgbXRyZ6SzGVyLGwgbXhIGVyLGwgbXRyZ8GSzGVyLGwgbXRyZ8GSzGVyLGwgbXhIGVyLGwgMS

```
byBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFu
IG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNl
cnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVh
bGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRp
bGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0K</ds
s:Base64Data>
                </dss:Document>
            </dss:InputDocuments>
        </dss:SignRequest>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: No


```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <dss:SignResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-bd6cd6f2-9300-4e91-963b-
0c189c66cb0b">
            <dss:Result>
                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            </dss:Result>
            <dss:SignatureObject>
                <dss:Timestamp>

<dss:RFC3161TimeStampToken>MIAGCSqGSIb3DQEHAqCAMIIHyAIBAzELMAkGBSsOAwIaBQAwagYLKoZIhvcNAQkQAQSgWwRZM
FcCAQEGBSoDBAUGMCEwCQYFKw4DAhoFAAQUySErJYEqdFwOFyp2icgkiDF/MiQCCBOdo14M6bWdGBMyMDE0MTAxNjE1MTQ0MS44O
DJaMAkCAQKAAQGBAQGgggUrMIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU
3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xM
jEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50M
SAwHgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFU
zCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebq
z4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3F
eh54cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi
5jDBMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwg
gHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZ
GlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1Nlc
nZpY2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEG
DAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwO
DAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsd
mVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4r
vVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpAB
wE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6
pfClWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/
ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3MYICGTCCAhUCA
QEwYzBXMRQwEgYDVQQDDAtBZmlybWFTdWJDQTEgMB4GA1UECwwXVGVsdmVudCBHbG9iYWwgU2VydmljZXMxEDAOBgNVBAoMB1Rlb
HZlbnQxCzAJBgNVBAYTAkVTAggcbqJjqBfPZTAJBgUrDgMCGgUAoIGMMBoGCSqGSIb3DQEJAzENBgsqhkiG9w0BCRABBDAcBgkqh
kiG9w0BCQUxDxcNMTQxMDE2MTUxNDQxWjAjBgkqhkiG9w0BCQQxFgQUcolJjtfgLL8+iKSv73FwDwJEkZEwKwYLKoZIhvcNAQkQA
gwxHDAaMBgwFgQUCy2O7ZpW2Svo/nFZvnZdr3jvdjAwDQYJKoZIhvcNAQEBBQAEggEAZ8whnP6TGRozWloB8x4ohTiodyBv3P0Uy
1u3IVRZHH552SFMe9oyQx+111JF2mgA9f+aq5fB15FR9eW0TGW0d0ZcgOQ7cY37mBFRSHAJlnKZLRoz2D8D2a5usJlZwvjsKDdMl
o8frCQUefSlZDJWiHn2fUwgaAGp38bm9st87DDdJNGT+7qqIrj6tj15dbv19+KHZO9KJCbOW6TNIs5Y/IOw/bRD4mjMzIq3mO4gS
tIQKmfAHafLDnE7dUVluMv/zmj9Ly7eNEe6h9D0bdBYsYrQiKB5L6nHcV3QUveyilUlB93JhhAau9qM30nvc8sRBW1gALgT/5u/K
XceKqSOcgAAAAA=</dss:RFC3161TimeStampToken>
                </dss:Timestamp>
            </dss:SignatureObject>
        </dss:SignResponse>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Ejemplo 2. Solicitud de Generación de Sello de Tiempo XML

Petición:

- Securización de la Cabecera SOAP: Certificado (Método de Inclusión del Certificado – Binary Security Token)
- InputDocument: Document/Base64XML
- Petición Encriptada con Clave Simétrica: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14134730255721461668007">
                <wsu:Created>2014-10-16T15:23:45.502Z</wsu:Created>
                <wsu:Expires>2014-10-16T15:28:45.502Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" 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="XWSSGID-14134730254 51-
337560492">MIIFRTCCBC2gAwIBAgIIFl4IlQK/pRkwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3ViQ0ExIDAeB
gNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEwMjMxMzAwM
jJaFw0xNTEwMjYxNTA0MThaMHMxEzARBgNVBAMMClNvYXBTaWduZXIxEDAOBgNVBAsMB1RlbHZlbnQxIDAeBgNVBAsMF1RlbHZlb
nQgR2xvYmFsIFNlcnZpY2VzMRswGQYDVQQKDBJTY2huZWlkZXIgRWxlY3RyaWMxCzAJBgNVBAYTAkVTMIIBIjANBgkqhkiG9w0BA
QEFAAOCAQ8AMIIBCgKCAQEAkch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0ptsmAVJ9OJ7D2gMv
PgQNJEOshdFyG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MPxKb4NZm5fFd1LGApXNEPZ0OCO
xpGkIMwn/YkHSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0aWqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u6+GuHKijZ5LUeV
rSpjcRq9Nhp+gVvqnaxVlmeRgG7C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQIDAQABo4IB9zCCAfMwga0GA1UdLgSBpTCBo
jCBn6CBnKCBmYaBlmh0dHA6Ly8xNzIuMjEuMjQzLjEwMjo4MDgwL2VqYmNhL3B1YmxpY3dlYi93ZWJkaXN0L2NlcnRkaXN0P2NtZ
D1kZWx0YWNybCZpc3N1ZXI9Q04lM2RBZmlybWFTdWJDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsd
mVudCUyY0MlM2RFUzAMBgNVHRMBAf8EAjAAMDsGA1UdJQQ0MDIGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwQGCCsGAQUFB
wMIBggrBgEFBQcDCTAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0c
DovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM
2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EB
AMCBPAwHQYDVR0OBBYEFAIYOhNZWFgafngAgs9tQ74e2yeYMA0GCSqGSIb3DQEBBQUAA4IBAQBmeMs+UdPMWY5Icyn97ZR//LOfk
6ElAfgxRs1y6DH1oJdiWUnVkHmSgGNY+Y4j4y74TMiH25naizyyKQzmGoHw7KOgTxxqUEwlEHZPuf5GIJxc+/a0askEItRRgf9po
zjL2+RS4YMU33xJlyBZNQ4nrvlKyNx50favpiKD2kOuHFqu3CypQzEvWw8uW5RY6Vvmujc3pztwjZtMeatWTbxMS8+c4wfT7N5bg
RFCH3t/Wu/yhKQlnfkXGLdpOeIt2pxIKH15UR7ODMmlNcIIRJQPoCPm5PWPmo24BkTb5U+nr1y4I5yY/gkIOammYYORPb10i1vx9
bRX1llTnWg4/YNX</wsse:BinarySecurityToken>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1413473025449-
1343337141">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-14134730255712523677777">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>rUVmEbQbc0IhJ5rl9J1p9f+GsxE=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-14134730255721461668007">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>2/xSczCHc+j0fliwl1IGCjiBnN4=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>OwLW36R26btNHogpbE2L49belV2Yje/BZF3XTBqdJnQPUwjsmjyaaKypTIq97vvjG8p5vmzSM4PP
Yst/50QViMooyqIf5xnVn4qkP7AHi+H2asSN8rGt3BikhYQIxmMdjh3hPAZh9ZJdRIL0z4I/JyVc
d440yHJF8N2Ztr4auua5rWjKNPp8Y7PN9Pm9GbbqjvWXqqbCtMX6UgetwtxvlAVlPWE+K2po+hPy
yLA9p5GZAsZjYqnaIlJghNqmiBFCsYu5lA9S1BY217fU07zbWpG7d6EMLWm6GQs/r92T0U4wmH0K
ghFR/ButebXrmqz6CQMS2jy9W89WiiMNQknTgA==</ds:SignatureValue>
                <ds:KeyInfo>
```

```
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413473025562-
1174063227">
                        <wsse:Reference URI="#XWSSGID-1413473025451-337560492"
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>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413473025571252367777">
        <dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
            <dss:OptionalInputs>

<dss:SignatureType>urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken</dss:SignatureType>
                <dss:ClaimedIdentity>
                    <dss:idAplicacion>appPrueba</dss:idAplicacion>
                </dss:ClaimedIdentity>
            </dss:OptionalInputs>
            <dss:InputDocuments>
                <dss:Document>

<dss:Base64XML>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiIHN0YW5kYWxvbmU9Inllcyl/PjxEb2N1bWVud
CB4bWxucz0iaHR0cDovLzR0aWMuY29tL2ZvdXJzaWduL3NpZ25zdG9yZS9kZWZpbml0aW9ucyI+PERlc2NyaXB0aW9uPkRvY3VtZ
W50byA8L0Rlc2NyaXB0aW9uPjxTZXJ2ZXJTaWduYXR1cmU+ZmFsc2U8L1NlcnZlclNpZ25hdHVyZT48Rm9ybWF0PkYCkFERVM8L
0Zvcm1hdD48SXNzdWVyPkZpcm1hIGF1dG9tYXRpY2E8L0lzc3Vlcj48U2lnbmF0dXJlVHlwZT48Q29kZT5vcGVuc2F0PC9Db2RlP
jwvU2lnbmF0dXJlVHlwZT48Q29udGVudFR5cGU+dGV4dC94bWw8L0NvbnRlbnRUeXBlPjxGaWxlTmFtZT5pbi14YWRlcy54bWw8L
0ZpbGVOYW1lPjxEYXRhPlBEOTRiV3dnZG1WeWMybHZiajBpTVM0d0lpQmxibU52WkdsdQpaejBpVlZSR0xuUZ2lQejRLUEZOcFoyN
WxaRVJ2WXlCbWIzSnRZWFE5SWtSSlIwbEVUME10V0UxTUlpQjJaWEp6YVc5dVBTSXhMak1pSUhodGJHNXpQU0pvZEhSd09pOHZkM
2QzTG5OckxtVmxMMFJwWjJsRWIyTXZkakV1TXk0d0l5SStDanhFWVhSaFJtbHNaU0I0Yld4dWN6MGlhSFIwY0RvdkwzZDNkeTV6Y
Xk1bFpTOUVhV2RwUkc5akwzWXhMak11TUNNaUlFTnZiblIKbGJuUlVlWEJsUFNKRlRVSkZSRVJGUkY5Q1FWTkZOalFpSUVacGJHV
nVZVzFsUFNKMGIxTnBaMjR4TWpRd05qQTBNamsyTkRVeE56VTRNRFUzTG5odGJDSWdTV1E5SWtRd0lpQk5hVzFsVkhsd1pUMGlkR
1Y0ZEM5NGJXd2lJRk5wZW1VOUlqTTNNVElpUGxCRU9UUmlWM2RuWkcxV2VXTXliSFppYWpCcFRWTTBkMGxwUW14aWJVNTJXa2RzZ
FZwNk1HbFdWbEpIVEZSbmFWCkI2TkU1RGFuaFFZMGRXZFZVd1JsVlFhbmhHWWtkV2RGcFhOVEJRYW5ocll6QTFhR0pYVlN0UlZUV
klVbFYzWjFSR1ZrcFZlVUpMVTFVeFJsUnJWbUZKUlRGQ1ZXeFNTbFJyVm1GUVF6bHJZekExYUdKWFZTdFFTRXBzWXpOV2MyUkhSb
XRpTUZwd1ltMUdjMUJxZDNaamJWWjZaRmQ0TUZsWFVuWlNiV3gxV1ZkM0sxQkhSbmRhVjNoellWZFNkazFzU214alJEVk9VVlpLV
gpWTlZOVVpYYW5kMldWaENiR0pIZUhCYVJ6aDVWVzFXZDFCcWVIUmFWMUp3WWpOT1Jsa3lPWFZpTWpGd1dUSTVlbEJxZDNaaVYxW
nJZVmM1ZWxKWFRuWmliVGwwWVZkT2RtTjZORGhoVnpGdVZGZEdjR0pxTlc5a1NGSjNUMms0ZG1KSE9XcFpWM2h2WWpOT01FOXFhM
2ROUkVGMllqTkNiR0p1VG1oa1F6a3pXbGRKZG1GWE1XaGFNbFo2VERKV2Vsa3pWbXRpTVRsNVdsaEMKZG1OdVVYVmFNbXh0VUVNN
WNHSlhaRTVaVjJ4MVVHcDRhMXBYVG5OVGJsWjVXVmRTYUZOdVZqWmFNa1pyWWpOTksxQkRPV3RhVjA1elUyNVdlVmxYVW1oVGJsW
TJXakpHYTJJelRTdFFSMUpzV1RKNFMyUllTbWhhUjBaQ1dUTlNNVmxYZUhCbGJVWnFZVmM1ZFZCdE9YVlFRemxyV2xkT2MxTnVWb
mxaVjFKb1VWZE9NR1JYUm5OaFdIQm9XVEpzZG1KcU5EaGtSMngzWWpGClNlVmxYTlhwalJ6bDVaRWRWSzFCRE9UQmhXRUoyVmtoS
2FHSnVUbmRpTTBvd1dsUTBPRnB0UmpSUWFtc3lUa1JWTVU1cVdUTk9lbmQyV20xR05GQnFlRzFpTTFKM1dUSTVkMkZYUmtWVWEye
EhZVmhPY0ZreVJTdFFRemx0WWpOU2Rsa3lPWGRoVjBaRlZHdHNSMkZZVG5CWk1rVXJVRWRzYTFCcVJUVk5SRUUxVGtSTk1WSjZkM
1poVjFFclVFaE9iR0pIVm1wa1IxWnJVVgpkT01HRlhPWFZRYmxKc1kyMHhWR0ZYWkhWYVYxRTRURE5PYkdKSFZtcGtSMVpyVVZkT
01HRlhPWFZRYW5oNllWZGtkVlZ0T1hOYVZEUTRURE5PY0ZveU5WTmlNbmhzVUdwNGFHTkhWbk5pUjJ4cllucEZLMUJET1doalIxW
npZa2RzYTJKNlJTdFFSelV4WWxWV05HTkdTbXhaVjNjclRVUjNkbUp1Vm5SU1dHaDNWVzFXYUdKRU5EaGlibFowVWxob2QxQnFRV
GhNTWpVeFkKbFZXTkdORU5EaGtNamw1WVRKYWMySXpZeXRpUjJ4cVlWaFNhRnBIT1hsYVdFMTBUVk0wTVV4WGVIQlpNbXd3V1ZkU
2RtTnRWbnBNVkVWMVRsTlJlRTlVZDNaa01qbDVZVEphYzJJel15dFFSMUoyV1ROV1YyRlhWak5RYW5kMldrYzVhbVJXV25CYVdHT
XJVRWRHYW1SSGJESmhXRkkxVUc1T2RtSkhiR3BoV0ZJeFdrUjNkbGxYVGpCaFdGcHdaRWhySzFCSFVuWlpNMVowCldsYzFNRkZZV
WpCWlYwNXZXbGRTVDFsWE1XeFFhbmQyV2tjNWFtUlhNV3hpYmxKQ1pFaFNhRmt5YUd4YVJUVm9ZbGRWSzFCSFRuTlpXRTU2VUcxT
2MxbFlUbnBKUjA1MllsTTFiV0l6Vm5sa1IyeHFURzA1ZDFwWE5YcFpXRkYxWXpOU2VXUllVbnBNYlZwMlkyMHhla3h1UW5saU1rN
XNZekk1ZWt4dGVIQlpNbXd3V1ZkU2RtTnRWbnBNYkU1MllrZHNhbUZZVWpGYVJWcAoyWTIwd09Fd3lUbk5aV0U1NlVHcDRkV0ZYV
2xOYVdFRXJUVlJyZDAxRWF6Qk5lbFpJVUVNNWRXRlhXbE5hV0VFclVFZHNhMVJIT1dwWlYzaHdXa2RHYTFCcVVYZFFRemx3V2tWN
GRsa3lSbk5oVjFKb1drUTBPR050Vm01aFdFNHdZMjA1VVdOdE9XMWFXRTV3WWpJMWFHSkVORGhNTTBwc1dqSnNlbVJJU25aVlNFc
DJXbTFXZW1GWE9YVlpWM2NyVUVka2VXRlhVbEZaV0UKb3dZVmRPTVdKSFJubFlNamxyWkVRMVdFa3dWV3BWYVU1VlVFTTVibU50Y
kd0VlIwWjVaRWRzYW1SWGVHaGpiRGwyV2toUksxQkhVbnBXUjFaeldsZFpLMUJET1d0ak1WSnNZa2RXYlZCcWVIQmFSVVl4WkVjN
WMyRllSakZoVjFKb1dUSnNkbUpxTkRoTU1teHJVVmhXTUdJeWVIQmpXRlp3V2tkR2FtRlhPWFZRYW5ocVdWaFNiRm95T1hsaFYwW
kVZa2RHZW1GWFduQlpNCmtacVlWYzVkVkJzU1RoTU1rNW9aRWRXYm1JelNuQlpWVTV6V1ZoT2NGcHRiR3BaVjA1d1lqSTBLMUJIV
W5aWk0xWmhZVmhCSzJWWFZucFFRemxyWWpKT01WZHRiSGRRYW5od1ltMWFkbU50TVd4VVYyeDZZVmM1ZFZKSGJIZGlSemwwV1ZoU
2NGa3lSU3RRUXpsd1ltMWFkbU50TVd4VVYyeDZZVmM1ZFZKSGJIZGlSemwwV1ZoU2NGa3lSU3RRU0VKM1drZFdlVnBZVFN0UQpRe
mwzWWpKU2JHTnRWbnBRYW5od1lsaENlVkpIT1dwa1ZEVXdZMjVXYkZCRE9YQmlXRUo1VWtjNWFtUlVORGhpYld4dFVHcEZOVTFFU
VRWT1JFMHhVbnAzZG1KdGJHMVFhbmhyV2xoT2FsWkhiSGRpTVU1MllrZHNhbUZZVWpGYVJVNTJZbGRLZGxCcWQzWmFSMVo2V1RGU
2NHTkhPVlJpTW5od1dUSnNNR1JYVWtSaU1qRnBZbm8wT0ZwSVRrWmxTRUpzV2tkc2JHSnVVbXgKVmJWWm9Za1EwZDFCRE9XdGpNR
lkwWTBkV2EyRlhWblZrUjFaVFdsZEdjMUJxZUhSYVYxSndZak5PVlZwWFRuVmhWMDUyWTNvME9Fd3lNV3hhUjJ4Mll6RlNiRmt5T
lhCWk1qbDZVR3A0YTJNd1ZqUmpSMVpyWVZkV2RXUkhWU3ROUkhkMldraE9SbVZJUW14YVIyeHNZbTVTYkZCcWVIbGFWMDUyWTIxU
kswMVllR3hpYmxKNVpWaDRlbUl5ZUhCWk1td3daRmRST0V3elNtCnhaTWpsNVdrUTBPRm96U25CYVJrcHNZek5DZG1KdVRtaFpiW
GhzWXpFNWRscElVU3RSVlRWSVVsVjNaMVJHVmtwVmVVNUxVMVV4UmxSclZtRkpNREZDVld4U1NsUnJWbUZKZWtVMVRVUkJOVTVFV
FRGU2VuZDJXak5LY0ZwR1NteGpNMEoyWW01T2FGbHRlR3hqTVRsMldraFJLMUJJVm5saVJURm9ZMGRGSzFCRE9URmpiWGhPV1ZoQ
2FGQnFlR3RqTUZKb1pWUTBPRXd5VQpucFNSMFkxVUdwNE1HRllRblpTVnpVd1lWZFNhRnBFTkRoTU0xSndZMGM1Um1KdVVuQmFSM
FpyVUdwNGJtTnRiR3RWYlZaNlkwYzVkV015Um1saVIxWjZVR3gwTjBsdE5YWmlWMHA1V2xaS2JHTkRTVFpKU0hOcFdrZFdlbGw1U
```

```
1RaSlEwcENWR3RrUmxSRFFrMVdWV3hVU1dsM1owbHVXbWhpU0Zac1NXcHZaMGxyUms5U01GWk5TVVY0VmxOV1RXbG1VM2RuU1cxR
2QxcFgKZUhOaFYxSjJUVlpLYkdORFNUWkpTSE5wV2tkV2VsbDVTVFpKUTBwTFUxVXhSbFJyVm1GSmFYZG5TVzVhYUdKSVZteEphb
TluU1d0d1NsU1lZWazlTVm05cFpsTjNaMGx0Um5kYVYzaHpZVmRTZGsxc1NteGpRMGsyU1VoemFWcEhWbnBaZVVrMlNVTktUbEZXU
2xWVFZUVkdWMmxKYzBsRFNqSlpWM2d4V2xOSk5rbERTazVSVmtwVlUxVTFSbGRwU2psTVEwRnBZbTFzYlZWCnRWbmRKYW05blpYb
EthMXBZVG1wSmFtOW5TV3BGTlUxRVFUVk9SRTB4VW5sSmMwbERTakpaVjNneFdsTkpOa2xEU1hoUFZFRjNUMVJSZWs1VlkybG1XR
EZrVUVNNWJtTnRiR3RWYlZaNlkwYzVkV015Um1saVIxWjZVR3A0ZVZsWWNIWmliRTUyV1RKc2FHSkVORGhNTTBwb1pXMDVkVlV5T
1dwaFYwWnpVR3A0Ym1OdGJHdFZSMFo1WkVkc2FtUlhlR2hqYWpWaVpYbEtibU51Vm5kaU1FNXpXVmhPY0ZwdGJHcFpWMDV3WWpJM
GFVOXBRamRKYlZKc1l6Sk5hVTlwUVdsV2VVbHpTVU5LTWxsWGVERmFVMGsyU1VOS1dFbHVNSE5KUTBwNlpGZEtibU51Vm5kaU1FN
XpXVmhPY0ZwdGJHcFpWMDV3WWpJMGFVOXBRamRKYlZKc1l6Sk5hVTlwUVdsU1UwbHpTVU5LTWxsWGVERmFVMGsyU1VOS1JrbHVNS
E5KUTBwcVdWaFNiRm95T1hsaFYwWkVZa2RHZW1GWFduQlpNa1pxWVZjNWRVbHFiMmRsZVVwcldsaE9ha2xxYjJkSmJFbHBURU5CY
VdSdFJuTmtWMVZwVDJsQmFWVnBTamxNUTBGcFpHMXNibHBYTldwaFYwWkVZa2RHZW1GWFduQlpNa1pxWVZjNWRVbHFiMmRsZVVwc
ldsaE9ha2xxYjJkSmJGRnBURU5CYVdSdFJuTmtWMVZwVDJsQmFWWkRTamxtVmpBNFRESmtlV0ZYVWxGWldFb3dZVmRPTVdKSFJub
FFhbmgxWkZjeFJWcFhUbmxhV0ZKMlVHcDNkbUp1Vm5SU1IxWnFZMjFXTUdKNk5EaGFTRTVhV2xkR2VWQnFkM1phU0U1YVdsZEdlV
kJxZUd0YVYwNXpVMjVXZVZsWFVtaFJNamwxWkVoS2FHUkhSbmxRYlRsMVVFTTVhMXBYVG5OVGJsWjVXVmRTYUZFeU9YVmtTRXBvW
kVkR2VWQnFlSGxhV0VKNVdsaE9iR0p1VW1oYVJ6Z3JVMFJuZVU1NlRUQk9hbWQ1VUVNNWVWcFlRbmxhV0Ulc1ltNVNhRnBIT0N0U
VNGSndZMGM1VkdJeWVIQlpNbXd3WkZkU1JHSXlNV2xpZWpWeFpGaEtjRnBIYkdwWlZIZDJaRWRzZDJJeFRuWmlSMnhxWVZoU01Wc
EZUblppVjBwMlVHcDRhMXBZVG1wamJXeDNXVEpzZG1Kc1NteFpNbXhwWWpGT2JHSkhWbXBaTW14MlltMUdhMko2TkRoTU1sSnNZe
kpPZVdGWVFtcGhWemwxVlcxV2FtRlhTblpWTWxaeldsZE9hbUZYT1hWWlYxSjJVR3A0TUdWWVFteFZTRXB3WW01U1JXSXlUakZpV
jFaMVpFUTFjV1JZU25CYVIyeHFXVlIzZG1SSWJIZGFWa0o1WVZjMU1GSkhPV3BrVnpGc1ltNVJLMUJITlhaaVYwcDVXbFpLYkdOR
U5VSlVhMlJHVkVOQ1RWWlZiRlJRUXpsMVlqSXhhV050VmxOYVdFRXJVRWRHZDFwWGVITmhWMUoyVFdvME9Fd3lSbmRhVjNoellWZ
FNkazFxTkRoak0xWnBXak5LTVdOSE9VUmlSMFo2WVZkYWNGa3lSbXBoVnpsMVVHdFZPRXd6VGpGWmJXUjVaRmhDZGxFeWVHaGpNb
Xh0WVZkT2FGa3liSFppYWpRNFl6SldlV1J0ZUd4a1JtUjVXVmhDZDFwWVNTdGlNMHB1VEcxR2QxbFhUbTlhVXpWNlpFaEtNV1JJV
FhWWlYwNHdZVmM1ZFV4clJtcGtSMngyWW14T2JHTnVXbk5hV0ZKWVkyMUdkMk5IVm5sUlJFWnJXbFJSTWxwdFZUaE1NMDVzWTI1Y
WMxcFlVbGhqYlVaM1kwZFdlVkJxZUdoWk0wcHNXa2RzTUZsWFRuQmlNalZRV1c1S2FHTjZORGhNTWtacVkyMVdhMkZZVW1oWk1te
DJZbXM1YVdOdFJucFFhbmd3V2xkNGJGcHRPWFZpZWpRMVRtcFJlRTFxVFRCT1ZGazRURE5TYkdKSFZtMWlNalYyVUdwNGJXRlhlR
3hqTUVZd1pFZEdhbUZIVm10UWFuZDJXbTFzYzFwWVRrSmtTRkpvV1RKb2JGcEVORGhhUjFaNldURkNlV016V25CaWJVNXdXVlExU
kZGV1RsVlNWWGhOVkRBME9Fd3lVbXhqTWs1U1kyMDVNbUZYT1dwaFYwVXJVRWRHPYkZsWVNtcGhSVkoyV1ROV2RGcFhOVEJRYW5kM
ll6SldhR050VG05U1J6bHFaRmN4YkdKdVVTdFFTRXBzWTBoS2JHTXlWblZrUjBaMVpFZFZLMUJET1hsYVdFSjVXbGhPYkdKdVVta
GlibEpzVUdwNGEyTXdNWFppYmxKdlVHcDNkbHBJVGs1aU1qVXdZVVEwT0dSSWJIZGFWVkoyV1ROV2RGcFhOVEJRYmtKcldtcDNkb
VJJYkhkYVZWSjJXVE5XZEZwWE5UQlFhbmhxWTBRMGVFMXFSWGROUkhkM1dUTkJLMUJJVG5CYU1qVnNXa1ZTZGxsNk5EaE1NMDV3V
2pJMWJGcEZVblpaZWpRNFdtMDVNR0l5VG5aalIyeG9Va1UxU2xWSE9XdGFXRWtyVUVNNWJXSXpVblpaTWpsM1lWZEdSVlJyYkZGa
U1sSnNZMm8wT0ZsWFVuRmtWelV3WWpOTmVGQnFkM1paVjFKeFpGYzFNR0l6VFhoUWFuaDZZako0TWxwWE5XcGhWMFpWV2xkT2RXR
lhUbWhRYW5kMll6STVjMlJ0Vm5WWk1teG9Wa2RXYW1KdGJHcFpWRFE0WkVkc2QySXdOWFprUjJ4dFlWZE9hRmt5YkhaaWFqVjFZa
k5TY0ZwdGJHcFpWSGQyWkVkc2QySXdOWFprUjJ4dFlWZE9hRmt5YkhaaWFqUTRXVmhDYkdKSGVIQmFSemg0VlcxV2QxQnJjRXBVV
lZaUFVsWnZPRXd5Um5kYVYzaHpZVmRTZGsxV1NteGpSRFE0V2toT1JXRllTbXhaTTFKd1lqSTBLMUJET1d0ak1GSndZMjFXYW1SS
GJIWmlhalE0V2xoT2FtTnRiREJrV0Vwb1kzbzBPRXd5Vm5wWk0wcHdaRWhXZVZsWVRTdFFSMXBzV1RKb2FGVnRWbXBpTTBwclVHc
EJla2xHVG14alEwRjVUVVJGZDBsRVJUQlBha1Y1VDJwSmVrbEZaRTVXUkhkM1dtMVdhbUZIUmxOYVYwNTJZMjFSSzFCSFVucFVSe
mxxV1ZkNGNHUklheXRRUXpscll6QjRkbGt5Um5OaFdGSTFVR3A0YlZwWFRtOVpWVkpzV1ROS2JHUkhPQ3RRUXpsdFdsZE9iMWxWV
W14Wk0wcHNaRWM0SzFCSVVuQmpSemxUWTBkU2RsQnRjREZqYld4cllWZE9hRkJET1RCaFdFSjJWVzVDYTJKNk5EaGpNamx6WkcxV
2RWa3liR2hTVjA1MlltMDVkR0ZYVG1oUWFuZDJZekk1YzJSdFZuVlpNbXhvVWxkT2RtSnRPWFJoVjA1b1VHcDRkbGx0Y0d4a1J6b
FVZakpPY0ZsWGR5dFRWelZ0WWpOS2RGbFlVbkJaTWtVNFRESTVhV0Z0VmpCaU1VNTJXVEpzYUdKRU5EaGliVGwwV1c1S2JGQnNRb
mxrVjFacFdWTkJlbEJET1hWaU1qRnBZMjFWSzFCSGJHdFZTRXAyWkcxc2RWa3liR2hRYWtWNVVFTTVjRnBHUW5saU0xcHdZbTFPY
0ZsVU5EaGFSMVo2V1RCNGRsa3lSbk5oVjFKb1drUTFSRkZXVGxWU1ZYaE5WREEwWjFKRlZXZFVSVVZuVlVWNFFsUnJSWFpSTUVaV
VZrVldUVlJGT0dkU1JWVm5WRVZGWjFWRmVFSlVhMFU0VERKU2JHTXlUazFpTWs1b1lrZHNhMWxYVVN0UVIyUjVaRmhDZGxFeWVHa
GpNbXh0WVZkT2FGa3liSFppYWpWVVFTTVibU51Vm5kaU1FNXpXVmhPY0ZwdGJHcFpWMDV3WWpJMEsxQkhVbnBTUjFacVkyMVdNR
0o2TkRoTU1sSjZVa2RXYW1OdFZqQmllalE0V2xjeGFHRlhkeXRqTWprMVdWYzFibHBYZUVGYU1qRm9ZVmQzZFZreU9YUlFRemxzW
WxkR2NHSkVORGhhUjJ4NVdsZE9hbUZYT1hWUWJFcHNXVmQzWjJKcU9HZE5ha2s0VERKU2NHTnRWbXBaTW14MlltbzBPR1J0Ykc1Y
VZ6VnFZVmRHUkdKSFJucGhWMXB3V1RKR2FtRlhPWFZRYkZNFRETmFjRm95Vm5WWk1teG9VVEo0YUdNeWJHMWhWMDVvV1RKc2RtS
nFORGhoVjFKd1lqSXhhRlJ0T1RCaFYxcHdXVEpHYW1GWE9YVlFiVlo2VUVNNWNGcEhiSFppVjBaUFlqTlNjRnB0YkdwWlYwNXdZa
kkwSzFCRE9VWmlSMVowV2xjMU1GQnFkM1pVTTBKc1lteE9RbFpFTkU1RFp6MDlQQzlFWVhSaFJtbHNaVDRLUEVSaGRHRkdhV3hsS
UhodGJHNXpQU0pvZEhSd09pOHZkM2QzTG5OckxtVmxMMFJwWjJsRWIyTXZkakV1TXk0d015SWdRMjl1ZEdWdWRGUjVjR1U5SWtSR
lZFRlVRMGhGUkNJZ1JHbG5aWE4wVkhsd1pUMGljMmhoTVNJZ1JHbG5aWE4wVm1Gc2RXVTlJa1ZqV0U1aFNUUndUMFZ6UjJ0dFkwM
VNka3hyWXpOdGNYcEVPRDBpSUVacGJHVnVZVzFsUFNKUFExUnRjRFF4TURRd016azRNVGN6TURVeU1UQTROVGt1YjJSMElpQkpaR
DBpUkRFaUlFMXBiV1ZVZVhCbFBTSmhjSEJzYVdOaGRHbHZiaTkyYm1RdWIyRnphWE11YjNCbGJtUnZZM1Z0Wlc1MExuUmxlSFFpS
UZOcGVtVTlJalV4TWpJeElqNDhMMFJoZEdGR2FXeGxQZ29LUEM5VGFXZHVaV1JFYjJNKzwvRGF0YT48U2lnbmVyPjxTaWduZXJSb
2xlPjxDb2RlPkZpcm1hIGF1dG9tYXRpY2E8L0NvZGU+PC9TaWduZXJSb2xlPjxTaWduZXI+RmlybWEgYXV0b21hdGljYTwvU2lnb
mVyPjxPcmRlcj4xMDwvT3JkZXI+PC9TaWduZXI+PC9Eb2N1bWVudD4K</dss:Base64XML>
                </dss:Document>
            </dss:InputDocuments>
        </dss:SignRequest>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


Respuesta:

- Respuesta Encriptada con Clave Simétrica: Sí
- Respuesta Firmada: Sí (Token de Seguridad – KeyIdentifier)

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14134730260181902275155">
                <wsu:Created>2014-10-16T15:23:46.019Z</wsu:Created>
                <wsu:Expires>2014-10-16T15:28:46.019Z</wsu:Expires>
            </wsu:Timestamp>
            <xenc:ReferenceList xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:DataReference URI="#XWSSGID-1413473026057135890 9087"/>
            </xenc:ReferenceList>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1413473026018-
1394505154">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413473026021-130771239">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="SOAP-ENV dss ds"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>942TtpLczFiYbh5Cq30F7zJSHgU=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-14134730260181902275155">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsu wsse SOAP-ENV"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>5ILhv+n6bgTJDkV6IDKMQwd6TjQ=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>TCIJWt+T5hE5nxYTBKoWBQR/y+SivXwnkl0rnnrxv1/duiPfIAwOYp/2TZnEQPj9zzvNJAmrZI07Q+fVd
xC6wTsuZYJyYnoWGpAn5chQlDwbjlL56jiVKfRIcWBbvqvE2f06ofxh16lSHxeuYm7XuteDoSgCyu1LSJufZ2eEBC8u9hzpMjv3j
s21XEJm2JfEzbRWl74KKZF4Nxp0OCAGRPEPJ9nacqlbsG7sIelfv3dJ1xJVVP/8xiF6RGbnxvUn3bkam/MCvXtNL+bz2enJdnXmE
IjgFCqhCNRD/Pjx6O4cxcMRP/KbdRdW+iQLGfW+ntNKqXasIhBNxI5al++K7Q==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413473026020-
1888065249">
                        <wsse:KeyIdentifier 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#X509SubjectKeyIdentifier">Ahg6E1lYWBp+eACCz21Dvh7bJ5g=</wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413473026021-130771239">
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="XWSSGID-
14134730260571358909087" Type="http://www.w3.org/2001/04/xmlenc#Content">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:KeyName>symmetric_key_test</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>

<xenc:CipherValue>WgoZDGMOK/iyKWy59/X2Ur3f7jUMPwQxkt9lI3+0x6sDMb8BSz+szRpbpUB84wdQ7ZrXw/w39/tW
3Rz9p2wmhnxFfCm1l5KUxx+0XHG1UaqU0M0Ih8bocr8SXEGGBQxSbqPXAP9a5EjPukMbksPYxxG2
2g8tNXlvL72TXSmk4ZFNzTwiXOc4MoAmGo4vKSGhum6zqv78kLbvpJyWhvUJpWHSgRF4ANoc/qd7
dezEIu15ThLezJ18St47FUunpksKtTrjA9z2BusyRGPKmtycQCNwLcIg5NeMw9ufTrf6SRaWhUPG
```

```
kUZJumUjoqt+N6Wq/0ZG3V63Pa44N2YjiHjwGHwLxrKcIwrctgq52usnDAd6W/0NIRU15fEJH2kX
pKW3WeGz2LAJsdur3QBjn7dwXfKX3vVqVjzeyQgdfN7jF/x2ABdYvHnjtzbpHZq3khAAKZu70088
ctUtfwItOJh6Ig4oGhWzPaVlLqQDcPgsFEnEh0fxOAWOTOa0G1UphIfNvP+Dn2cILoKGyMSLeERz
fL50/vVl0FB1NOp8cWXS1Qjs9DUDVtH+siGtFeqlXCjSe8iKCQuvGMxQTnT2/2Bf/mKABPv9dCy/
VHY+Zl9bYGBy9l3GeJ00OpIueBNzVli1PhFL22D9+R7IzundhCJV9cj2Ffax0XrPyh1qF/tc50MM
7ksUK0HtpTtf9lsExpV+IrgQ9NN9WI2qyz3JKf0hbK/P7xQuY72zIV35vUyY1EVPnpjFyRVNOhq0
5XDMcqfUjKcVEIS6V2BnfGJQiLrFh4bhBxxK+7Azez1gvbf7hiTC04cbyrj8aScK4rhg7LF/Bhe6
1wEvi2P20wccpp08t51ykjodK+/1v4v1UTpj3kRwGzDMRC6O1Q5ihpKbQX9K4bFDhoapp0YDcVZQ
xQlkOx0YIj6+zLkuGVEoKlRTm2JsyHX/VXtUl7LnyT1Wn3bAordM4oNW4dJCZe2mj6yNFwf8g8y5
Z0r21zN7Vgz7hfDKUarZDn1aeYRgnxOyBV4X6HWjaFc675hU8U7vUXtZsJdbU95Jbwk1zM8CTfHQ
48poovGjwAq3nihk2EDCbsnFTf4oN/vAQI6ynRsXZ5ur/OcfBF4LaUfuFoLsPTG2rSkBYR3OgLvq
Cs5yXD2P8VLfbtgibWcpwGjFJOlGwSYhKaKbgv/9DLL7cHf5kUYwopWYKX21mfhUfS5Xg8gkRHC3
701p5hYkJIjVl1QzKqHaPo0aqx/CwdvAR64XEi+F7JFFVpeBMZbeDTxg/2dId9YsVFrjjOS+RTzG
riWtrA0XPRyP/foM7y8FvQccbQKHKP0LOOAPYfQhmk87bO5xEAsLlkhDoTjHaIF9C+DX+w6bh+uG
2udVv8JAlzpSMm6Chl857vIcD+bLna+j0vlDv+zy7RXQuST18HnhAIGyAAnbyiRNIg92ypX/quEg
K7+YFfe55goMhuPx1SGjfm1atmZEKFg0b7SCGfMUgJp3XoqY97UuIVN1Xlz9aBhEmV8lyDM+uvdu
GWbngPI+p9kpTWeLvJWGPNGMjkBvfAt0ssCbJxH/N5sDKD0AcvdZWQmN8WjSZn9tR55dymKMMoWD
jJS2BcTf+l7ro6N/3Sz1wpDHKXpocMU+S2R1eTz8ZQ4aPpVJ5I1xzMrEEUO7ydfVw41xY4k229iK
OhW0BGfsMidr49KMACgM/XITCZ+Bo25OtpZiaNMa5CiySgyDbrDefVdD6DqgbAWBxHmL/XX/i+Gb
UWdQqFmaYJ6A5UYWoi0w2kP1X1PlJ21Tuqri3l5+0gLPAQj/LChc3pfzwNJ3lW0PLcuSgOayukdk
aKuxFafw10fnONV9PcPEBv98KV9i39JASLSb4fh2wYrqCNem+WnZhSMFTbsgswId4xa5T23M3fWv
IDbohW4rGydOnygdtce0Hk7wS7eabR+P3IEq67i6iORj/g9HTy8YnWr4J49Y/lhbEmBSVgaHOpfI
ihkhS0SWk53AJWbGuLa/9LlVyw8QDYMO9C49/Z5gIi0BxI3SW8OaY02vdepuCTGFqgyZkTbw1e9n
qGfc733sIXtD4JrRGZrOCBNU0SnsLcuCw193EzgYNdyv7By75btl6x6qeZ3ctYau3RDRhgp9fv5K
e6h0dxbT7ictQAC+mCT8j593aofctTs6LcoLhcG1OJQCPMrhjt2SvH7Cx25dgKU+TmWHLy57ufF0
q8Y/O7dDG8dtrwiqT/7eutSw5BuYoTsoAmJIJfIXkWv8v/lufvZIw7H2hh11Xxd0hYDCU/n0GDx5
1i0Wr3YL30uAlcJ/fWhfb+s26528KglGU99j6B+I1DNc6O0EjD+EEGBDJ76xwX61GgZDnNw/wQSS
RaGhIPjOFSYE4WT2zF7NX3oWnSqBvjrKCUe8YzwqQ+xhEJejFWG+Nj/4k9xqwSSN2UZFOU/XJ08E
d4h6LxwcL3EiUkThQd/HrW8IZ/k9/kh1CG6JIy1XTagERN6tSTHrWy3Zvl2EIh6rGTdgtPaGJg+z
RMuVrf04lU9EgOXsPZblpe8KuTFEh3O7L/PWXBGvIB7SBnHuxPFqp3krpqEILnWWSVhIxbJhGQ1J
pP9FaHLfy55eCRJDxhtovnul5aQZov5zN4MxxMtktn4i3iW941aK39lLTd7gz40PPhhGiNBhltMK
9NkQR6b97KxQMcK9AI6PgRlibbJfRShFMYTv4x+VboZLatO3ngrFpFoINKejT4yzAO7j9IaFO/XR
8ZWtBXK0Dg8+dYP5LHfaGHA+5oyHqxj39+H9N6iNLrlFyukx3qiCK0czh+KXJR5sXaQRuY8TCLYH
K7pcbhSfQWjNtxCanrhXvzHn/lcuMgd0kye9sRens251P+43r64jlvwOGcPFW03KYPqH0o7nAwda
B6tCSTFJLAhMxm+HlkC2Aon10ZaN053dd8yfDyksmrDjj1ii80JxPANwGJrVjUBGoB0GlxQ0hI7N
Qvcy6uTkoGBY/VMttclU4BBr+AJGCH0+5Y17BoIlFJJsAh1poBafC0yZ3491v79ckynTTD5uwuHX
TJcm8QPalV66eQOdzdDt9DU/NOSwxUD4ZyKJj7/Iahm4309fuaTLYlnPj7Lq/g0bP1ddEum4Yden
oRTJlhWmM9q0IkIP6VMX5UV5AWC7CkuVo5v9LlRw6dldBYhcacLLQzDjFDBC5CTTCHBtnus6ukPU
Cm5N7volw0qeUzMec11KElg+bU3na5WZHqjHbmqDW8u4+04CHaEsP/kscBjSElXS0BldpDQ8brsM
Up5KVeedBfp8A6b/C7mdNev+bcwL68HVlqaYJKLDx/zJGMyRBrnWQo99njqHOmc7579fK9SreJQ3
vyzvg4laqpv9ryHgy2M8tMdGj9+Cs+3GbXR4mRuoVgn5G0Epp7kPbhqMXKEKuldLE7mDJkvDka8S
pEDTCoxmME7yGupZ8vYKmTAk0SduWYb5rdbOmjvx67+ctMBqEyaPAG9e/XzlOxH6AtsOhUzJLa1w
yZ8f/tPZ6U8Gm7vnvWtyFi18nThEyt2oZSZy1u+2Z06ll5OxQzzuMrx2tv5NVwgwFv2/Y/7SuLka
FxjM8WVX/e74Dh43pRZxFjwfjg3i5OTf2ITXROnPQJdsp7wb7vyxAxkXuyyBKE6OhAvqQFrnO7Jy
q3yyagmaXJbjyDpJ0ljPBx7e+7JdDzMBEVKW6QraOu+eVjiEEr3OX5uCBNfLDNIYFRonwQYNOoSj
tAHqt1ijFShXzyl61gRiWvNINp5VdK2NaE1DehbJY8YHOLQK5srUEjai8xBTwzyB64IszEr+ISix
t6X2ZkQbIZs3/+gZCfMiC5cxsb2aKDnetX3wOihKutPFiLSODw1vRCIxawbgARnsS1o8LlGLUKWn
8Iuae99D0EsrzPGBpTBAJCbH5puz8BwUpoRV3dx4F8l1TP6CRT2Ba9CR+vVKlZF54UK7RSnGsf0Y
que7slsFYdLqJvDwWJIrDnAQW6xMOdY87Oc6f+ivS8chuvPt9YjmF3ZQxiZ/v51erRhaYDax69/c
Gsx1H5VP7bvI8lkX4YWttdLrV0GFwcaNgG4nQU3bDEjzeNW9KNBVFPomMpOMrseOtwCVNBkatCjt
b55s299vEJ82HOdmndH427rl1CJDDZXvvJX0vN1Thc+onuxKowkV6TXGGCQ+hd6O2QzOWBRUHxZz
nRH00odvt5yr08Qh3cLpQY8I66W84NsaLN6/uQo3NjGXelrqtZB4AR61pd/jb1OTiH7wOWdyPnDT
3lM8H3AbN5tW3IEcr+AaRRMdXY4v8ebemjSH2FFK0fdncsxhgmrwJSHkz00mV0rctPDSz7taT9mp
1aknxrwBAYcVaFtpJFI2ghiyAMXh+OaIxZ88LKBMkIQHfV+7/GXq/bWSjikpexezlfeJljRsYPNw
T0GVRoTPjqoUBH22yO6LduHCkb8Obvmlu2VGUf3kBtWcQGlMVH319K9YMfs1AefomDKocmTrLls8
MrOQyZLR/iyF+vpxVBU9tCYLdyfffKKDMf92X20ZqPVqoGUKwwbupjNDf7BLQVdCy5GjQoVViU0a
3DVjee/GglxLiHFyhLeiLnRc4CXpqV3GeQvI/awfE8k2Bzq8G80mbEQWJ+FvlDdsbdUQ/vyZvIvW
mLtmWwP/zBqEmWVsWwdRbFaLtUdgufdHOlFeJpYkRLaL4XVYHxloUSp4mHLnUV4WlsjT8vjikiDe
Tp6kBHyzIBsocxjxv0tn3ZgLBF/rjqadjSK+EQBK0yMGSNV8qSyreD1xRNu2d0LjNd1DBilBtlpr
1iSm9D7esrpIB6ZkNFgr8qF3dYZw610cgDfzV11TxvX3VeBJ4JWsPjzoRnpSRWYrbcYvlnLsuaJ2
J9q7aFIg+Y1K5J/bhfR53a72eduhetIsvC50rhsRnP8EG+iqlmKZtN4zqF0A1br9dq3Kbrd4uTIG
657FuUquLzKTdeA4+cmaFRCxpFgCt1U7dEVlGXym7toJp20gneej1k/5yS/5xVQJJrfR3rSsJmFd
443idPIHEcaRz2F1weYkGjzq3BeGl1Ttzf5FKPf6iXGFFlD4aiUf2lnfkMlIQVxqy0ialvlWdEaX
YAri8zoRSlEpTht2aJ92+6bh7uhrlvPOjVQ/w6+F9ifBCPSXMf/1yx0lkvYKqTDb8kR/LJsYzNKo
HRymCMgqtXtYHf52+gormZxWgQ/NPBwlZa2IEK8u5PUG0oxckKEaAtIZ5sSpd/qLTPtzZJ7tkkbp
oIemv3C5dNY+L+MtXWQ44aoDocUPgbvgBFgi+KEIJo05jkpQqNJj0d+/H+NI0UVNOB2l3TbodX5D
HOPO0pRQkVzSNffAJBYNvl9ma3k5SqLT2O7Nl0sco8GUv/PzZ6/vH4rSd7tOSydishk+Z6XSFjqX
OX7juMkz0R0RBuAewJyhoHMbdEapXmzRmha8BRy5am+fGJgN+KqEAdPmp5i46aWTTW3pMlIClX5A
+SisuL8dm+rmQEbMakIKFc6NhQm/CLeT+AaVypKslm+ePR8C2el6BQIZyahgjxwpbPawfDuiIUVO
mT9gE4nGHYht3W9QHVypDzVniewUHViMyloj+g0Lg0zBy82KIeJ074A9aL8MQtFIEjj5ItYzVz5y
2/nxCqKWG00fjWiX/LK4VUzLQGZ8Sbpv1FOi6S1scgFkRDIHYaIoBCqEKpxY73mLb4M0MfwPc62z
TqqVvk3abGlWs+ZeDtfBvGe4XIW76jy+D8QaUGeTvnTumhZ+lGye+sRpu7/B4XGbNw0j/Gr/xXzM
aNvVKMD0zVQ8zP5P3AyDdcQSvAWDx2GVoYB8o7SEuoM04ZRydZCkthbFqtdtHfrwwx7DgOieLLTo
LTE7EIwkbRfQFyFrR0PsK93i8NJl72nMqdslwpNse9CTItSqLG6ZULuAkCVOboCqAmOcNNTfLVSe
```

```
s15Ia6nkctS2beSCeZIboHxIp34QmUAnaoS4d3zpphAqqj4Zj3fUPbCk</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Ejemplo 3. Solicitud de Generación de Sello de Tiempo ASN.1

Petición:

- Securización de la Cabecera SOAP: Certificado (Método de Inclusión del Certificado – Binary Security Token)
- InputDocument: Document/Base64Data
- Petición Encriptada con Clave Simétrica: Sí

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14134733422581877622780">
                <wsu:Created>2014-10-16T15:29:02.197Z</wsu:Created>
                <wsu:Expires>2014-10-16T15:34:02.197Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" 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="XWSSGID-1413473342106-
2119084864">MIIFRTCCBC2gAwIBAgIIFl4IlQK/pRkwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3ViQ0ExIDAe
BgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEwMjMxMzAw
MjJaFw0xNTEwMjYxNTA0MThaMHMxEzARBgNVBAMMClNvYXBTaWduZXIxEDAOBgNVBAsMB1RlbHZlbnQxIDAeBgNVBAsMF1RlbHZl
bnQgR2xvYmFsIFNlcnZpY2VzMRswGQYDVQQKDBJTY2huZWlkZXIgRWxlY3RyaWMxCzAJBgNVBAYTAkVTMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAkch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0ptsmAVJ9OJ7D2gM
vPgQNJEOshdFyG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MPxKb4NZm5fFd1LGApXNEPZ0OC
OxpGkIMwn/YkHSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0aWqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u6+GuHKijZ5LUe
VrSpjcRq9Nhp+gVvqnaxVlmeRgG7C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQIDAQABo4IB9zCCAfMwga0GA1UdLgSBpTCB
ojCBn6CBnKCBmYaBlmh0dHA6Ly8xNzIuMjEuMjQzLjEwMjo4MDgwL2VqYmNhL3B1YmxpY3dlYi93ZWJkaXN0L2NlcnRkaXN0P2Nt
ZD1kZWx0YWNybCZpc3N1ZXI9Q04lM2RBZmlybWFTdWJDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVs
dmVudCUyY0MlM2RFUzAMBgNVHRMBAf8EAjAAMDsGA1UdJQQ0MDIGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwQGCCsGAQUF
BwMIBggrBgEFBQcDCTAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0
cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04l
M2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8E
BAMCBPAwHQYDVR0OBBYEFAIYOhNZWFgafngAgs9tQ74e2yeYMA0GCSqGSIb3DQEBBQUAA4IBAQBmeMs+UdPMWY5Icyn97ZR//LOf
k6ElAfgxRs1y6DH1oJdiWUnVkHmSgGNY+Y4j4y74TMiH25naizyyKQzmGoHw7KOgTxxqUEwlEHZPuf5GIJxc+/a0askEItRRgf9p
ozjL2+RS4YMU33xJlyBZNQ4nrvlKyNx50favpiKD2kOuHFqu3CypQzEvWw8uW5RY6Vvmujc3pztwjZtMeatWTbxMS8+c4wfT7N5b
gRFCH3t/Wu/yhKQlnfkXGLdpOeIt2pxIKH15UR7ODMmlNcIIRJQPoCPm5PWPmo24BkTb5U+nr1y4I5yY/gkIOammYYORPb10i1vx
9bRX1llTnWg4/YNX</wsse:BinarySecurityToken>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-
14134733421051891476621">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-14134733422577863852 49">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>BR1aHEK4o+Ht7/zhiKitc/Ug8F4=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-14134733422581877622780">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>faEOdASlc/ZYdlbLAdtt1VdGtuA=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>F46VPJU1ZJHG/X62Uz1GG/nlQqVjSU41191jw2ok4BGhrJNjwCoB8CsHFWAbKHSmeka09twfaHJk
LprBx1AwR75x5ncQerjbE/F7dcVWML6tEjIVIUHL8ZA3t24ZBtNTnO/+ch2ghMfJFYoDNUGBxvOt
B4Sygrh1OWDeVscbc078+zB5vNVB6hRsRqg4RK+pzAeeF7Oul0J1WY0O16Own3wBh65wtmCcjoLd
WBGVO4k9pigAK0Kq4yyaEcIu+o+miO+KvbyKMBSgFQM/DF5nrban0+VOIQRqUwiy1keVqndWeal9
PAdZTNgsIAlDfwuryyU7DpfTsTfggwl5h4aLhA==</ds:SignatureValue>
                <ds:KeyInfo>
```

```
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413473342249-
454962975">
                        <wsse:Reference URI="#XWSSGID-1413473342106-2119084864"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
            <xenc:ReferenceList xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:DataReference URI="#XWSSGID-14134733421928758408 91"/>
            </xenc:ReferenceList>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-14134733422257786385249">
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="XWSSGID-
14134733421928758408 91" Type="http://www.w3.org/2001/04/xmlenc#Content">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:KeyName>symmetric_key_test</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>

<xenc:CipherValue>k1RbCWwkoO4yQ5/RalKpB+r8Mpqm9AKe1xl57+MwDUwFUHJ2lzmyp4rqb6anWPE4AvxCE5sd+GRb
SKfEVlNVJxpx9OqKJ8W45FqtQAcnGDBxIiNJc/kPVhFVQJrmePzPoGXM6+nUdagRDarjjsb4sJsJ
Rj3c0yy/D7IpiZ2siXa2Ebq7w8JNbYMMAOHTpEKNZVSz/h/4vJ3ljOK1enWZjOihBCRfU58JBuQI
xQcEBkP6cFqTYmMnGSKHCL01tZvQt2bwjGAQhIDzaOTX8NQtUanH9vJCAeXjN5JflsV+nY+JY/Ra
SADOjfJPecbhCX13PJEC5JvSpM7AjjIFCDqT7/JwUmITnatTInIqcaDai2Vz2OnWcKvW4Yr2shsb
4aaOdohw50f7/DMk+hFCnhmo+UCcCR2C+wmX/4QZGI9Q/B++W3S4xiOZZ1G/NtRnCv8pwzqrl250
VG3xl1t+VqmE65IcUC5ovVHLej/aigUbH65S/7P1MX0d3Auk5dM4dTYPvWlKUrANZCU+PKcZOPsH
1z/xK2cd1gRs8lXg9yIbr4+GWfet/fvKVjvCSSUnkhTpRtFz1HopweSm7rqB7kUsUOrPZjgdOc8Y
1THLIcqd5JoYZOFNH+Wj7ub/jS2TGJOFPVkLU+XwROT4ytfxQsPwzDuQSxKy8g/pgOTZ9qlncTue
RPIhuS+Agvrl2q99/Ku6RPOdap9bX5a79xiG9cNY7pB+zy3BBihXhTNBqWKd4AAMCHTqk/sagP9D
xO41NOtJ5NwDzeH2AkpRtzgt1Bo5yuDGoMCKG+jZpQZQErnsWpI2/iUYQYPL4giGlTa8a4n4vr2F
veCH/6dY/ZFoeqdD7FT6MK3KUqG7WscAsRVAzb16N7TbHqC5VKq23C+Gx22EhV87KFN7Rvs5sRlN
OkQDlRvBv1w1rzrg9ygOa0fqlvuQG32MZbL9UnPo3sW7pc9rSBxwkqasPOhezafsvzwilLu8PHlP
UEo2CM8Ww6rqRn8y67ywDSNkkA7C1ng+S6dESEVFgrVYI4WIaG0oZfS+s+6I+dxnk+OI/UhF5gPn
k4cflK6evDFH4wiwlIYz+I7f5tbnpa0oifVO8b0oB8roeFRcC/ikPBbVriIRwC1zVwloD0pkvRpc
4wEyCqnWhWJ76mQR9QhBmY54YDZn0tECIquYnGueyD/DERxhnd5rmnV9s5oNCFA9qFsZR8s93AwW
Rv32HQEIJ82LKPHPrWqH4rmURcwOUm2uAIq9yS3QWevfLf2ZgChXNL3XMXVNKPgc4vUbsRUS0Vwj
VKj/c24oUMgRfTqC7eaQHkhHZkGH02l2JVCCXDEw+cnuyt1JHfATi+0vPvSvRn4TIOVKcoibbWQD
e9o1tjXTswg59xeu882eiPXKCXcRUbpN2q2WWDQDafde6ljAAbAFVlV9TLquoovko/qppWPM8Gva
4Tk4Oxo7KBL86ccYscySbJrE7L3aCJwsVezkvGrsr1tQYIdG0YDbL62Rrui8THj1ycN/pNBEK8iV
rvKsvMdF6+jVTehPF+aosYAbi/d68bEBCbaMngR59ahTn1MKtJ5vDDz+gw9IyIndnUtkEUA2faOG
vHwxv75dftJegGpUdsjsiVFEMJgsgcyBdBl2DTak0fBOA0kXHrJy0oU4/lwCCoh50SG48P9qlosD
l/wtcQXQyaVTpdu4j4xyfTR1pOvngoewELPfYC/vD1on9lH1FQa5QwFClj051MPszOB4Ym42zGDo
NnZBRFKA1AF4h2x8q0CikzNcgEq3Y+fDFGiCbh87WQcOBoD5g6G1Oi8HktngYZr8iYhlKj30zbq+
ItROwALWDf7WJ5getiKRB7dLkSX40yPCLCm6aQvfMec5GAhDxZAyi1jZCJW75XH6LpyZz5/UQJgs
eRSAg6a/khdWJSP443YrE/1E0K9bNDVyDT+sHTs/JwuhNsCXvK1JcjGM9eGdzmSS8ucFsBXcqPYC
TFatjPZtslq//ctFrQf9//HeLL7uv3/Irp9DWKOEdd46+3H7vFQZqXFgJLbwwAjfoX4tevb4FVLz
WQ1D9uheNKosaE4CCfKV5t0yYx3CNY0h1bA0dWPk8VjsQBsbUOIggorLOrsSg77cm5jXE4waw8JJ
v2oyQ+2X5yZnHw3HSwdkLvhh+/NoD5XSHcyF6ZwQF6PoRPY5vgYu0nasgwW3ID1GWVo4NmeZMFTa
6t37FAuXJWQAySxL3dXFmYOqkrYkapIApmtKqsVsqHwMY5+ngDiqVW2FLjTy3jGJHVYgihtVpPS2
V7c3KaiWSuLv1g/u8lAc3lVYja7PFQdIupREIZYASvEJ5NujdeBSjLzQpddybeiSnNxnPVecXvrs
oZ2fQX/c3fYR9mS1RaneT0EFCEn1JZuNCFbyydFPtyCizqJ9B5GPBExNlepXF3Y6pzyVbJmdMhik
qic0koYKrq75+qszVQ7SRpFpVaFmu9YcMgC+lElu1R6nl5PaMcCvv4ISqblxDENZ9GzXQAkynFkr
wXc5SB2uLROXTG12IjNZvjWl8fuUr+LLNW7qea+DXdC4935uFGsfeErA9Oo/aHvmSwfSjX/JW4MK
gnIytVozrCSZC8Qrq4S74ghLxxg6KeJfoHQaVt3MyaDkYX8kK+292DxUHEpbdNEmZ13cwUOJDKY8
dnMTN4aLAUmb3hcrX2CwBNwyDic9ueHzf4CfBAdFzoW5jbC+3hyejLL0f3Oj/ugFdviCX8LAxN25
nhLUQedsHqYZt+V3SjhioX+9DHzNYx88+My9J0tw8DBPYeOH+7fxTYyslDTUvHc7tIibnqGhc3Os
8WHJ8zGJ/Bd4w411AWVnGxMeYYydSfipNE7gMw684JXad9C9iqLNWg0RTHKBN4Ssw0evFBUrOo8+
klCXu+8NYSJ/SN2XvZ9E8zLWP+rVpZgu7KA17iVmlge/rFcltJTcBIk5V63llxnnWwLY5s70dqgf
f4ljEihBcknp5DLmnhGREfRtFvHJhpv/P5Veo+wG0t/cLS0D0m/fcVTodT1M3+CrE6Hf3aXvtgPj
mQaz+ZaanWEOsSKSjIZvK69f7P+QzNOLpE+rjJW7mmCNI7Ab5yxdLXKQWnQRvShXWGSOC1HKtX7g
CGzisM6Ka0aCoNZg0JVz0rAXagu+/1PtraeIpFcX4toVzwhPnvVa7eQ0VHJb8XEe2mCI7ECIV6yL
5yz3NYwgB6Vt37tnqLSXAbB+slO4FTCpCXB2dYyaTCWr5MKz1NJv0cSeT7nPF1LKDhr0EKemkl97
Wi1W19B4nVLklbgehlt1pZ/FbcK2XXtY7R0+MYSibQUq+gJsIjWVtgQT9xWUzVILNJvWpy2jXb6z
ZYHrr5o7+mFIHqRW/kB3FsNfxzMgndj6dvv5A75Kgm9EqxH+87jbhjkCrSKSjpeXIvDiGG/3ek8h
owTeQQeihsDy8ewqwmB3Lzof8jU1Z+SVc4xxJ3FdiQBZflsOoIrn4Zb0d5tg2/joeymo4IeS8vgZ
GR+fCPb4xQN0ld3qtYK0MHXOXt6KqDMowIYvaJjZ1Jpj/TwgX4lgMR7TJAM1L5zFH/p1frgBjKHt
FNekAcHdIAMvXlsu2rStMz0zMCtiCffyIdI7TJ1vw2uuWGPGc/m0iDN2q8jmePIvWWIOMYOKmGay
BTI57/UH8LhNNIV3Ew+GupVOTTm/dlCd9VhNyzR/KFuJHPtTbie/BvyTIxJPYT9FUdymamyi4PF/
jOiPrmd/VWPoD/1Im5VC3zq2xRp5p9ve6W/ZgdEosg0nMgIEN0PeXFQbnxyDYAQNpcHF8o1RVMSH
hB+Q1tm4qsSW5wke/i64yDjjITvjXSx+iNMaPu+tuXf2MYozjlFW0Tw7kjIZqaoo/sFHyiwnUPhh
```

```
890RfBhGCOtApNAX8QwoPyvLfbgELfBvN0HpDHdQrP7zYebfrP3zy89a18ksy9r4RESSfem2ZAxU
u7eHUgxs/X28hcn0zDBmZTTUmkxMj5/FU0Pl0RawgKC/u3jRc5VSfU1fqIVdf09P1xjNk/TwhI+O
a1raKrIeHygH0uczlZVXLeNs7mbqp8FJjLBybMXX3ydIwYpG8Eskp4tIo78zh8YHE+dsGw4hy2m7
N+gGDptfeUflYy4YHe49MYaFdQVakrNmalopXWMxPnN+a2m7Y5SxENcg/lBVQVJkGmG6cTUNDv+O
H+MbltRUKLIlha0EfrDZZSJkk+HlNqC/98NeuxSFDSNY95Hi+ySu3JMO9b7rXGqswfClt0HBqT/J
Hq4UEUFWA57lsrJ86KIuqi9oj321m/AmCyOZJseIkFvCK9+aJml4e5lu6c2tlSXD2hejG0UW5Jtv
lppOzSqCDsrBBBHRoWrIWNkjvdMyH3RBgyePyGontRR7QqY8cAC7Vr5wTh0sdjS4AFChm20TlXJD
IpvVgifzatUJew/QYQLqbzvV7OW0Tc9DlAtdD42NA6WWZ6ZMREBOs+FZtirB2W5aGg4CvT9qQiAy
18Om7rSre9sB7rNRDC28tIAJYMUsK29kBCjECDVdCfpjIMnLZKsLhkKTgtYibpBS/p0vDN7zxq9V
FXJMeo/PaAjrBlHnAGJQ3Rv5eyUHuYVBjHwKbcAScHQSU1ZPUMg/lP0jaiDXAdQ1QXL0OoDdJ4zU
F2RCw7M1Dp76ZiD7XWcabbuk5V82qjT84gMSBYMii1H6h/SSn01RAyXWsqfdcvUL5aJILocNKXu0
HIz/HKkfJstewgfdU3KRe0Ngx94IvrKN9+hYARrhNXyxPRWzPgDv5C/qMH8OYW6J2OV34TiRL0m9
VZP7PUzRTu5LBwc24v87zLyWOulFWyjSpSVgkpYOmTCRJa7nJIWwSW9227agLHhi9LPt5/QP0dY4
1sXR0qlDF800cuHTKaYMdrosiFZv3n/onE3/gGVVW0DIPVzQA4XBbEZbYUveHhwnFiXyowbZrYSJ
IGj4/ePe4ELInFjHVoUwqavNeVHwqn6tOvr5HMlY8R29My5Yla2i9XsemeO1rPgOv4aUYuenc0qQ
m0AHxv2XwpepVgKKVsGueaSIkM0tqOa1Hx5HxGEgXp9aGv49vR2lZCp5d++Y7hMBaX4nIe38SOMT
y51TlxO7DNuijnpCF0Sq4sNXA0SXLyPx43tPijQiUFITgB4/LxBzzXd0Rhfer1ZJs/1N43aHYOBE
m6e1uAbZoPoM4zxNJzLgKFgLDaaAuYIcPknac/JtedKauUHssaqXL47L4A6gDVowZGbQEPB4RHr2
J9AOIcjYmmZT+BfPfNNWL0VWeYQj35ZT53ScJSliQiWiKTWU0UQPB5zPN9dBaZUKkp7ax2vNk3mJ
gMR3tvPcPiHNdR083FzNq/iKGsQ7VqujWAiyNoTUmamJ96f9+m4Q0M872MbG0bsR/cCrTMX4dsEf
t/YnWaogRUcCXJ9wPBGW1b6Kp3WjDZdNSGg1fvn8tWt5JEj5ieFDu5LMEn7QW6CI+ruuYv5keorT
UauiJ0ipR2Z9nRUuJsTxqKrU3wSrpcZWug9Vsreu/6DJInHUFgFlx4Y/4RTTof9JWV4NY7JoNxPS
z7V6v7g+LcNiFYNj1iGQ/kYpgWjnsZ9nXCew4BG/6E1wxfSHxZvZ49juvTH35PK3mDT46x8fy8Yn
n4aMWBZztgcg83EvZu6VooIdD399D98Du+CvngsHhjsVR94Htx4c4HgDfbThgTYAAD0lbTVT3tmu
Gteb4UR6HW+FHj+F+bGpicu4KSqKlQko9TE1GeV42PIf+re84gYHJCsixumaHuHyn5ZA6Koa2xPr
p1NTTlZQzdj+X4C5HFjjMcs52rmHc6rvuQCI9MZL5U9xvuimZQu1M5u+4mVul4/1tvnOQhJ6pklq
6T4hIK2HbF3WrCIVEq+CHQi0Wl8f72MqQg/MgXaZYQq68CoLoTe81nEVV5ivAwT7hBuCSZKwjPCi
CKJBRBQVGEBWJGy9scIbMHloBG/DvdDofo4GAAkNoT09sREvlWe81Pep2yeZV68Q9aICNZcdp8E9
5h/JosjWku4kBxntJHmxjcsWkPk1gGqjBN9RGnJuGqoZ28wzROJxFKYTXYwhh9Yjvy4cPKf8+QzO
QI8RhsKr5kBYEW/SM4ldDOT6p33PRaHNzCUbv/dreMJFOmrXda0I2x4nrHD5mwFjTCOq5jzSaK7I
1SheiJeL3iWT5Rcxnk+zdGV6+hnPdF/01v5VeFG/0Zp0QJ7yJ8OHpwpVe7n6ZN9fyPg7a6Ni+dRm
0YBaBMKKzaSyCjIfWioDU8QvX1XdwYXW/oXjUcaX4CrxUV42RxKXxg0KFufMdIXYb9wFrxIAncMe
z8jOoDleL9CxawmM1pHE8mpGzjF9XuFmWlPL9TpKzdmtinBRjT09GRluPB6TlHk08GOeAaJVpEZL
z+C5zRMZWeE2uWnYvRJvS0Uue02bFTyY2O6+qTlS1q2Zx3m+iGN6eBin/ivSM7pHYADNtwaxv9/u
rTUyVeLZjd9J7g34vP9ppFR2e0Q5weBKmPHhCj8fpDxGkrm4yRogzg+1BjZGSKNrdBYJsk6psltz
mZXISMfUei+3R2asM2W7wkzerAcdwlwVRn07TSunA6M8oY6ygrdUt447UvO+CnF2AAdSlN3AaY5+
oX4KXlQeQ4UnVnB+VJY+Da/SxCqcbp49SKLvgws0iOwt0AAMiNNTDvjBhgKFjCh5Lnt0X8jwM1hU
zLA27kFM63cNA3tHuNeQyYlEqU7HcULum+hoTRwnO/aqlNg3o/deFHCDgTFlTbzoqeWMdR0koSB0
mOKxOddo7if62SmQsmTXW/SFieV9hFm04trjVD5M3jDFJ2d3NTlHzU8HM/XdgiKKHbt6TwBklmLv
oYBbbnA6vDdPBZmBihAnu0YkYROA9JGg2+H81+W6TY8xyeqbdvxLJRg7gbgDR3I4US4b253MS45g
BVjp4NzcmVqb5G7yDrSk2hH8AL6lQqTm1Jf9zSNW9SVN7/kFcaLvZNH26p2WUlZ6WWzCbcrCgkjq
X+guYYRNBZSv3xZrONDPk9A0+Nevs5cuZMb/CHXQfQNBwfOBw597MsebBtKAyscdgvl544Msu+Df
mB+jnO2lmU/0zvSzy4mo73sS8E9pFu7wEqM8S0gFcA2N4s2njb+bSFnbiqpYJ+Tgp5TqRrn9ViJY
/XoAUTOaaaISDjYKI4l3YHV7GBiel7aPXWPbm1Fu80XZsvyf1p/qyCZ//EOQRjQYYZ08AgeDRo13
cpg6HQ4/NFPdswUXMunpolkpOnMhzS3NozsRvP6aM8zuSfLs0zs9kfKg960qfAUQgFKboQARmQOe
bYILLRUG2QKjEVmOdGSTDbgRf/Z3d4BmXnAyLjZgORxadnyBYONchdm56uAOFJ/kohzE9xBUhZMt
Bh5kLeLqDXLKm2jwig24qoXjRU3vkszkIG9R/a7/irE2nVHs56xhrlIlXz4HRYoiYENRDNcXQTGV
ko0YcR0jdfxTRYgd3NNW+xhsu4LDmX9aqdx+GS8EUN5kE7iNvyzqcdONrK5U8DtbR7fu9/eJJMmm
d0MoqndklWmOi/ZLK+8bYgOXtNI3OwoXSO7rjnVpu6YHETVV+Wle3/j2aopEmCsTJ1DuAbcc/5Ly
7bT51Ew9EVzTzq2PqV30p6mnlpYYlWsy9iqxIhaMAjyVUYl/se16CnByllgIuuTOSBDvtU3acf6Q
fPF9Wx0/kDFBtdt8ebI4mhQv3i1jA0DzGmwtuw/Mk4oLUTJxeMux+katrZV/VAxCcZ37zY8uwWYV
3d7YgwGm/1timjD/ezOya8B0sgJqPBwezNSowFFlMbdAJrih2NBQh5NgIDhO+txwr0MthT8v3aQR
kM9klJm6bg8a5NHBovVNqdGu+2EP+2e8Sg8I7snSBv8U9DyPVtKyUsRqAkysszH0KOEAilMGvAT
o4+3vI7sTh805UBjQwWgqcRvA4i2JLw5VGekD7iI2MOdE3t/PNG7JkcDQKtHLzKlUErdJS97xABd
L5g7ZEBjX7Y4vyaYbzuCAaOYGdG0DOUZsRJ7sZvG3PMbnxa3o7FPDz1OoBN9Pc92wjBs4BucjBt/
KcmTlevCZ4I23pIjcKkScdS5jD7p6YK+B1nKYz19+VYjuczKQtF2xMbG6nU2TbxHPNjzETK8rq/g
vQ3WC6Eb8Wt71niPfUgrW/A4PwbtxcLvjCCSVKgYIbszp7YTxrA7nZ4tHVzZrcoS/abT0O6rfxKQ
oYFHS8KAH2gB4zIwtdQngOrf6SLABAY7l3XcBLzJuwa5r99Uegz+K/o7KmSYAM4H1cZnVL1s3EY8
6n7C/tFQWf1Dd+yTYvv7f/KAl494G/1AsXIKjeo0SuystMhOoKaPqd8/5QDtD40ElqCSDdTS+wqQ
kYsl8m5EHwj0tPyZKLZ9/VrLsXx+a5vAidwCnl2P6PBoyJ6+g+VwAPz7snCXjen5ACLDt4bK+L0I
B//V74yWLhjC8N3U2uXtjXdME3bMvF5cNpqYEoYKuHOBfLDbvDisEgv4bIg922G9AITThCzKmndJ
HJHXGlRjSU2cocPv2UZqLurwYhu5nMoAEfpk9aAtCJ8TKDHyqDLK8Se6SDt+VZXDjS6Iwrhyfqhs
7DcOBb3+39MV2+onu0UH1D9YaTfmiG3pf+psuDjelonAlFyTmsgo3x+Zy01GxT/HQvQ/ppWq8Y/r
nByb52vnwvm++yJRAtJP3/KK+3sxZx0kqC6JlH/W+MQwNC/jXRWMPvAJ4Q01Oi2uY1h2Tnisc3Jf
mG2aZsfMVjvehVVvWK3dDa6+C0sed9zUb3fnYnKOo3uzBiO+SqLYNwG+l9QbO+PaPSerfVnX1U/6
LQ62vtEiBrW/a73XXcMszlMNqZ0OlEPi02zxT/GXUaIQkiufk0Q1U1ats59wZHztDQbYuWzag4A/
0sDzc9la0Cc0GltAu8WzC1V36Aj/y1QAB+XeKfo+9VU9Ar40PK4ogzZrqSVwN3LZE+O6IH3/4wJb
YS0X5SKwKYQ566MRwAdOx5fFCLF/0jFzKlTMJoP2JYTV05n/CnsqCzOxWwuAK6RWLESSRkuilvj9
KfVtLoH5hF6AS6ujT7RYMO/cbtMLmiNCxvpXfPLmVv4H0j2Owg/bGmn6D8Y6UeBPG/pPt8L3Aymy
vfeEn/YnSEbryd83rupfWSADJydl4Rf9UB5mVmfS1qUIBBpAcGXMA3q4bEokNwJKzK/Mgd/xqsNj
3j+Xv+g+tjN/rWGNB933hI2ChLBLRFN6opBxRh4pPleTArAkNAlwdP0eA3BJXURf0sYm7FsGotK8
lvcXz0aysmywCxV7l1JcZqKTHqMWLN63EUIE4dZKVVqBJ05uiQC7kmp1PLBKK9ButxWkGRblKuKq
VRQBDsoCLllvSATFLbFqWEZm/t7ZRI50KvOyHLGtMKPKgXxieTM3/ZngRuf/uUvZTmgcOb1bAfCZ
b3QpPqDckQpv7XmKCYKbqoppis8xLJAsZnpCzqCaEh1wgli8+7PTKE0aOWeCLxU+cwbODzbYexxA
```

cZ3DG/8RcK2weavNtKPw8zSMaScPhcnJyC+sPJv9P7UL5kGNfSl29n+wYy3grFycLJ3gTV+WTrn1
Sy/nHYkmlOtnwIZApImRsdVZ5KoILh0/ApdBjuuYI8fYbEJQ0oqc5b1W0wlo2/85nAltoM29WCnC
K5xn1ZrSWJdZkVzzquwkDQZYEwcfkwXMnNnrH/G1hSmKSUds84k+xWEZlmSVoEKBWIg+trwPQ+L0
P063PCAzDJ9RrpuXE2RObS2ts8PUfe4J4/qvwmylj/thuA+7R9rmjyugCRuSJbk3eEVyyNhpN5ZW
OjVNZCNT4Fu/GecC9iFbqOR1PePgs/3xP45Um7HXYVG1CflbInQnLvH+aZzGxyAkiQFlZL3QS6Sn
zS3NoJsWjTsInwgMGMDc2xH7lrOwBGGWIRvs59P16nLfXwK3YzAqG3nrr3gTogdVbhaZl1QuaqXD
RB1PEo3V6Lj6A4rFXPkNL5y1ZnSXHktywhxvDym2j5Totc34qTZCprxmdiLxyvch9bR3jlNmrrlE
MGvIUBchpXI1EMfj9yAcx2R9f/K+k6zHIwLlIW6Lw794AsOHLjfzoV4NupdjHExCVJbOxUs818Rs
CSLR63w9+Kfa8Dwt7GFLFLEaFQNmeTzObRUXNBGrlI+CT/V8o/eZnkYrzb81kX/zYRYNNefugWhz
puSjzohwBvUoi2K23Z+VguWDJblFzZpzbI9UZoqsNDL4tB0xnKmPBdpM6qJCusH/oT9xOYxuK+iC
GHNtfrDNluwXPfRe/H9zZKrRaSX7U75rPA5u/IKjBj6VAr8PeYx+wcvfUz6XSImdmWM5CPRu19xp
T2ZG8UApGHVhYaSRUarQQyUBIwBitPutVwA0sd/oHfeZN5INI/CQE3Si8TRX2B0NN0TERFw59IgH
Y8YV3ZEUi4Wumsr/n8Dlhasxb7N84p51exMQ9+aX/BfbhuyVgOKw5IaNKx92TvYDoQCi3YQKoThR
G1TUOi6j4AXGGZsFOMwIppYMCzWWmc2KVLct2x3B09Al4rQfSdczYXyHTx/XzqH0IoJBwasN2Tzz
z9IT1gj1VkN60mpfc81F+JgyrHK1sjH1uoPmK/jiEHw2PrLt5wAqYFV7xRed1yMgw0bB1hWkL6hN
f2sBPl0klcvnfahZcREbZzTOhupQdw2YkZ/KOMZrwnbPNVvH7oV2nW/V3fqLLt1UEIUY9ovJdvTl
WpD19N//TR04Xh/5ap1pb7v5aku+S8qnufb6hi3AO1ArXlswTQJxKLZjiAwVqntpxJVAb+GBAkOo
0YEdvaXAVd3NCPAnq31a6lSa0cBfQV2xMRJ1WFYq8kuaJmFXvUN9sq6AnYpfo9zHY5iMuxJzpQml
o8vCnLQ84JIO1HGZ1XSVHZ8nmHe/kqRU+N3cYaA/0lc6iMlWyyC2MEJDSqAf4g8qUMNQ+yAxykr6
ClayP1GiiIkJRNd/qkrCF65SBL6CY0XIzZJTulCwTzDKOp6oJkmJobv1PAOW+Y06w7+wMdkXF/72
AmDjkguH58uma8j9kVRDyFEO6wb1vzXm89FDaNy/yOiUcfmrPCZwoLV5hOMPX1ZV11sURP1KIzZV
JcLA39d9oQneVsX/onkL8BBiS7tMMdhdei6AqDH/znrD+aCF8Mx+l1QPTzqd2OZQH9Tmb3tOwV3e
RF9fL7RIhHQmRN2V1+Nen7V3DLUmjkvq3PLk34ZLcpZ52eD5vwA2iDYkURIy622MIt5ROjwp1ytP
w4//Z8rs5rBNSrpho0rpD6iZxvEcMmD6EatNVyE5n1o8xSyUn+7M4lvUSMMR3LcGTL0Ge5yTI/e3
g5KGRMZeIIczKkvfx7r5BhS3r/WZtqFcAjfJRXNyYAkCbRpe8r8lcrNgOBM16XOEX3royK49hwno
KJjF66to9gaQopRiTG0EPbxOZI0mWy6HoLl1PGFE5Scv+wSwwqj+mJXOczzxBso2hONwuYfdFr5e
a6c2zkW1JXnKRoNdBYvFgC9aynImDk8xXYkgI7WOyJkuZopGJTrHg5cs17P+/LehxrZs3n9LRzV2
TQNjDolSLe9SgdIjlzpSZFwDGS4wNLiGUVlxGvRrPiSYJOBdGici2SU10kxR27VrnJR9kNU7l6sz
WhP4wwBldt62lUJueevJF/t3d8EecPyLjRmnBtFp2OICgR1vtogwQzrpYUuZDoiTLDFewLFLHhxM
upDxmd769D2ow88UA8alHAq31BHGCMLoTkyJxAwkyrbXEb5iUzXzUzrYoKNu5FhlESd1yV9mjb9O
8XOwSq4tZ0sixSy4dKqWkkTf3r2esJO5Gi89tpg3mW/NKp6gq5rZNf4Lg5/4DUx+PYVKv7P2y/b5
SoQkvpOQTTDZa0+w3QafloIYyKiWQJ0SiKu1Efll1qboXUjRxvaCI8J4yvV6mbjeCb9eFHtJTGxQ
AIbWuuPHeXtxsgmRe/8NPfmooSeZZHBEMFCZxHUKhcqKJyhqYoF/VKz3U+dgUCUfPnoDgU6w5Cn6
xltNu4iITijsugIpejgv6evhhOfIjabwOe0BqiQ5Z6cdpHoPUmoFc96EJxSnljnu8FYWkbImCYE8
0iy3jtrjfYgX8hmvAw7vReHDDYCU1COpkco0o1ZA+vqKh6MDyVo8620P9qjjZjQ3JMdSdNTXbeD/v
mQs/erffJJkkV3dYEDQ6kWZvdjR9tikudUyCewZ69xwDsUbEkXvCCXcLx7V1Ibd+XOSqJxDdYGdK
zTgJsONa9TjW4LG0z/FgBuO5UVmJSDknhJb8MLA/JxS4LuRWGs04t7YfvP/aRLMeTIj4bUjWz/11
DfElWU0KAzDNmQ1kpqhdE8ytFvLN1u8JqXfAZgH6NujnTkjdR5pmwon4g+LjUvFPKRKVkbKpPv5b
kLTMtd6a5t10AsaA+gSSAGvZ85D74u2xfqbcLI7+IoHl9fYTtjOt8alVQvUd4yr2lX/+2/yrQicF
kx62u/4HWebYKyXPJj/8jWeOo82u3DgOfdHmb9+xiz1McX3Xh2XQXEcJ4VJfAjYdmPxH4rmgAOfl
0aoXeMWprYoMJ2x3IXs90tkygWG0CaP+9q0LqJhO26eJTXLdFwq98IE8JlGgrsIs9tMRxQKqfPKu
kiGB5xg1jzGfyawGP7tfhWxMo6IwQZ2ygnBbmCQVpdKci+7pkb046NakpO0Mo3zPZLX/ceNesGW6
a6Tfegq/iMtUgs8clYi15zLsUdkngMxsVivvQT/a03D4caYdSvbxL3BcFvSZiBWvejpq5UU7sfoV
aHtGnF8SmkJG1nGWhdcgvFmDxYf/e1UzkQDyz1ETNhBgogKpg3wzMV9SNLhE4rjEx3vq0d+5551N
hJh/Rgq9QqYdSdu6j7iPo26fd3QEmpMH0yhNUhmZtzvWciEOB+Anhw5/xgwDpFITksZfH0BeIE49
nJnVsCCALl9RqYDm5qUI5QdhjfWpSqiq+fx97EI3D4CvrX7bRh2YmhFR4ZBu+8hIv1avAYeptsEW
7QNuzONXNQJiEOsVS9bdM4kSYcW+2bnoWYgkDPFmuUUu/2kikN+SyihdpFNLfNe5cM0/oMkZLfgh
0WK9oPS7+bLcVPqu5uoLzdFzu1PQ/hPWW7ozbGJVVsLAKsaK64JRtQ7jyjfO5hkYDeSF3DJbi7WY
EcRhl81ZI519UubAkYKYcNKYVtEy93Ng2uUfvkKWaUnvUb30ytxuKTInz/gpA2cPiBf6ypL9uzV3
QJq35hFX39xikevZK2t3YJ0Qs8ZhjxLboOaew9xVld48aNUpN3mqZxgg5qHyC9wIRWo/aOGzND7i
3uM6tdcf5clLjt7H9EDURvlaZbNe/7NDbDcUXTGMBzSt6HHO9AzMktoqPbF29xbbFFukomt2JGIN
5qGnTJalTgFVaWNpE5s4trIt0cOfX1jFVRmqvCE0tIqHA+5mMTG04/p0ByhHrS4qzr4ksVFzdTPK
jEIbNocmua1ThhTnw0QwfGoKR81bnvoXDcP2msFphGvsQY9mPIjmVwvevUPn2i1DYOhROEkZJVtO
JqVZmlftuQdF71MtpqMtUT43ETBxYrH44Jj3VyUH3juyqGjzE/+VP+1ASEEO1P6M58E0UnOjVy0r
smkoiZVFp/FSc52Afn1vhRFB8ZgA3vjHn6ALphyXPMrlrhSQAimJw3mQU7EMDonYs6YUdvtf3EPR
OTA9G3rmWyPhDQysdqiRJw4aVZOkzoOwVmE2Av2VcX8553B+aIgYmRY9Yp55y+5/hFDneDFgAv0d
J/wc95i+tZcIyS6Pwq3eNQk5LldMxAh5hs6b5JW14R1hfjEY1xcmctYOW1cRGWIxRGlhbvzNQV+U
uomaz15JRFz4p1851pi5ftuGPk2nLEuwTTpIk22Z1FupuJd2EWyW4/chV4duAqohcp1+yCTgtm2t
f6PprdUwaNlKYjcb80n0d7F1s44E98AMC9hisDVFjmM1RgQ8Pkk8nlGB6ie9i+nIuV2RNf/j0JK+
A2yXSC/rcgS4P4wOA+Yuq5XadUA1lci/nn5kH23XChSpSIBmrxF+yuof+SNHF8Unbm2IqRRFgTvY
FiL+nxQ5QmiIfnjXowrDEp79qTefysCoflgwVpFCris0ggS/K3hYUU3BWimDhwG0Y8ZC+qWiI6d8
m2GYjmUO2AlJcsn1kGHA/L7bfXVvMv/3lpgp52N6H+Sbeb2FNEM1YXhB1DHuOku069gLPSM2EXc5
yCSwk/B+pWpQ5ANctN2/VJSVS0x64jyZN/KwQpUSV2HDp6F7cUydN66VaQUhjCY304fpQvlckmjB
CLw5WwfDoWGgwMcLfXcNUdvO9KbnHCUmSSUC95ttAYGacvxNk740fRToRm+RjbJ0R1wjOnERbL5U
sByLzXcPawVwo2WdZqPmhEKvwx0EXDYnoYjMXtP60Pirb9ZSV0eGLfMqluKCUP8DG5aswRoEexAu
F/UwvyjGRI8IDO8gP68RyUOnN7CvQqTRL0csiBJ0JsdJaOVNsykehwoBqo4chiPfjl0BZ+VjOA2+
4FIlh56sZ7hI2NIy7MALy+3tYHth+iGnVBVBzbu8AKMbah7ZdjZSW0wVoJ4U99gBghQBzQBWwd98
57fzBf2WibYGj6Vj1ufGjyYMDMxWS3Y97NA8992+6mMfRu/Nch2ZnK0U+jeAWPOdRDwwJsap3Oty
AFkD40iHripqks0JqbMRbylFViA1cuoXVOyxUjJ7V7bK6xIvd+4D6bVz7oiGoJUujTFb+M/B0r+i
yPkUvLp3743x3xtfy63PpkeI2ydOzAwpxQScAlSd7UU3bl4xYozwHcjheAMw46h537WDEZj18dck
e6j9+sHObfQJv6wnetjB08w6qLXmOf/fi+MpybEQ1YrzkS7A88JsWFMdf9JeV37qX1AzKfnRdIj8
vpjVe9gEadFGF8IsQ3AnAA053Mx8tEUBmuuJyEIOZebOznViVMW30W6qox93FGXFMBrE1bhIRCdI
g3tnhzoo52wmNMDt7zt5/f2GYv8nuEhJtTcbiNeP2UREkQXUfOBQA2V140uskwIdVW+jaTmPSiCC
WDHToA7ryIfCdy6hXUK1UhPH1TmMv7uhYfuvhEHu+LoqWUD7cpkNaCW3NCemKXpVHrvzyRtwyx+n

```
nxnw+bDF6jMZ6VBrsJxkFBx5rpikTv9rfPnZ4lZNTbT+21Krgv9gl1C6l6Da3KMVQJCabqc5OxnE
2AO9xMhHZwTVC/TdOPI0TvFQ/kiWuvxWkV/YWYBjfEkBngXUx5GOMDRiLgW9RAtPeJk376mW3bfB
2R4FzZbj7upogFLGhFjhpsBf9uYxDn45UaUk2oxnXCBuKxy+0LbYD6i1oqwydIKQXhMybWAFbW4B
LyG+iVPZIxwMfIOcfjv5HagouBfHhn+6CAtKbyS1eWlhLsGXXuhZpJrJMLlHImgDBKwgXfc8I2HL
5EHAQ3T3Z7OQ2siPTSSRs1IDRQss9yMMOMGOZeLYcWMM2oMQeTijnSgfQwNmRtunSvQ9nf3VLG9z
d6+NhaGsEUDgLLo1V6OxdSQRaWZAPXdsd7wUQW6Y6RcmxHUyNfIVHscnGKX6SAN+Mntsn5jPlt3V
w0tazBlpUOEXGEawD6VnpzV+7IrNiOEbWZfnwCIq940wy+cp2Zs9t4+7pSth4Me9tIemDJbVQL5r
JC+d/x4d/Jhf+CB5Y8/PvKphitIKysOxxLRNjNg0YETydFTu10+e/VyjY6NJKkszSiINBTZBQDvc
TC80Py0YgWgaSY3V1zQvyIxgYwZmM46PJQv1L5ri3waaOu+jPepnPXGp7E5pzVg2kmKImaKt5te+
rxgrwffTEzPVr6IgcGmm4UJ+MEmh5ckKdDECXp1cEiCCt5ShN86hLpHMy5D0hoPzRzpwKg0esAe2
yYn8FkDDt1DK9PInDvwJKI19Jc0oUsQMFw5Dj1B0t7HmGfKhU2oz/xLhvSuXUqq2S6sgIB/fzNWh
/Zq6vbEh+5mnUcAyJ3f81gPVHxgdPikmAWqyFJMPQw1GWkE7Kcj0Uto0jcINat7R2DxppkfCK0Hs
SBUtZPVtPyFd9O4/yqjyl4LwYfieN2R7QsxqzNzdhy1ACxOXSp7qfIpN5ZjRaVpfcJjOEbo3YYLc
dG1A7gMys/Ye0iK+4Hdn1fKn9eN9qAHUuQo5OeWPczkgS198x9io9MWJhhmL7lJwtI9VMs5cFYwn
o+W4gg6jpyl8omp6ZXNAAWvbvhYCAGWsMoksr3+sCtOz33xlRqoFmZL7kMaomeJ7rTtK0USETqHD
1TJkaQPHFAqz0tHkwk+cNxedKpBbopiCaaOTSB/nu6v0GpOtZI5rqYv9xsegAE0tT5nf53qrha3N
aPFJcFtm/lKzhCAvHoiT+Sf6igPfBq7Y4n18dWD5Hbg5Tdc78/w3TeNgPNli/Lqr8cyAHE9II/A4
FSZCGNuPwKHSDz2HGRLfZMHYLFwu8l6tC4DCaDUpX4VqZ3M0QxiwLUqUX9JIHJsjIZCUSZ1QLuyA
OPhlZYb+8jYD86c4qYXpaC5SVvDNMFpB9CypbjnZCZNkvnIlO4IWNd7dOattKtR3t76jqHNrByGL
mP3+/L/wTkMLa7cnalCj3IMjhrHMTU2TLh0vYEo2bJ044EHYOH3o7+4fu31qq0sohpyqCN7Y7pAh
ngB/Vr9D+WI8CgkqxexMeTpvjXjSTE892+hfG8jTp+07zIL4oQbEFTVKWDi8vjMfIwBcrF/nO19X
ZCXLaBJhhYV387oj5ODpUIepc9/svIPGvRWyKit0RvkYaoHL6/awsPsmVCjbz/xTtdSwWME5yuDZ
ZNmIhNdJbHj5dz1qEcgTR8kLhQFuTAF6mxBwvF4O8Gh/TQ32/H0tc+tF+R1lkxMGdEHb3amZV07F
KwwEizYfpwDFUKbNQSE54iptFIn3R8CX/oATKoNtlGu1hkdsgB0Fb6143+hkXNW2bi57QAE+rW+t
qUiE4ZBhZWajLhe2PyctZe1uM9rQSszYsmrjTvqXk8eBUIUGd81jj/htwTAZBCm42R6v2AnU0Bdx
QP4mbHHfa2piHjxfO0eFm4A3TRJeRlIm/ZSDRbGXshQD3lQXtj4r2F228tV+RwQ1oh/v7yYRR4RB
xgtLg1AtjQwHXbiaQlvXMpC3wJVgoo3I3t22Iy2mw5Upk59egLQBhMoJdIBukUiBMMYKmELQPmgs
y0vBglGU0ZUMrcwJ+lXtw/0Tk1PXwVeIL+gtVNuIIkZRl7BC/5Yq87ALu6fdq0DIN9bWQQGxjQiB
Zzftbbp6tCgDm29srb21OhXMZt4wB/wjR64oOfsQrqjgLpbu7pJXxDuf2Dn6vHtShqUFShXOj+pz
sCcOt+OD0hLpGAm1k5RdW9QdL8aZ4Me9LEt5To0y4Zvw5m9ZxKMEzZfNmJP+tUIzkJbK9kR5nYmC
ThCha91EnJ8kXpJyPEAdMNo3Z9sBpd0bCq3GRTlrJlSYzg/MPxW1XPSn1K/sqHyDOKbsHhb4Z1U0
zFpMdD+VD4a/x310U0j2GXKXp2J+gpAXlIboZNVJMjWuP+YKpaXVDWOEbakvTr/3BDEjZE+QyAmF
6LSwaQavSTUMMuD7T8eBWawQjvVmPaXrqbT49xl4hbEUsvcXXUA1C5A7QEAGBGbJn+bCIWuBiS8i
cxA5IUda+w5qY6Uj2QphfVFqyynKd2NQFqJgeDrVP3cxGfk8ME39N2l7fOq+a4Dz+7QP2ez06EJe
6SuYUQaKJoJl4k4N0B4S0U8Iy/GOK9QRu4IkNE8gpvTxMpDtuQ7OE6ta0CPWRgD07DSEVj+8Xid7
EaDny40w09zy2wUmwwOd92b94w4xQhXwnaZzFmxVT+M08kB08dSju1/+5e32feZlOdtxSnaLktsy
aaX2VJg2s11Jihxl2kG5/W0fi5ne16hEpovyEoP4wrV0Eb7e68g6TaypRtL+ROLccwR0aIjYKGt3
olaSyLD9Whb8jIm9vLHs7IHOI57hWxC2V/csDeJqABOnY3xJLL2J1n+4Nhzmx2MP03IAcfSCYskR
emyg+rqxJIniNs6WDMc2yufqDgvqlYUG17ulkZs0TQ+IuX45RG2bJbP6wPUESo7g+RI+NHvgYbUM
MNBLn1oLIPvrmrTcVSlB7wat1v6zpEpzZWk8Av5/1aertsXUL+cuVkwAeN7/WqVwfz97DzF/V+g+
KbZh/a4DcXx2</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: Sí (Token de Seguridad – BinarySecurityToken)


```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413473342647-929499707">
                <wsu:Created>2014-10-16T15:29:02.647Z</wsu:Created>
                <wsu:Expires>2014-10-16T15:34:02.647Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" 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="XWSSGID-1413473342647-
1639185597">MIIFRTCCBC2gAwIBAgIIFl4IlQK/pRkwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3ViQ0ExIDAe
BgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEwMjMxMzAw
MjJaFw0xNTEwMjYxNTA0MThaMHMxEzARBgNVBAMMClNvYXBTaWduZXIxEDAOBgNVBAsMB1RlbHZlbnQxIDAeBgNVBAsMF1RlbHZl
```

```
bnQgR2xvYmFsIFNlcnZpY2VzMRswGQYDVQQKDBJTY2huZWlkZXIgRWxlY3RyaWMxCzAJBgNVBAYTAkVTMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAkch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0ptsmAVJ9OJ7D2gM
vPgQNJEOshdFyG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MPxKb4NZm5fFd1LGApXNEPZ0OC
OxpGkIMwn/YkHSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0aWqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u6+GuHKijZ5LUe
VrSpjcRq9Nhp+gVvqnaxVlmeRgG7C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQIDAQABo4IB9zCCAfMwga0GA1UdLgSBpTCB
ojCBn6CBnKCBmYaBlmh0dHA6Ly8xNzIuMjEuMjQzLjEwMjo4MDgwL2VqYmNhL3B1YmxpY3dlYi93ZWJkaXN0L2NlcnRkaXN0P2Nt
ZD1kZWx0YWNybCZpc3N1ZXI9Q04lM2RBZmlybWFTdWJDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwwrU2VydmljZXMlMmNPJTNkVGVs
dmVudCUyY0MlM2RFUzAMBgNVHRMBAf8EAjAAMDsGA1UdJQQ0MDIGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwQGCCsGAQUF
BwMIBggrBgEFBQcDCTAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0
cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04l
M2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8E
BAMCBPAwHQYDVR0OBBYEFAIYOhNZWFgafngAgs9tQ74e2yeYMA0GCSqGSIb3DQEBBQUAA4IBAQBmeMs+UdPMWY5Icyn97ZR//LOf
k6ElAfgxRs1y6DH1oJdiWUnVkHmSgGNY+Y4j4y74TMiH25naizyyKQzmGoHw7KOgTxxqUEwlEHZPuf5GIJxc+/a0askEItRRgf9p
ozjL2+RS4YMU33xJlyBZNQ4nrvlKyNx50favpiKD2kOuHFqu3CypQzEvWw8uW5RY6Vvmujc3pztwjZtMeatWTbxMS8+c4wfT7N5b
gRFCH3t/Wu/yhKQlnfkXGLdpOeIt2pxIKH15UR7ODMmlNcIIRJQPoCPm5PWPmo24BkTb5U+nr1y4I5yY/gkIOammYYORPb10i1vx
9bRX1llTnWg4/YNX</wsse:BinarySecurityToken>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-
14134733426474534989 58">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413473342649-1566885839">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="SOAP-ENV dss"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>0kkKyznc9DmcH1QdgDYQhtIc7KQ=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-1413473342647-929499707">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsu wsse SOAP-ENV"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>qWgVDOlbhPUh/qqBTba4V+Bu2Es=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>J5bAp1zuiAyFnCrmt40+qKAUBic4ZxFJ1NRxENso/uOXkktPJy724Czwmx+lZ5XtgUi3n9GyoIJSdUvpU
Vg6dzD6dlrPho65iHgdZkQt7Q7dINQKcHnJkaDZN8arFPuCeSDJnkpk93XlpMHfXZhciYm57RO1VIp1beaQecucfomD8+ahInst8
hZpIxUJSkODzMFrsUJDozL5O2vtjcE0UOAjcCw/1MKb2yBjFJ5yCHHAw8KhNWKz1Pm2WNAeWwigwNpnTw65oHL/5o1k3TVpU9T5D
9SBQ8mGX+kK8/MdepWvbbFDXP4f1YPEdcxzgkjwQVCHlfQoRZ2yyLtZhXunQQ==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-
14134733426484919409 45">
                        <wsse:Reference URI="#XWSSGID-1413473342647-1639185597"
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>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413473342649-1566885839">
        <dss:SignResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-67ad6ccd-7a99-4072-95a2-
3f63bb1f4d3c">
            <dss:Result>
                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            </dss:Result>
            <dss:SignatureObject>
                <dss:Timestamp>

<dss:RFC3161TimeStampToken>MIAGCSqGSIb3DQEHAqCAMIIHyAIBAzELMAkGBSsOAwIaBQAwagYLKoZIhvcNAQkQAQSgWwRZM
FcCAQEGBSoDBAUGMCEwCQYFKw4DAhoFAAQUySErJYEqdFwOFyp2icgkiDF/MiQCCBOdo14M6bWrGBMyMDE0MTAxNjE1MjkwMi42M
```

DZaMAkCAQKAAQGBAQGgggUrMIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU
3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xM
jEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50M
SAwHgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFU
zCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebq
z4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3F
eh54cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi
5jDBMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwg
gHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZ
GlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1Nlc
nZpY2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEG
DAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwO
DAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q041M2RBZmlybWFDQSUyY09VJTNkVGVsd
mVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4r
vVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpAB
wE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6
pfClWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/
ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3MYICGTCCAhUCA
QEwYzBXMRQwEgYDVQQDDAtBZmlybWFTdWJDQTEgMB4GA1UECwwXVGVsdmVudCBHbG9iYWwgU2VydmljZXMxEDAOBgNVBAoMB1Rlb
HZlbnQxCzAJBgNVBAYTAkVTAggcbqJjqBfPZTAJBgUrDgMCGgUAoIGMMBoGCSqGSIb3DQEJAzENBgsqhkiG9w0BCRABBDAcBgkqh
kiG9w0BCQUxDxcNMTQxMDE2MTUyOTAyWjAjBgkqhkiG9w0BCQQxFgQUGRM6K0dPl0wCiilOJcWGkepUMmcwKwYLKoZIhvcNAQkQA
gwxHDAaMBgwFgQUCy2O7ZpW2Svo/nFZvnZdr3jvdjAwDQYJKoZIhvcNAQEBBQAEggEALBAbntjkf8/1U5NjC6dmQMCVnCGLIh2tA
GXZqNVEPOAacXOO8exAQ7zspRk5550zDc1A0ZJv1Omuo2CszQLA8wJ1cDgVCPMQuKPs5je9gLhYdYBwou4Vgaq3kc2F+j6APVijn
tUeffx4/sz1dsK2xLzRJIpYwke3FR+mCHSVEAi5HUeDscUBMCSnuOsku9+3XKFfyEzxMxVVhWPVttB06S+yrNX52JKZ0naxpK/Zr
A1c4gzVjNcBpENoac9gTjYp2KPPMzxWUrxNAplV63pM+zNPTlGw6V5QUEsF4YgTl0TAZsK1Md9KEL59hLzOmwztNn6oGB6c+8Ihs
RyajBEtowAAAAA=
</dss:Timestamp>
</dss:SignatureObject>
</dss:SignResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

A.3.2 Ejemplos de Validación de Sello de Tiempo

Servicio discontinuado (deprecated).

Ejemplo 4. Solicitud de Validación de Sello de Tiempo ASN.1

Petición:

- Securización de la Cabecera SOAP: Certificado (Método de Inclusión del Certificado – Key Identifier)
- InputDocument: DocumentHash (Sin Transformadas)
- Petición Encriptada con Clave Simétrica: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413474128035-871892913">
                <wsu:Created>2014-10-16T15:42:05.254Z</wsu:Created>
                <wsu:Expires>2014-10-16T15:47:05.254Z</wsu:Expires>
            </wsu:Timestamp>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-
141347412525334488837">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-14134741280351238157106">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>5bihWWSrcn+psZN8nIh2HOribzc=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-1413474128035-871892913">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>AeBV1+WIt1tLhrxOQkQpVuk/4PI=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>aE8y9eu9A0FC4ZScaYnO5dOnAVwHzvcVYVd/lV+xccmXDjTbdiLvSu4wAtMrS8oYVyao040frR/K
DRgqMQJ7oCzaw9LIJZNRykmuCHPaKfGBXZ21Mgj79Xz/EYOsMstq4OeV/k6kM0JnsZbNIqAufTvM
8hA7iBKw3+ITH/+t/hjcPf5vZ3NQK2kSrlSPBM9sTye8Vou1s3N4xp/pma+Y0+ZSEnPGdFWcPMEt
bZyzU9LtYPdKgYWtcbLro//jWEC0GxlNTHvIzDVoCLiYeh0u2UUYrmyQtdzDGHBU9EVcENE8Je9P
JPP+j35TlGzp5iYEd4LNVts46g6p2edmrUEwEQ==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413474125254-
1218149107">
                        <wsse:KeyIdentifier 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#X509SubjectKeyIdentifier">Ahg6E1lYWBp+eACCz21Dvh7bJ5g=</wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-14134741280351238157106">
        <dss:VerifyRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
            <dss:OptionalInputs>
                <dss:ClaimedIdentity>
```

```
                    <dss:idAplicacion>appPrueba</dss:idAplicacion>
                </dss:ClaimedIdentity>
            </dss:OptionalInputs>
            <dss:InputDocuments>
                <dss:DocumentHash>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <ds:DigestValue>ySErJYEqdFwOFyp2icgkiDF/MiQ=</ds:DigestValue>
                </dss:DocumentHash>
            </dss:InputDocuments>
            <dss:SignatureObject>
                <dss:Timestamp>

<dss:RFC3161TimeStampToken>MIAGCSqGSIb3DQEHAqCAMIIHyAIBAzELMAkGBSsOAwIaBQAwagYLKoZIhvcNAQkQAQSgWwRZM
FcCAQEGBSoDBAUGMCEwCQYFKw4DAhoFAAQUySErJYEqdFwOFyp2icgkiDF/MiQCCBOdo14M6bW9GBMyMDE0MTAxNjE1NDE1My43M
DRaMAkCAQKAAQGBAQGgggUrMIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU
3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xM
jEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50M
SAwHgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFU
zCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebq
z4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3F
eh54cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi
5jDBMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwg
gHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZ
GlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1Nlc
nZpY2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEG
DAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwO
DAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsd
mVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4r
vVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpAB
wE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6
pfClWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/
ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3MYICGTCCAhUCA
QEwYzBXMRQwEgYDVQQDDAtBZmlybWFTdWJDQTEgMB4GA1UECwwXVGVsdmVudCBHbG9iYWwgU2VydmljZXMxEDAOBgNVBAoMB1Rlb
HZlbnQxCzAJBgNVBAYTAkVTAggcbqJjqBfPZTAJBgUrDgMCGgUAoIGMMBoGCSqGSIb3DQEJAzENBgsqhkiG9w0BCRABBDAcBgkqh
kiG9w0BCQUxDxcNMTQxMDE2MTU0MTUzWjAjBgkqhkiG9w0BCQQxFgQU6iqGbJY49u11Oe0dHni2LvapMNQwKwYLKoZIhvcNAQkQA
gwxHDAaMBgwFgQUCy2O7ZpW2Svo/nFZvnZdr3jvdjAwDQYJKoZIhvcNAQEBBQAEggEAVEbNkz6ie1epOcxqyI+EMM8Dt6oyvWnWm
5+RnKA6dFP4+LS8SLs95j+98QRqT90DbBVsmIasPIJW4ZYUSs0d4UObrUwTdu81iZcEHCjgatn6mb8S33xqlVL4LcfxkldnveCvW
vroX3SVdv+6RvSaLHcXilUskg2lpVzeVYcPYxeODqEahWDIZ6DEY63v7rZmqUbL73j75aPcnL6C8+chAjyI1Nx5OQBL++G7b4sWK
8lS+W/11fgrouqdXXhtVy/9vI4os6zkFBPqskBW43lRENOxaMlKDr6fQmpWxp2kQ3iPgZJPieg5MgZ+2cvc3zXk20o4rqUXS8Pvo
xLrZa7xRAAAAAA=</dss:RFC3161TimeStampToken>
                </dss:Timestamp>
            </dss:SignatureObject>
        </dss:VerifyRequest>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: Sí (Token de Seguridad – X509IssuerSerial)

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14134741281543121800 99">
                <wsu:Created>2014-10-16T15:42:08.155Z</wsu:Created>
                <wsu:Expires>2014-10-16T15:47:08.155Z</wsu:Expires>
            </wsu:Timestamp>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1413474128154-
84067893">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
```

```
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413474128157191232318 9">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="SOAP-ENV dss"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>uBWPXWpYJV9STWoWvsJG44ad2oo=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-1413474128154312180099">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsu wsse SOAP-ENV"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>jLaljaSEQtlLV4BUPdHer1qY+Fc=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>MuDakRQ5Zug3jmgjL8RJfYPkni2Vcce1O6zdbmGzR8Io0o5gu4TV/x+sFgpb5drIEkq4zR+w4qv4qM1lQ
fyLhiEUqqUr/3KIcyIf1O8YJbIW6GbfQoljDiqhQZxeVFc1+Ck8l2k9+bT4yKVoPimEBouKfTNXZIQsKw9+5omq3zLeAqS5VCneY
Sp9OsaCA13M+QxdiJ3QMfqHexg0q4LvA2d2nOJXequxboLbhu4a8hazxztHw2U90p3JazSQW0FC7h7fIZVx3JQtLn84T3QhxCTHC
NorIzBAzVnHx2Lk1atR/m6x2Knl9SxlJHfv6t8uMGMRaMt8ZKESL5tplbf8qg==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413474128156-
1506002930">
                        <ds:X509Data>
                            <ds:X509IssuerSerial>
                                <ds:X509IssuerName>CN=AfirmaSubCA,OU=Telvent Global
Services,O=Telvent,C=ES</ds:X509IssuerName>
                                <ds:X509SerialNumber>16117351527344796 41</ds:X509SerialNumber>
                            </ds:X509IssuerSerial>
                        </ds:X509Data>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413474128157191232318 9">
        <dss:VerifyResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-44d1417d-9a40-4831-a004-
5e66d3c42f35">
            <dss:Result>
                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            </dss:Result>
        </dss:VerifyResponse>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Ejemplo 5. Solicitud de Validación de Sello de Tiempo XML

Petición:

- Securización de la Cabecera SOAP: Certificado (Método de Inclusión del Certificado – Issuer and Serial Number)
- InputDocument: Document/InlineXML
- Petición Encriptada con Clave Simétrica: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-141347462920379523147O">
                <wsu:Created>2014-10-16T15:50:29.202Z</wsu:Created>
                <wsu:Expires>2014-10-16T15:55:29.202Z</wsu:Expires>
            </wsu:Timestamp>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1413474629201-
1293403523">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413474629202-1610461795">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>0FRhf7JyUrdnebLwpOUsf/6QSaY=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-141347462920379523147O">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>EAaJ5lFNb4KnVucPNAwBl4Y1Rco=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>iVbD0A4pmfX9zAcRLivbERyr5eQ8xoA+KDpIbpMWwM7u68Q3oj+Xjwt30aPOQKtW0eAJJ1aUPH+O
WCI4WWR3HkAkSte01hbPDk1l1M8audRI+sXa6aErpH5ZuSpiHDj+HtEV9ewfnwodQ7G0aynd9MRV
NVq4InwCywkQZ64IjUBjjmUsX4COOmzKA/26L646D6pEosO7BvhlbmTunwiuGr+Ak5MXVeHvbHWs
NpowAC5wtxsPaU/vtILyAU+0CJktMB/ELrzW4kI6AzJRxRLhz2B0r2nymdEJcrpTgVreTCvXxD9z
fxgoaPygqOjnOfQcMnKDM0z1Adye3+w348dDdA==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413474629202-
2026363248">
                        <ds:X509Data>
                            <ds:X509IssuerSerial>
                                <ds:X509IssuerName>C=ES, O=Telvent, OU=Telvent Global Services,
CN=AfirmaSubCA</ds:X509IssuerName>
                                <ds:X509SerialNumber>1611735152734479641</ds:X509SerialNumber>
                            </ds:X509IssuerSerial>
                        </ds:X509Data>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413474629202-1610461795">
        <dss:VerifyRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
            <dss:OptionalInputs>
                <dss:ClaimedIdentity>
                    <dss:idAplicacion>appPrueba</dss:idAplicacion>
```

```
            </dss:ClaimedIdentity>
        </dss:OptionalInputs>
        <dss:InputDocuments>
            <dss:Document>
                <dss:InlineXML>
                    <Document xmlns="http://4tic.com/foursign/signstore/definitions">
                        <Description>Documento </Description>
                        <ServerSignature>false</ServerSignature>
                        <Format>JXADES</Format>
                        <Issuer>Firma automatica</Issuer>
                        <SignatureType>
                            <Code>opensat</Code>
                        </SignatureType>
                        <ContentType>text/xml</ContentType>
                        <FileName>in-xades.xml</FileName>

<Data>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPFNpZ25lZERvYyBmb3JtYXQ9IkRJR0lET0MtWE1MIi
B2ZXJzaW9uPSIxLjMiIHhtbG5zPSJodHRwOi8vd3d3LnNrLmVlL0RpZ2lEb2MvdjEuMy4wIyI+CjxEYXRhRmlsZSB4bWxucz0iaH
R0cDovL3d3dy5zay5zaW5nbGVzdG9yZS5jb20vMCMiIENvbnRlbnRUeXBlPSJFTUJFRERFRF9CQVNFNjQiIEZpbGVuYW1lPSJ0b1
NpZ24xMjQwNjA0Mjk2NDUxNzU4MDU3LnhtbCIgSWQ9IkQwIiBNaW1lVHlwZT0idGV4dC94bWwiIFNpemU9IjM3MTIiPlBEOTRiV3
dnZG1WeWMybHZiajBpTVM0d0lpQmxibU52WkdsdVp6MGlWVlJHTFRnaVB6NE5DanhQY0dWdVUwRlVQanhGYkdWdFpXNTBQanhrYz
A1aGJXVStRVTVIUlV3Z1RGVkpVeUJLU1UxRlRrVmFJRTFCVWxSSlRrVmFQQzlrYzA1aGJXVStQSEpsYzNWc2RHRmtiMFpwYm1Gc1
Bqd3ZjbVZ6ZFd4MFlXUnZSbWx1WVd3K1BHRndaV3hzYVdSdk1sSmxjRDVOUVZKVVNVNUZXand2WVhCbGJHeHBaRzh5VW1Wd1BqeH
RaV1JwYjNORlkyOXViMjFwWTI5elBqd3ZiV1ZrYVc5elJXTnZibTl0YVdOdmN6NDhhVzFuVFdGcGJqNW9kSFJ3T2k4dmJHOWpZV3
hvYjNOME9qa3dNREF2YjNCbGJuTmhkQzkzWldJdmFXMWhaM1Z6TDJWelkzVmtiMTl5WlhCdmNuUXVaMmxtUEM5cGJXZE5ZV2x1UG
p4a1pXTnNTblZ5WVdSaFNuVjZaMkZrYjNNK1BDOWtaV05zU25WeVlXUmhTblY2WjJGa2IzTStQR1JsWTJ4S2RYSmhaR0ZCWTNSMV
lXeHBlbUZqYVc5dVBtOXVQQzlrWldOc1NuVnlZV1JoUVdOMGRXRnNhWHBoWTJsdmJqNDhkR2x3YjFSeVlXNXpjRzl5ZEdVK1BDOT
BhWEJ2VkhKaGJuTndiM0owWlQ0OFptRjRQamsyTkRVMU5qWTNOend2Wm1GNFBqeG1iM1J2WTI5d2FXRkVUa2xHYVhOcFkyRStQQz
ltYjNSdlkyOXdhV0ZFVGtsR2FYTnBZMkUrUEdsa1BqRTVNREE1TkRNMVJ6d3ZhV1ErUEhOQGJHVmpkR1ZrUVdOMGFXOXVQblJsY2
0xVGFXZHVaV1E4TDNObGJHVmpkR1ZrUVdOMGFXOXVQanh6YVdkdVVtOXNaVDQ4TDNOcFoyNVNiMnhsUGp4aGNHVnNiR2xrYnpFK1
BDOWhjR1ZzYkdsa2J6RStQRzUxYlVWNGNGSmxZV3crTUR3dmJuVnRSWGh3VW1WaGJENDhiblZ0Ulhod1BqQThMMjUxYlVWNGNENND
hkMjl5YTJac2IzYytiR2xqYVhSaFpHOXlaWE10TVM0MUxXeHBZMmwwWVdSdmNtVnpMVEV1TlNReE9Ud3ZkMjl5YTJac2IzYytQR1
J2WTNWV2FXVjNQand2Wkc5amRWWnBaWGMrUEdGamRHbDJhWFI1UG5OdmJHbGphWFIxWkR3dllXTjBhWFpwZEhrK1BHUnZZM1Z0Wl
c1MFFYUjBZV05vWldST1lXMWxQand2Wkc5amRXMWxiblJCZEhSaFkyaGxaRTVoYldVK1BHTnNZWE56UG1Oc1lYTnpJR052Ylm1bW
IzVnlkR2xqTG05d1pXNXpZWFF1YzNSeWRYUnpMbVp2Y20xekxuQnliMk5sYzI5ekxteHBZMmwwWVdSdmNtVnpMbE52YkdsamFYUj
FaRVp2Y20wOEwyTnNZWE56UGp4dWFXWlNaWEErTVRrd01EazBNelZIUEM5dWFXWlNaWEErUEdsa1RHOWpZV3hwWkdGa1BqUXdQQz
lwWkV4dlkyRnNhV1JoWkQ0OGNtVm5hWE4wY205UWNtOW1aWE5wYjI1aGJENDhMM0psWjJsemRISnZVSEp2Wm1WemFXOXVZV3crUE
dkeWFXUlFZWEowYVdOMWJHRnlYMjlrZEQ1WEkwVWpVaU5VUEM5bmNtbGtVR0Z5ZEdsamRXeGhjbDl2WkhRK1BHUnpWR1ZzWldZK1
BDOWtjMVJsYkdWbVBqeHBaRUYxZEc5c2FYRjFhV1JoWTJsdmJqNDhMMmxrUVhWMGIyeHBjWFZwWkdGamFXOXVQanhqWVhSbFoyOX
lhV0ZEYkdGemFXWnBZMkZqYVc5dVBsSThMMk5oZEdWbmIzSnBZVU5zWVhOcFptbGpZV05wYjI0K1BHUnZZM1ZhYVhBK2VXVnpQQz
lrYjJOMVdtbHdQanhwYm1admNtMWxUV2x6YVc5dVJHbHdiRzl0WVhScFkyRStQQzlwYm1admNtMWxUV2x6YVc5dVJHbHdiRzl0WV
hScFkyRStQSEJ2WkdWeVpYTStQQzl3YjJSbGNtVnpQanhwYlhCeVJHOWpkVDUwY25WbFBDOXBiWEJ5Ukc5amRUNDhibWxtUGpFNU
1EQTVORE0xUnp3dmJtbG1QanhrWlhOalZHbHdiMU52YkdsamFYUjFaRU52YldKdlBqd3ZaR1Z6WTFScGNHOVRiMnhwWTJsMGRXUk
RiMjFpYno0OFpITkZlSEJsWkdsbGJuUmxVbVZoYkQ0d1BDOWtjMFY0Y0dWa2FXVnVkR1ZTWldGc1BqeHRaV1JwYjNOVVpXTnVhV0
52Y3o0OEwyMWxaR2x2YzFSbFkyNXBZMjl6UGp4a2MwVjRjR1ZrYVdWdWRHVStNRHd2WkhORmVIQmxaR2xsYm5SbFBqeHlaV052Y2
1RK01YeGxiblJ5ZVh4emIyeHBZMmwwZFdROEwzSmxZMj15WkQ0OFozSnBaRkpsYzNCdmJuTmhZbXhsYzE5dlpIUStRVTVIUlV3Z1
RGVkpVeU5LU1UxRlRrVmFJMDFCVWxSSlRrVmFJekU1TURBNU5ETTFSend2WjNKcFpGSmxjM0J2Y2Ym5OaFlteGxjMTl2WkhRK1BIVn
liRTFoY0dFK1BDOTFjbXhOWVhCaFBqeGtjMFJoZVQ0OEwyUnpSR0Y1UGp4MGFYQnZSVzUwYVdSaFpENDhMM1JwY0c5RmJuUnBaR0
ZrUGp4bmNtbGtVbVZ6Y0c5dWMyRmliR1Z6UGx0N0ltNXZiV0p5WlZKbGNDSTZJSHNpWkdWell5STZJQ0pCVGtkRlRDQk1WVWxUSW
l3Z0luWmhiSFZsSWpvZ0lrRk9SMFZNSUV4VlNWTWlmU3dnSW1Gd1pXeHNhV1J2TVZKbGNDSTZJSHNpWkdWell5STZJQ0pLU1UxRl
RrVmFJaXdnSW5aaGJIVmxJam9nSWtwSlRVVk9SVm9pZlN3Z0ltRndaV3hzYVdSdk1sSmxjQ0k2SUhzaVpHVnpZeUk2SUNKTlFWSl
VTVTVGV2lJc0lDSjJZV3gxWlNJNklDSk5RVkpVU1U1RldpSjlMQ0FpYm1sbVVtVndJam9nZXlKa1pYTmpJam9nSWpFNU1EQTVORE
0xUnlJc0lDSjJZV3gxWlNJNklDSXhPVEF3T1RRek5VY2lmWDFkUEM5bmNtbGtVbVZ6Y0c5dWMyRmliR1Z6UGp4eVlYcHZibE52WT
JsaGJENDhMM0poZW05dVUyOWphV0ZzUGp4bmNtbGtVR0Z5ZEdsamRXeGhjajViZXlKbmNuVndiME5zWVhOcFptbGpZV05wYjI0aU
9pQjdJbVJsYzJNaU9pQWlWeUlzSUNKMllXeDFaU0k2SUNKWEluMHNJQ0p6ZFdKbmNuVndiME5zWVhOcFptbGpZV05wYjI0aU9pQj
dJbVJsYzJNaU9pQWlSU0lzSUNKMllXeDFaU0k2SUNKRkluMHNJQ0pqWVhSbFoyOXlhV0ZEYkdGemFXWnBZMkZqYVc5dUlqb2dleU
prWlhOaklqb2dJbElpTENBaWRtRnNkV1VpT2lBaVVpSjlMQ0FpZG1sblpXNWphV0ZEYkdGemFXWnBZMkZqYVc5dUlqb2dleUprWl
hOaklqb2dJbFFpTENBaWRtRnNkV1VpT2lBaVZDSjlmVjA4TDJkeWFXUlFZWEowYVdOMWJHRnlQanh1ZFcxRVpXTnlaWFJ2UGp3dm
JuVnRSR1ZqY21WMGJ6NDhaSE5aWldGeVBqd3ZaSE5aWldGeVBqeGtaV05zU25WeVlXUmhRMjl1ZEhKaGRHRnlQbTl1UEM5a1pXTn
NTblZ5WVdSaFEyOXVkSEpoZEdGeVBqeHlaWEJ5WlhObGJuUmhaRzgrU0RneU56TTBOamd5UEM5eVpYQnlaWE5sYm5SaFpHOCtQSF
JwY0c5VGIyeHBZMmwwZFdSRGIyMWliejVxZFhKcFpHbGpZVHd2ZEdsd2IxTnZiR2xqYVhSMVpFTnZiV0p2UGp4a1pYTmpjbWx3WT
JsdmJsSmxZMmxpYjFObGJHVmpZMmx2Ym1Ga2J6NDhMMlJsYzJOeWFYQmphVzl1VW1WamFXSnZVMlZzZWldOamFXOXVZV1J2UGp4MG
VYQmxVSEpwYm5SRWIyTjFiV1Z1ZEQ1cWRYSnBaR2xqWVR3dmRIbHdaVkJ5YVc1MFJHOWpkVzFsYm5RK1BHNXZiV0p5WlZKbGNENU
JUa2RGVENCTVZVbFRQQzl1YjIxaWNtVlNaWEErUEdGd1pXeHNhV1J2TWo0OEwyRndaV3hzYVdSdk1qNDhjM1ZpWjNKMWNHOURiR0
Z6YVdacFkyRmphVzl1UGtVOEwzTjFZbWR5ZFhCdlEyeGhjMmxtYVdOaFkybHZiajQ4YzJWeWRteGxkRmR5WVhCd1pYSStiM0puTG
1Gd1lXTm9aUzV6ZEhKMWRITXVZV04wYVc5dUxrRmpkR2x2YmxObGNuWnNaWFJYY21Gd2NHVnlRREZrWlRRMlptVThMM05sY25ac1
pYUlhjbUZ3Y0dWeVBqeGhZM0psMFlXTnBiMjVQWW5KaGN6NDhMMkZqY21Wa2FYUmhZMmx2Yms5aWNtRnpQangwWld4bFptOX
ViejQ1TmpReE1qTTBOVFk4TDNSbGJHVm1iMjV2UGp4bWFXeGxjMEYwZEdGamFHVmtQand2Wm1sc1pYTkJkSFJoWTJobFpENDhaR1
Z6WTFCeWIzWnBibU5wWVQ1RFFWTlVSVXhNVDA0OEwyUmxjMk5RY205MmFXNWphV0UrUEhObFlYSmphRVJ2WTNWdFpXNTBQand2Yz
JWaGNtTm9SRzlqZFcxbGJuUStQSEpsY0hKbGMyVnVkR0Z1ZEdVK1BDOXlaWEJ5WlhObGJuUmhiblJsUGp4a2MwMXZiblJvUGp3dl
pITk5iMjUwYUQ0OGRIbHdaVVJ2WTNWdFpXNTBQbkJrWmp3dmRIbHdaVVJ2WTNWdFpXNTBQanhqY0Q0eE1qRXdNRHd2WTNBK1BITn
BaMjVsWkVSdll6NDhMM05wWjI1bFpFUnZZejQ4Wm05MGIyTnZjR2xoUkU1SlVHOWtaWEkrUEM5bWIzUnZZMjl3YVdGRVRrbFFiMl
JsY2o0OFlXUnFkVzUwYjNNeFBqd3ZZV1JxZFc1MGIzTXhQanh6YjJ4MlpXNWphV0ZVWldOdWFXTmhQand2YzI5c2RtVnVZMmxoVk
dWamJtbGpZVDQ4ZEdsd2IwNXZkR2xtYVdOaFkybHZiajV1YjNScFptbGpZVHd2ZEdsd2IwNXZkR2xtYVdOaFkybHZiajQ4WVhCbG
```

```
JHeHBaRzh4VW1Wd1BrcEpUVVZPUlZvOEwyRndaV3hzYVdSdk1WSmxjRDQ4WkhORWFYSmxZM1JwYjI0K1BDOWtjMFJwY21WamRHbH
ZiajQ4WlhOamNtbDBkWEpoY3o0OEwyVnpZM0pwZEhWeVlYTStQR1psWTJoaFVtVmpiM0prUGpBeklGTmxjQ0F5TURFd01ERTBPak
V5T2pJeklFZE5WRHd2Wm1WamFHRlNaV052Y21RK1BHUnpURzlqWVd4cGRIaytQQzlrYzB4dlkyRnNhWFI1UGp4bVpXTm9ZVVJsWT
NKbGRHOCtQQzltWldOb1lVUmxZM0psZEc4K1BIUnBjRzlTY0dSdlBtcDFjbWxrYVdOaFBDOTBhWEJ2VW5Ca2J6NDhjMjlzZG1WdV
kybGhSV052Ym05dGFXTmhQand2YzI5c2RtVnVZMmxoUldOdmJtOXRhV05oUGp4dlltcGxkRzlUYjJOcFlXdytTVzVtYjNKdFlYUn
BZMkU4TDI5aWFtVjBiMU52WTJsaGJENDhibTl0WW5KbFBsQnlkV1ZpWVNBelBDOXViMjFpY21VK1BHbGtVSEp2ZG1sdVkybGhQak
V5UEM5cFpGQnliM1pwYm1OcFlUNDhaR1Z6WTB4dlkyRnNhV1JoWkQ1RFFWTlVSVXhNVDA0Z1JFVWdURUVnVUV4QlRrRXZRMEZUVk
VWTVRFOGdSRVVnVEVFZ1VFeEJUa0U4TDJSbGMyTk1iMk5oYkdsa1lXUStQR2R5ZFhCdlEyeGhjMmxtYVdOaFkybHZiajVYUEM5bm
NuVndiME5zWVhOcFptbGpZV05wYjI0K1BHUnpSR1ZqY21WMGJ6NDhMMlJ6UkdWamNtVjBiejQ4WlcxaGFXdytjMjk1WVc1blpXeE
FaMjFoYVd3dVkyOXRQQzlsYldGcGJENDhaR2x5WldOamFXOXVQbEpsWVd3Z2JqOGdNakk4TDJScGNtVmpZMmx2Ymo0OGRtbG5aVz
VqYVdGRGJHRnphV1pwWTJGamFXOXVQbFE4TDNacFoyVnVZMmxoUTJ4aGMybG1hV05oWTJsdmJqNDhhV1JwYjIxaFRtOTBhV1pwWT
JGamFXOXVQbVZ6UEM5cFpHbHZiV0ZPYjNScFptbGpZV05wYjI0K1BDOUZiR1Z0Wlc1MFBqd3ZUM0JsYmxOQlZENE5DZz09PC9EYX
RhRmlsZT4KPERhdGFGaWxlIHhtbG5zPSJodHRwOi8vd3d3LnNrLmVlL0RpZ2lEb2MvdjEuMy4wIyIgQ29udGVudFR5cGU9IkRFVE
FUQ0hFRCIgRGlnZXN0VHlwZT0ic2hhMSIgRGlnZXN0VmFsdWU9IkVjWE5hSTRwT0VzR2ttY01SdkxrYzNtcXpEOD0iIEZpbGVuYW
1lPSJPQ1RtcDQxMDQwMzk4MTczMDUyMTA4NTkub2R0IiBJZD0iRDEiIE1pbWVUeXBlPSJhcHBsaWNhdGlvbi92bmQub2FzaXMub3
BlbmRvY3VtZW50LnRleHQiIFNpemU9IjUxMjIxIj48L0RhdGFGaWxlPgoKPC9TaWduZWREb2M+</Data>
```


```
                            <Signer>
                                <SignerRole>
                                    <Code>Firma automatica</Code>
                                </SignerRole>
                                <Signer>Firma automatica</Signer>
                                <Order>10</Order>
                            </Signer>
                        </Document>
                    </dss:InlineXML>
                </dss:Document>
            </dss:InputDocuments>
            <dss:SignatureObject>
                <dss:Timestamp>
                    <ds:Signature Id="Id-ffb5decd-db54-4a61-8aa2-46eb208390f3">
                        <ds:SignedInfo Id="Id-7e025906-ca95-4ec0-94f4-7b346e86a2e8">
                            <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 Id="Id-f6c8dfe4-9d52-4793-967d-da908c249592">
                                <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>8OyCgfb+r+W3fwJvo9VQjC4Xxkw=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-d2b0d0a3-b559-4237-9e37-ece6d24da320"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-4e2f3bfe-9e3f-4e2e-
83f3-2ea880b3d016">
                                <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>bOSu9WnXmKk5a9+OniXMWvD7T98=</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>

<ds:SignatureValue>MUxt0Pl3PdtKcpI3+JdDR3zO/iOEdvikk6djhksk0H+u4lEu3p/brzuMvj1k3yOfWN9xIQat6/DUvpKvo
h3ulROAn0ilX4gMRmJJ0d5ajaoPXfaOA8eZlh9GW4aJW/GxR75A0ra/61k2NKSXDRTHKZh9pt0WTtQ2URABDVaXfTmz1xM3znHGl
axkTb/d81N6wMaJyA0d9HfB68JCYU2+0PZd38f8GA0UTlUrwdpj/2EubByeq1h33YE2Li19L0o9Qc3ymfWug7zbBSHMWe9YcAbF0
0c0G0rWX7zPB9qxkm7xD+5R/FbEgwj2brhV/qbhGFuaaVHo9+eYaEOTGJ3aAw==</ds:SignatureValue>
                        <ds:KeyInfo>
                            <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3Vi
Q0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEy
MDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAw
HgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebqz4t
4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh5
4cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jD
BMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwggHO
MIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlz
dC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZp
```

```
Y2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEGDAW
gBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAv
ZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVu
dCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4rvVH
7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE0
7uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfC
lWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/ivH
ByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3</ds:X509Certificate>
                            </ds:X509Data>
                        </ds:KeyInfo>
                        <ds:Object Id="TSTInfo-Id-4e2f3bfe-9e3f-4e2e-83f3-2ea880b3d016"
MimeType="application/xml">
                            <dss:TstInfo>
                                <dss:SerialNumber>1413465482403100098</dss:SerialNumber>
                                <dss:CreationTime>2014-10-16T17:50:28.990+02:00</dss:CreationTime>
                                <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                <dss:Ordered>true</dss:Ordered>
                                <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                            </dss:TstInfo>
                        </ds:Object>
                    </ds:Signature>
                </dss:Timestamp>
            </dss:SignatureObject>
        </dss:VerifyRequest>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: Sí (Token de Seguridad – X509IssuerSerial)

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14134746295051463196 5">
                <wsu:Created>2014-10-16T15:50:29.505Z</wsu:Created>
                <wsu:Expires>2014-10-16T15:55:29.505Z</wsu:Expires>
            </wsu:Timestamp>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1413474629505-
1376135510">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413474629507-373617289">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="SOAP-ENV dss"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>/mMMI+euufUIz9D/cbenETnwvRM=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-14134746295051463196 5">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsu wsse SOAP-ENV"/>
```

```
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <ds:DigestValue>Df732ktVYQSotuSKpONPG5285KI=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>

<ds:SignatureValue>MOBQwWijP4B/i0xLxmuRsMLxdrYXkH/sSdW8CzDnTsyEFxnHZJXLzc+V8aL7/Hj60PP32M7BS3t1CbgA2
WdRwUmJAycjPGQWYQAEUX3KJfXg9FaqM0XXquZPtzqTLNj3foUjY7ebTcfCnOI9HwRA91h5D8ZUr51P4AVDWg7ExsDAVsbsvSeKV
cZSHp8VItpdDdtZUVGgHpC5Uie9de7Qdf4yWc7G9Q4CMwAqXWYQDIZSafGw1XikTrOH7l9H0Mv8uFL+FrpGxsWpUsRYb3TOeZxiw
mv0DlXKOOmwYKs1PVq/J4Vw9PgNWf2oOtTSTOtCbqNrb/j1jSTcKEa2ybij1Q==</ds:SignatureValue>
            <ds:KeyInfo>
                <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-
14134746295061287387206">
                    <ds:X509Data>
                        <ds:X509IssuerSerial>
                            <ds:X509IssuerName>CN=AfirmaSubCA,OU=Telvent Global
Services,O=Telvent,C=ES</ds:X509IssuerName>
                            <ds:X509SerialNumber>1611735152734479641</ds:X509SerialNumber>
                        </ds:X509IssuerSerial>
                    </ds:X509Data>
                </wsse:SecurityTokenReference>
            </ds:KeyInfo>
        </ds:Signature>
    </wsse:Security>
</SOAP-ENV:Header>
<SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-14134746295O7-373617289">
    <dss:VerifyResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-f8e9ae65-9d13-49e7-a224-
686b323dde68">
        <dss:Result>
            <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
        </dss:Result>
    </dss:VerifyResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Ejemplo 6. Solicitud de Validación de Sello de Tiempo ASN.1

Petición:

- Securización de la Cabecera SOAP: Certificado (Método de Inclusión del Certificado – Key Identifier)
- InputDocument: DocumentHash (Sin Transformadas)
- Petición Encriptada con Clave Simétrica: Sí

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413526402293-1099570243">
                <wsu:Created>2014-10-17T06:13:22.292Z</wsu:Created>
                <wsu:Expires>2014-10-17T06:18:22.292Z</wsu:Expires>
            </wsu:Timestamp>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1413526402284-
1068388888">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413526402293-1522541787">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>QyAjW7rvFylFRa6SEly+wGNfIfc=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-1413526402293-1099570243">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>Ehbahpis8An+fZBujUMfXGbfvlg=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>aGjw93eOcd1WQCqdDcDXj4+AUeOu5g4waj/a0XVv7xnx0zKTmYuC11Cp59FpK+bBsMoOXMJMWD6N
KOmIOv+L2/3hv2l2i08uek5VS1idXF1GmrIRU6u1cLcUci/AZb6874hcnis8YlVD0XDxLugZZlax
QzWPMAy2T3ioemmf4cbCCgsBb50FHfE+yVjeNrXnKIJ6+Ss0y3QAcoDiYv//bbFrZvgCEgv4VxKz
5hR5XOGgDYxTjs5SOtCq/Wv2exxQB0EbPrH2fDqTp825xK+ySFEgVRrzO7038haSRBus33rAe5RT
To7gGtlUnLbq6Ag+Ug6fHt0MNU5DbxttiX8dxA==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-
1413526402292192195328470">
                        <wsse:KeyIdentifier 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#X509SubjectKeyIdentifier">Ahg6E1lYWBp+eACCz21Dvh7bJ5g=</wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
            <xenc:ReferenceList xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
                <xenc:DataReference URI="#XWSSGID-1413526402292-251464275"/>
            </xenc:ReferenceList>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413526402293-1522541787">
        <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="XWSSGID-
1413526402292-251464275" Type="http://www.w3.org/2001/04/xmlenc#Content">
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:KeyName>symmetric_key_test</ds:KeyName>
            </ds:KeyInfo>
```

```
            <xenc:CipherData>

<xenc:CipherValue>AQjqEQoliLphijK51paAzl3tMZGu29g8K1yffWSgqxxQhPx1xwzPwFUcPFO8dk7p/uD9J664aIIV
UodLRrpbAw4E4FRskMBQxeOOUO03dRiXUF1JgbDr9cgF9eTHmmkJ/hwufWhHx3wlavTBFPCWz8i4
p8hSXIepKoiBTcqEYCZGbwyz/wbaSsHK4pbW571FTlrVt27qiPQXlCwpnir+57ov/hMGc33gg/Up
Et0ndrUQTPCZAoGHVjo9pO1PfliyMRNOKAAvS7jDGDAYp703IyAgGHF8iEAOynF+SUmJ/vjd7eMc
dvyW813SZWo92MxMOfkPV5SYEtrz/o1TtCExFAUkQVkWqL9pBRzJkX5elkoilH9+3Y3H4qNs8LCL
H7yGm7UUPuGKeFAZ9+DwmteODgn0KM0fqr92KQ2L+UmUTb1RQrTFRWOSW6B/2G9eCvq1QQ8TbRoY
gn6NnImRVoRVHOSIPp4r+UHK3PzhmQZF6a2GZpWKOPsFCrLacc9n6hisndfaDA3R/xaublEjdtz2
mQGbOv0G1QQHWn6dmyhGS/DSVsz//+nwCSRZiwzcZXK36Zg8b5ZuJx8S5vgAB9uxP0tHeq9lr8u8
bfgfSQFjUsNn9k9SZ3EH5sC879UnpUuS4/KS2XYFqELMeIgTyET5n5OAs83FYkb4s/sMMRaDOyo7
+AmDh7OOjArN4yNULjrY3hIG29hxKcAt4pD4pi8oEKn746/Kq3rY2D6o5Cg+PtJH1upaJ+KAFf38
71EvWwhhwRxIFQ6uKpYCNEy9/xHYxPIKf0Ajh0FEU878sABp8NoMh+HBhe+6QvbRwuUQf3RVU6Ss
SbtiO6znl8Aj6MHff8A1SkOOZiZOPZUPBU3lDZbD606llZjBgMZVklKQfb/1Berwtyjq1UKR+fN4
X3UxTS/CzhVmxnKEY9F7fuMt4+AfLn0JM/GSDNnEStYKyotry/1auumsdxCqKTE2oYiOOPdESsg7
kLZyHrEKLWkGrsk0Z7z9kDFjhhljTNmrBFn1al0GBvXpLqLjDnrYFgQYLBQ+4xQdbTJHuFf4HSx4
OZDAVpjp+RMG33w7Z/BXiIebGIZNxmT2pjYXsHEk8bTszG+AS2KN05Rk3zyBkDbVbRxgM9Mw4G65
zpQsKH60DqwDJ6FycAR3+rOu1tGaiau+uTvXGcN0BbXyP+5yH4Tt808Cka819oIqLgdiSSL4Mmk0
mdigrp1enmfoV84W08UurmEp6u2GPEHnKtrtLFnHX4iN9w8hK/V8/kIyeTp54jl+taT2iidBsn3Z
OdLXmwnya5lN8DYdZlVw/0R5RYXk4iGOmwGAiGuhBOs9HH7sl0q+oDYdrd91BxYMHFpYb1s5ojXp
6ju86FOeGg1nkBUg41zO3uToQIlTxoTLbqNrq301OOtst3zJsQg+YsDqH4LUOMyQ0cHwFM2swgfB
70BcrlnENvbJMWdH/+FLojXqp1JERaqmAaO+6JTWNq7otky684XLjTLmpQgKVjoaMK40rWgSd2AR
Jjfho7RXgxAhNKDmhdkKBHuqA4fbc6EKaJEaHwknDEwoSZcE5wDYRqzTpjXAlF8UsTGt5Ngw1SFp
3WoryWF70JnynvG/L2Ml1ub+9V8qRtCYFz4Ur2TpiqTy6xAVi782S5VXRyxnUR9xITsb7jDt3haS
/jCvgvRvxZ1EnW7YwsJm12+g+76PvTtWmVVZe4/OUlFkRiL9JO4IfXShj4YtUq6be7Zh/4GdjKMr
VreXjlLoEiPqPJ8LVb7r4a6UUgpboVnh/dAyjoNmM9XSq8NqlwYswNCYOS0UVU0yutqAA+iEX0RZ
1kKJrk37Mj2oL0fXeoZWMLcxQeBwpOsWXMvKQLa1wEpNHGpxSzyT8nuOpbBFrdcZDKPQISVF9bTh
fMlZgUBJ30awf/5riuDhr7TmyvqCJC4yZtPqX1+bj+oWx/h0Bqe6776n+dCtSVu29EEFDHK0X1e7
uONmLc8mP0DipukqrWlh8oxai+dkxg1JYHrSbkEvWvdyocWO4yG95reMogiC1RbBSy/TOqttOTY0
CbRsVG34+CxiIiuQrq9Wzvs9UmPzVHCY0Gb3qmV5SuuYngxmsl/fq5sVwuAo/CmJh8ReDnMrnJyN
sNPqHH/ie/4HLlafaJ+L/4hbL7pE4lBsUljD+TgDvrrkLhnwRid/uvEoo0n3zOB5Y20OD7EV8TtD
lB9ZeAdHTR/O1AchDNYmRf/hKbZJKeRd6NDSVU+jM6Rc5UGKzB5sSoHDtjCHgigzClPFMVBnSQ0g
LOoR2G4wERUydD1Dh2FMDYplX3EsY4F9sRbwrITwTlw7A7jLr7R/8SLgtEsabndpfl8OSxdybEaS
Jv28aYPXUzIi5pjcsfnX8pg0e33xKoXPHfYLK8iRI6pI/rCXu4qCas9CL+iZsaZenFOuCADoD7rs
7nAUm7OgJO7Olg/mm+y4rO8mVATUTSGQsBjE7hd7yzbcOhcjgpjBhYkmKrOF7a4kXD01Q6VF0ML7
U6pZMsc3b+i/r14jcSI22tJejlLGbkPOy2RbuB3+xrt+tGbpVz3hp8xJDzS416EwCuAI08b7argA
Xlv1Gjsp+FXiMuGmRgiT2y6V43RfcqLdfpIsVCOqyBYxCKyPGbpZzXuVdhG1cxSo7Zae+mVj2fRb
HK4bOGbbK5JfQsA2eoALSs0tPWyrW+th2F7jacncURxNyVvkCi0M6Z6Y8W7eTbz53FDMw9LAMwxS
ghAsAIZDsF3F+MXFJTyxW2+5gwI1wgSfTNoRvfDIbzS/lBVgIq1BGNymqWWRP2mL3Isnyirlcih X
wkgA282swx3eSyiUSFCa6ORoqkrEtKcWRGTsOSyk0Lq+qD/L0JYTS8SA0EliuOFoWufXUkxTNbAX
uUxLcaeaGjGFDXK0eet9eqyZZsibdE6lIm9vkG2LRGZ1FL7L4XX9US+KqwU3ZyixWidggB5ry+AQ
qZRtIu4aRe0oslp6e1lUFzZ1U2cB/Hit2RUhLAbOTcRl2SLONqjH5+Fy0ZoLnAQcmVJDf8duOndG
A5IM0bC/B5RL//sjwe+C+CJ2bwU19vsbaQlAXHkK964MEheZyBH/v98EUIwuPY/JhGzBQeB+CUYA
2sRy/FuqDa8SlMTcPCc8/yehVh7cV1fwOwnumj60et0toaxNF4CNp3WPsJve6Hs7fsdRnnKY/b4u
1rS5wWDvlZUSWhzAu2rNmCutwQAQJVwubhYpaa1PeTZ2zUH6mAJ39hPYgOGPFaGRjIyQX1vQPqMy
rFsaSX92vQOuhPDqpWXChJJlJ3gMZ7xQLM9Yf3B4PoQ6n1aqPiAL0bX/dp9nXZxJNJQtN1LC4iX7
VBOhOFTG9s+xv3KbK2jj5fBE/JDRhzQW/y2qgoCzSXLCaPKxkG+oD2XC5b6WhkAh4Z85KVJm9/v7
pjnR2AHJDWNb/674cqOKGEq1RIe1kJqSNqIFdvps5r1gR5jviH1u8W2J5vvNTiVVUPNc7NHhODRe
9rz4eWArT4aSCndFkGsd1g5LYAqlN3Ejjnph6RKIG465boeBBtzLcTT3ascBo3anmEBN6foVdkQB
i+vBj9HlwIFk9bK6cVdKQRhSQPWXG5lAD+nZQC5ahLMTAy59Q0q34aBhDfcKJRgMzu7LBe9O5Eu+
+7sJL2eSOy5VqKjaJSMEIgIx1ObJj0PAutpKjJ6g0Gmi4sepAs2afXS2vx5BlaVV2B/ovcfMTH0s
kGBUI8Ycx+q1IhId0aNoeDgNdCwtKzPqaFGHIOCUiv049hRL3oBwb9j00gM0nPTn3sRXs4Y4bB6N
khW5urb+y/GGXwsfUcXG6L3nunpzymCHysH3qyTVyoshdnJWWE/0wou+CthFdDEWXqDaz9L8BC7c
0a/12i+9I03qKjOR96RDaHC1gV+2mFKFjQ6HeodlLYYSjJ4MQ+1mu/KBEtLxJeHULW1kwArH5NkP
xm+lNQQCIFheDFy60GK/5ggKFtObQEv9GwuS8AvrPHQIFDxzX/WKhwOG4puUU5aPhEUAZ+B/F/Kp
Znb2md/pQFMM2OQj2LL0FwfpzdILkyLDdRNH8l+QDdvjhtn15AaqVKCcJGO0ZDXauvceyT+nSfCK
Bf36LCW8Regs6RHi4YKPUQiS/3HrHH5XfKlxOPn/+HvCgCSYl7QTk7nhtiZD2uEXHNOPyiwYxFpY
gtse6qBe93MhinJoHQvNah8gmo9/Sv5RtypdTtEleHhrThgTfoqXhSjsk2vvzGfzVKTF48yErGsQ
2zPuPRIQA1z7m9nedxO6r17/Du7Vz/MutKsMhytUXx8Mwypp8KdYQOm28AQVS7WxylKTU/D85Gk6
mHJJGp8ZjhFT65qzLFooXoJe/ISUG87EUnj93VYLL9X4Di0OjOOziOdxyDdfNNkcm8yv7HHc9EJh
yvxMHqdoc/FLEC76Qug4FQRytvSvQRzq9dKmielnJwR80J33LQH5ilkGI4a/6Mnno7oSP+c4JOp6
8a+Sduhr6j/UVuzJPg6/v+FlNWu/8I9GewJ4McpVTMSEmX6QQRtP3CCTRUC31ZBBtfsVXNw3MKA0
R+wik3fYJTHc9HN6+8wAvd8jb1kVvFJ9O3Ybt3oe17E8750gvgmrgd4nyGzEAzr9dzbfGqhn+Tzh
rM4vh5+u0kl4GcPNvUV+I4IsjyzGrwgTo1d9p9nTPxJhDrtjmrUL5Sz0xrM9wiFx+Sd7U/UdHyEm
6QKpy9PyRk54kTUm/wXsJJdFONPkRIwFQuJIV3JmzPsJnLJtls4Qu6clB+Ka0rajSEIGC+/JuoJn
aVT++MVvTY5lzlZE5aR0ci6n7VHTL5NEnRWyAQusxpFwS+lI+10WHjX0HkW84/zdNTNNp1HskDkn
k1LU+b/ng6T3l183yxoD6Z1BdplTlaf1afVVuz0oPKE33cGnMpNXAFHit7c+f4LlIONjCPsxnkkb
mVO+tJgVUrCTfAAXYbyTnF3IBx1gKKVgLZtbIQTEEHAu5oOT/uDYVq8Jh0SWmGYT27HdhrKZuP5P
5OMCG/wOvV4a4eNhn5AphTtFQKndrSFANsojpT6+Vqv2fJGWQCmh8b8M/f31MVwLN+E+xLk+eqKf
axBtgBqnAmX/kF4L9AABhGX5By1RfNwyY5L+xNgybxFr8aybRCAlIAFFFDZrVQP8442NqEy8IBQE
nwPyHgOKgkG2w7YdhHYQkmPCHgSAC7VxL3VqdU59GU4Gqw5yNFsi+qBfIGOyUuxSiJmWxnQ3TNx7
Cg51Gwyq58GNNVBUcn04fOEgWJ17zln521W2scjxQjw50zard8VDGRuojyJ0Q5/rWJjlthrrZ66l
VRQ5PssvTbrqNTTFiiL8hIdyu/9veVZISA9KprMAGv9s9ksa5yBu3Htc7djuCF/culAU2BT4iGGQ
j+4JMrc8+R7+kmxOkwWP0WC8d/0dkE5bu5KjHiw2iLIUumgAPHDR9z96zuh1LSzDIzIKJj/WLW54
```

```
9jtX0rzES8/nGoUVhgpyYNMnkiqoAysUURAw9zm1JOVJctfWnsXHbokOkyI2a/ehBH3gDKazPe1m
AsR3HLjmHGqm4qnxmqxQ3VkW94FCN3YTrkk+tB1NELMFQybLKnl7MeVPTGqXojC5LMEeokGZpXS/
GaYiSIVVP8YrN5m11qF+aseXO76puk3IYTtOn/pYrwuuvUEtYql7JNRPuA+4/IHx1tQtDouebsX5
bIm2meD4YdLBSk+YNCIAAFZIn8kfccvezAN6/r5/Uu2b8Yx5gY4TqycALggZosCHA5fKpnirTCC3
9QUXpEdPBeOeYqrDcHAOIVXnEXbaPWlr0lgCG3upxfdkoxj5ohbzI8RhNNwjjGbLTAkPT3efXKST
3I/w2j480J+9LPUJMIwkVElrmfy7BwZ72e63F/3FB9eWjFusPgicDr+Ngjfkpjc6UeU8CNxidp0l
4AZF1Hedf7hbIoSxorIcB5Z5HXCtSMOMu8u+iNZYksXz11gfO0PlIh9GLfwtLfIfrV4iUBDfSeU0
NZF33ifdPZWJUySIZaTOHQskQL3i8YzWUy42DSpcTOj9kUiDOGf1W7KxfsLebSLa0OK1zntmHt/B
ZJHrwH0EDWehbaQKickEDV5eZveiOMqaQ9pk0wR9GExa0EbX8VS8o9T+IOgADSEIan5+4MrcuB1M
vY6LQOU+OJUME1/BTWpbwKdmNsgq0nHGuWLKofW9HhdX9bWbvsYbuV/DIWrjJwBVP1L+mtCKTYGP
40+bdG5epcdkUVjzTD2IRI6ETQJpdj0BrzmrxWp4oicyeRvErVevbixsDuAr9kuylWnrqE596KC0
WkJB9dRrAbLmj+IN+qFxByW32UvCbGaj952s3ZWxCQCz09pd67kdDLxTIWQE9XteOl/Yiw8bjrVz
yE40AP9SpFlI3yTAEUUQ3wufU6TqC5cZQ3ytN3BWkbxkcIA5WoIHIGtfa1ZDummsXwhSMv8JMkpp
7sY6B5mu6ExqwEIFYoufE23wlRuZw2vWtrxsd/A0r3qQ2XvCJxDHPbTyhBj/8gk60aQjBeHztr7X
GQ+mn8e8aSY8lLxxpKjnChOm6BiIIuzndWRUiTe2pUg1YR7Jjm5Ze6ro8y/a5ULWNpM53hoF2IMF
FSMGP5/yGlEsw3uud9eAl9++RoGntvbs393nK62LGV5kQd/ltc84CYHkCaimPVA3g6v2Wm8Eh1ja
4j15iZqL6JdDwdPmr79FVXPwNsdxFcGFRW9/RquU3AiAH3Ef2tI9zEeOuHq97Cl9VwXmkCp33+9n
DLDqGFXQnzc7z/BX7Lpi3t0gzfkrmz0MdO+a7AI7f570drpyRAY4f/Mfu+rbILqzZ3AFaE2RQkh2
gxVZRpPAMKvt5fTvGkly7P2GQPBHSFydWi0g1/usvzRDXoDaYQHbxepFNezWeUEFGO6w0ovIzt0z
bZYBcNmvgTcJZHLcZjGY5Me7Zv8Tv7GunUu6Yy6siGWmWkl+Bi6G9IpNfsgcUT2kPwCQIrVTB5yw
k0Xco0c2KbFoHPP+Jk9SU6MhzeSUL6Bp7x3gvRenK2GyRonEIrDPa7lKUBHPWYTl0qwsCudI9v3X
EWt0/K97nlqpvKg4PF8fUII7qTn6FumE1iRqTL9eH3w/IB8rTsXf23YHlZ0NsUDH+4iEFPjMri62
RWX//zC9BaIo4w0OLDKbD2IC5Ccrh3sM98EidO54v+qSaCwUjN5lyE4xB34b1kzIGpQv/VED7T4S
eNEZ6/lJkjEpFKNJMmjf2SDJav7r13f7yH2Nlwo4yNE7Rw5rRbl+PfvGKB+yNKuD6HyPpzbgggjh
KirV7Vgirl4q1qm0SW8ettZGjPsckVPbGlf8UuWJW+bBQWf6AvQSIgKg0CK8tGQeziBp22OMLZEk
HEMOv5BRMpyfez6HlPR9fJN88EOyj+qmfZ8Y32WpZEmRsQa/RyT0C9PHIB15cOYQk9WgTm7XOU+K
lspZfODNVFsgHh16IILk7JNN6tkVyLm4upYqtqHmMaU7KZjwc6NuarIZ73Ovhz8VZfQ+WPc8RlBM
ypMgP9cuPY5aes+RLXY0QXhm3Gl7fxc4fxplE7paJJtZtKNflAADkwvt3phQB7LyGlftZSeeQVVl
rBLqJD8j4sqdW63j8I0BoAPSn5kTLwm7eEHh4+8AOb8tWF/+6Pxo8kuPET1VOV4rxK+NW14u2WFh
g75gm7H65RDh5YpQEsQ5E1PcPA9vGvnpNTM1/RiVUr84SFxzTDKV2SXpY/qBWAEfDkomK1WEQgHt
2OmBrz8ROUCjnJ+YUPGJ8KWB5xXfd2KMSqARUpXDa533VPObBVio3/1bwT8Y0ixRCKQaEXfct3h9
If8L4KXDJ6MQHReKUvBEaDVTflgyZe/QDdQRrE/5x3VHvELYE1XeKmKpNJCjDZlYG9FOPlAj4O9Y
VsUhgbGvtHd7oIEFnXEEnUCqEBQrjZ7roCJLDOY1mu6z3KiKn2L77MBv+kmiJkSb2tkXNTZNGTwu
kF42ZY0IR3Wutpfpx2v5HvLmd8VlLDG2nXeOOJm0ftAirPA2O4TgCSoixWlv1/7/Rs2VlSEt7fj3
Rq0X7lVKNH17feIRQ+YKxD3oF6Ny+Dlz+0WzamEbWpt9mi7mVFwlkMVummOlqecHLVJFaxu+6vlD
rSxr6UgsgkzvY1CBWtR6hfCWcrLHwMNjJ7AL16BeWupnpxnrvPXaMmqZueYytg0e9KGaWuVZ+ORU
uINBfYutLMgaavzezt1Ldgwj42gQc54NDRJygwl/BFVIBYIj8PyURHe+lJK4BvKpKG3QlVWwoL9D
JHZ4TyxBbDwstIVbhcV31yLd4k1gVvtAtCWUqRGwH3/ybzeb9P7EJLFGxWQIFHnv3LOHBFRxZFFT
RpMUJeU/0GyTxEigNU2kDsKbtzXI6RBg+XDz+cibwkn0JxbUgsDlN2eO/S8AtRawPg8eExbUSYo3
ncG64fyLKNpQutF8YJNDRojZUy4U3qsz89NKMqc/+mLQ0aY6aRddeLkWkr2Z+TnyQboM++POnsry
5ue4XJk2ckGRtuqUDHdYw3PQp0esd62HLf8yJsvrBkGvMe4VVLWjesMp6gq38H0BdB723igXPNF9
Xkk12o0ou3C68OUbE0MT8z9DrrXfjRoiJHTdAbj7m1aiyh/xail08fkPhfWD55DeY2I+0vFsaimg
aeNrNztN/RS5NR7raCxtj15VqsaPeSmJ+JdJr0WSIyF4FHkLG9T2AmmNxG6yxverfBDV+12xd3aR
fVtsmDDf7oKp+tqIu4p6IJ3BoZ7ZR1IZrVJTQexee0zVlNW4QaimS9cXMHRpfPrCh+JuIGnsIIln
Vbz8LeNCZUP/CGIwBzqL6Y4juxZl6OImBc8Ugg6UnTD30VrjdIxBNAFnAYhSfHp+tjYmk2GG6VP9
4K6hhNQ4Yf2a0JJnRpW6xYS5V8iQqAeL14b6s0D3L0rn8dp4rVl0KtwSAtS4tInrlPifebtYyv9s
Qd5Z0jIsmFe9MwwrfKT1erMkztd+o0ZSwJyACs5PGk21Wp9E63FxdzsfeZSTbM6BU2BqCU4h9W7V
ytHbQkAIwJBHIhwF1mQzap3Ffd+acgjoHUn8nOZjTYJiKmSL9Smfw5xSe4ypnruSu/Z0sQRTOZTN
G0CAL40pNluPjA+NQeisG83bmr+qREB5IdPz8D/1XTEdwWc23Zcmmr07L9RSUUFfz21s8V4IklvU
eF9GVmT6B1LJkQieGbIJPFjOew2zpPYVsfAOiocOKrdLhLsI7fUHYdbYvBSFsE6bvm/SkMCBzxpc
XdD4gZeE/JnNJ/tfotjhUFS1Q3etNJDTs+SD0hxp2ZuW4LzsE87+BvixyXVvA7tvuuPnJOjisWdq
DlEEzyc+bpZLMJHl9egzpGP4lT1FPzn4jROfU6FHQw4FgIs7ZYWdZN2OgUYjepLVh8Y6540/FIbg
A19zZ8zS7bCT/lqX/W7DyGuoXhIjq6Pa4mx+IEWmpIsf6lPRvJkidEUJds9VQJLtzyi0H15f0tHv
0aOjcMPyv/AUQ0ATol9coHXexc49E7WiOu18CSE9sheXgXTh8xsYm/uaXlqdy3Xy8cITSXt2CGyx
k81IuXsyE0rxRZzm/3CzRGFPQvtT/xCTSpGT2DF9QW2Vboor08G2q3V/0Ixu9wq1vCZ8mDxRmvTd
JEx2A5orRpKGGAQA+L1xCxzMe5LiVE6/TWVbtENGK5mUXM638VLmE9r9W6dKtUyE+NLS2nIPsb/X
il17AMKRAcjQvfTaAWY1/eF90r4OJApLac3UnSGqb02i6S2ZGM2LoehzFP62C4x3rWqXan42kGhR
kKze3FngvX9go8hebyJZiVMtVb5chLAf+z0a87tEgynZt6a9Ze1GIjQg9SmxXnLKAwtR1cN9XBwp
zZZUBQXNZnRzl/zeprvFvKb+GVNeYXFQrhBSYcO0xn8HfzUkGdSEFg/MTYJh2U1hAY24cpiuYz/C
WV1trEAIOriB5KiSyLN+TGywKMyJxeuWQNtLOXmVumI7r9bFD3lf9S+PmVC9PwxNrkhcYxObCWq+
X3PJ2W6a59Rumv4t0gkokuz+RldEIf8VBWIZv8q3t8kXAYTYb7zqHbOZ8USC4xUs/VmP/h9Q6eUD
Lt8pc3q3gX9a8CW7emfPg5jR6r1Vq+Ycw6on78Hs1OztNs7IleECYS2LbSpc4zcGbe2sioHyB7Ya
ZkV2xsD2UUw4ixUeJaGhn1DDIHXp+6bCTyC7viGh5MItgla7Ar8eF1gFkFSSA3hwH4oAy7mvK9bD
4jdnZiofV9/huh7aUjE5/epcXbtcw/r1QQkgOQ1dx24syrhtS11oMj058CrCR+O1s47z9ZjXVTOb
IfNQqWoa71YsStGJV8D32J9vJrGacgy/M+oe3RK4uW6krj5xJC/XOcJiB5QvFfWyTq/1ZlojQLHf
B85PWTkN5C+a5iWRMss2mFz1+afbcFLVl3nF+nJQmnSPuazYm4KgQpzhP+hPCtS8Ad1hKpR13hIf
6etNnOW37Nvk/8v8Gz+kugf0s4cks44u+CM4WJ1YyYBqaDaggvMXn7QJSMccaX6dv1s1M71+ebL4
apDl7z2FZM+sECASHt6J2xZ/4HHhyLj+EfEPMB8fyZUfxN1OzfJHzyNRBjOxrurG384lZe7AXdiX
S9RerP/WqakV/9tCqdt4x6Ouf9OfwYuHCjiqOTZFDaDZ9R3FmSMb++SK7zI6NMl3CkZDEeCW0NBs
HpRrkhQpca3igUaX1ADESHE0432wNHE+MQziuS94K49CDWzBJrrWxf/5xVjwqmBkulSg2limIyUK
+WscbSHszax/2uxWxMEUrq8vlEYQsyUyAnPg07Umh/U3xDuBjHkgE8BMdeLyX4wCLWz1bUf4OQ94
mn9o7Lx+EHlw3hBSqBtzjWV3yjBm9Ml8QrG3FFTsdsgRbsY7jrUoSgIb7f9Zh9Usi4NhGoBy6D7V
cRj/tlLd16ScUBiWT5L4RqAYXAPSRiyLpoAlBmBj7xe9hHRmeXetuEzbAIHD3FFzEdlnzqaAaAi/
xgaMrHyVdJlUBBgnL4uu0nZDIwUfydzDu10E8hhH4dGx9bcIg+QFnaAEnmavgfU3SQqMM5UeQ84F
```

```
ow6mzNhHKu4ESWhIcR/Yq2SKXh5KWu3zBWvgxOjv8VaClAMnhGpEiWVyeuQoCWqYpqeehDOy7UVp
c6GSIuWnMZnWUWv8SS7hQOKOMJB68JIs0HyKswhzqFLYa3+Hdvpges+K2Lc5F7ZVPxJjwq57LaAV
zjySuMikZ47vOrBudcZzE2sKDwg5EYqfEwqVCo1kN0QgOE8b59YOvPnyA0nEPDr8v5wwmZpvDsHo
UfzIAESrjFhXUEg/gIfSNY0huTYCbN4gGu/4Q6beNeJJRpUY4dSeDjVPXjK3vhwA08JekPMWNNCs
FWgIIsAMValS1Ir3JrTmcJQl4PGhxD3WqYDFbA84BOsiE7Ud5wK4acVC7hMq5/IZbS88tm9FTZvh
LYKKkBaMNHOdBrhAzZndYQ2misRV3EQzCeWyOJLfSYnb4WVd1fJGI9OXBb2V2fg6DTxmfpQmNAFx
tmfccgiDhjvpY7gtopxNuBN9KYp516RRNy4PKly9fKQIHjMK6o4SxZ8xXpDj5KcsNGvPEEsbxfs/
NX4E1a2gXi+WYExcBu+BAPDkGDs818jHUZJXiTDaJ/GiDiyVwKW5djSeTSQg8peEhWFCvQmsIS2+
sxRg0N+2GKCAevO3YbkKx0Aosr6g7Ek9VeenDpYFxXuPbzzZSaioWjSmCJBcc4n7F1fCfv2/JInF
php3aWLZ7/gwUacAl9v9TJm8dtm0/w5o6o+9DVgR7tqNUc3z1inzw0jazowWIXGs8yqkO01xM1ns
UgivSyddur3L4xkg0Aoe8gvfaqjw4foIZY1kAPDz3CDuuxmIXR9GrvrQjGPyoS9c69n42+ShpP7W
mOk08yMl9xQgTb9UVZbDX8B0Y/LyWJxzi7wnoVjNdGZ8ybv2FPMVfdrtgdKtsUoiC2zBMP8qyLKT
vFOy9vZnlXCfX/IQvzbofaPL+FQ4/F29h3gVuM2v9iMBSiwbQ2tuw8sBhu54D9za0GH17ZaEiYSN
l/R362SOAAp9PjioeTE7KT/BcjmVUj4pgfG1oFbhDyjTde0s7+Dqf7e21wYpyB4E4EDVQrMwtDOH
u0GXB3OZBoDwCRlp7PAespIfRsuEhD+GYvGuOE9QsRbrc8p0NrpT5PRIqj0Tvk2H1/Uc6xOK9Agc
venOUlje3pMwt28h8Rmx/7wcpw3TJgVkesJlyGrS3fuvecIGp6cUt88mHFTtCZNoBalsLwBVxweb
KCHmKV0U/b8YyloncEfK+fKLGi8svrTLf3+YWwLQ4RWjHn5nxYjFmOHdKQq5UU+lUnXk5LS2BxLa
8NMIk+HCc3Ht8faddcmm72tOTZweYqQG12E1CFBqi85Nas2TVz8J0SFGmZCWQn6WWQtXZCkNEbKT
8wNlYtPRdAoeC+wRYwJYpBc/lHp9Z9AQRLQ1Gbg8WYn4DnFI8ZMHmOpdPrpLZiH0WBCTpEmiBIxy
OcGZ932K+IIxPhJJa15gczJsE3cvSROq+CELGwRvKsuSbg7C+kSBa2a3SQFUHSFbIM9vRAxK9/3q
T4rvKRrxRZWfL9zUF/94FOA13yKHe1ffDYkKp18qFn35Beiw3VEDhz+TtPoTxA7CyxXLlSJoLCAg
UVoJsp5yaRjPr/MvhifoaozlTPamIFZoyVTRJpaecht7o9hNGFesesaVXLWjd5Pg4lQvzhoCjQ7A
S3uCX0ndG6Oich0TIoNgYt3yb2ffXGGkl99rUB+O4I5QWiIOy0xKGOP46ZGflQE4V6Z55AfK4mzn
lWHDkaDoKZ0feAGrBKnEgMZKpfvR6rnqU3e3Q+YDCRO9JdsLtWpDLDeEr6PITiXIB6P9jJ9yfgw9
6rHSOr1UCl+UaWG7Qcszr/AOo5Nvr2AYG2RMqYIkHuFhaFbRSCBjgaSZCj0Xi0ZTS6ubxPrKeWni
dfT1mXfQOa3x4a36mcWnmpqbcKCwlCxcwvG3NYkbtT1zkHpqpH1mjZzNucOFfmX7vqgS4JfXDpG7
NEMixAoXzVtqJUqpxyZGJP9HpUmF1ntxlPVOst1jVkh7SDK1Bz0XGx4TK6K4HQpuuZjNsS2RDVTF
kCGhHJOKUyhuY0TqYIBUcIsyh8bZ4ojPOzd5RF/n2DikoChI5F9QSmKrvGsVgxNBGdjCFwrGuMME
Q1UMXIE5hVCWY2j9am98gv5FKsQ8+h3YMA4o3hc6NDeCX1ffVysktwzZarAxkmfdoPuSApVmx337
AUVKipAZCM1XVxHr9mkShJTrMNGIOckuKJEoAJRVWYnzn9D4LtaE+EFYwaXilQ4XZB5JQHvdsCGC
+BuNc1CCA0k4fRTus4XcTIokKuQ9qH5wQZkVRxQ3daMS2MybvvqQqrY4cEYy+pc1AsYVvEqdcslF
Uqro3UulJn21E4VBp3S9K7prcMR0TYwuU4dDkH2AfhiFyyjDAV7WcwhFzeNZIgr6Li4ARH9BipUE
SulmETSlNY44DcDvju4DWME2oQuxYZ3WZFzQCdNmeAO9pKAtyAn7nCU+Ho+LaWtfjrBaPGRWUXWt
2rQDWEY4+BfGacN/pwAArieDdLdhOFJ53xDtbYfy050tPlvgp+GSo2qfim7E8WrXwi5zBpT8ghrp
T8lhV7LKOjP+f+3hwffuEoHK/BuxpXNyJo8fw8sHrkF9eJoRyvdIPwFWH7yZTTU6zJuiS8o50vgD
fpIew5JBgei0IhsEmGSrEkoPnCPlfZrqtxxOe97m+hIlDaPIjDQnRQ9CO3QEsyvOjmKvxHkScbEt
1bqej+bsUFaI2BK4yshHs7Aqx+ToXJqCEhYgCTdt5js8ZTR7BVGtBrfIMbhpPBprffOzduzq9/Fw
m28E3nYHJr9yhudQfT6H6IHJiOcS383nHvoBDQXFQJrDCY6L8zEnBDtKxjREtAKc0zdBpUU/C681
7X5FjDL+7XQgXnVab3BksvoJTZePvN0IFm8gY12Qqlf/EDVhT7nmPw8fyAcTrtSHP1v4G28XVxZJ
/H/j6mPOBd1kFI2bpDV2RrhCTUlDM47TcFMsnefgyXiRIkGy3/fm0OZwMPLDRZ5Nsb4S4EW7hnfP
fh4XG6rQz9XJbuxfSL2H1oVc6UfRntjmbRlJWWzE+f63EcaTcut6Fd8v0CgdnNY2wsuei15isQZ2
ySYBngVQWRnGnEDGyOAsDEVsXbOP3mW1B52J3/1QEAOdo06eLNsgpSW9Nn+xgyx60yfBfvAzzenR
hhrFZU4dkTEdLsNFXmIBv3UECP1BxTc5St9U8gGjbHrZMesGiu0ASA/SaC/qtLgjJEwnoALpRA5x
WD8r/yW94Jbr6D0AcbXGQ9gT81k0xFRd46MAY///dtj0g6ro2H5zMYGH8SOPBnqP5ceJkpTGJX8X
HnT72dwsf501YCqDBE662Ac5LtPUPuzs5mmGwaZnLRiWkHdXsb5TIvlYsl8/QEElw0t7XEn3uyU7
1ExmTu9kZL7PuwIYK46xIlXVv3TAri/CENv07WTJVY7y2ciEtmd1eS+jStmz3f0e6kOMGRPMeFpI
LqQVOVCJmhuZ8eFJQbAAgmqfxCha7i0x1z3w2O0JQcnq8cinBX7/FCwXSnOE66J9/gsz0dV2deTl
PNGpN9zVVCcGYaLv+zgY8sulBcEusfTg41wDWefuNpphjZpSpSgLXCEmscH7UQQ85z1hHfQjpyon
z5MrRScAD5PNRPD+6tUkGMCghTcPIhgf5g59Ag0LDfyAGrE3+sE2omSe3cD/D1mz3+TYBWSqNlHJ
lY8uzXnDrcbkqN1fIC9+d8TtttNiZQgcIewgxGqYVLBLM/848e/1usqu7Bz1+K6b8Jch/8U3qv7r
OGYAlUr54MQYhfnt</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: Sí (Token de Seguridad – KeyIdentifier)

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14135264025026380747 29">
```

```
                <wsu:Created>2014-10-17T06:13:22.502Z</wsu:Created>
                <wsu:Expires>2014-10-17T06:18:22.502Z</wsu:Expires>
            </wsu:Timestamp>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-
14135264025027000869 41">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-14135264025049951216 94">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="SOAP-ENV dss ds"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>32j9TwGtwR6z6GbDKZJH90dBxGU=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-14135264025026380747 29">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsu wsse SOAP-ENV"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>qyMaU2r/28UVE6dUmPbg3nMT5Vo=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>kPvDEBaQFzRUvlyKqvsQFAbIIy9DQ1s8gYZBpJbeaWdUN3ng9ik3CXfM3K/UECjQ+XuxwPlYMK26
1SNYjOakGI6lFrrb06Z4O+CkeTm2wHl29PPcF+UpL4yjgWmysinemhSbzJiTs9wr0PWOh8MxeDBH
Esow6+7thwRuGP8ANa5rJe+NSfY3bSOjPA+WO7OESs08CHclbNhPYG/XAsq5pyAc/4g+LYr1UdpO
D+/K4OlVQyZABpek1rhDNYCFUbuYJsNjgyGWcQ1TqMlps6lgZm57Pva8LqvYYx7hZH89Whbhu7gv
zm/ptrH3ycwNOKa69UFf/88Ew+1jm5GYNs0DSA==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-
14135264025038523222 00">
                        <wsse:KeyIdentifier 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#X509SubjectKeyIdentifier">Ahg6E1lYWBp+eACCz21Dvh7bJ5g=</wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-14135264025049951216 94">
        <dss:SignResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-dd7ed181-2908-44d6-8e80-
3206a65ac5d2">
            <dss:Result>
                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            </dss:Result>
            <dss:SignatureObject>
                <dss:Timestamp>
                    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Id-1ee327bc-
01bc-4a83-84d6-d71d5f8d9f33">
                        <ds:SignedInfo Id="Id-245899b5-49b0-488c-8ff2-b18980b4c66d">
                            <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 Id="Id-3da31f50-6d8b-4b03-a2d0-ae257588bcf7">
                                <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>+VbKci2rOHmHZfsQwmqYKBC1d/Y=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-1116a41d-e437-4660-a0f8-bc88ffcd7aed"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-c2b194d1-6757-4dbc-
ad75-a5e65ee5895a">
                                <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>OVEirb77umQSf8hpb4RYkrziA/4=</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>

<ds:SignatureValue>eZ6aUhpIhqAjkQhozxsNfn3wLaAwzitJ8DA2EebAglNzAD+zDPCQIt0A2W9W92ApowFjzFcDg1R4
0FEyTgjy4VNnShTxb3BZiMJHC3m4Ea0JxLjgdgYCUDS6NUF8QHqUj8Tr6eetV61Yc7xvNKvRBz1J
HouuCE5ieGsjy+m8p/PoTh76bvH5ldnywfZ5H8zYStRvwGPwraJZLPG9sxkQiDuC54EB+zS9KkXX
h5AyEXNmGXORM5EITtUL0XEGnlXpt6LHhKhPh6tN/5Te5x7ZxNEuhfjCnPxtClPrRATnU8Q8/W80
QyXIdYSf6p7ZBnwIm0ktdaIfRn/funCZoWQNDA==</ds:SignatureValue>
                        <ds:KeyInfo>
                            <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1h
U3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50
MQswCQYDVQQGEwJFUzAeFw0xMjEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMM
EVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAwHgYDVQQLDBdUZWx2ZW50IEds
b2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4H
lyxktK6uz6ArGjFM5Bebqz4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/
G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh54cAMZGllNVBbZEHjgBqS9THNO673
GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jDBMPG
V8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+a
WP8CAwEAAaOCAdIwggHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0
My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwm
aXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZpY2VzJTJj
TyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcD
CDAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGR
hoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2Vy
dGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwr
U2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYE
FPW/tms4rvVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabt
w/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6
HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfClWAznM2nejANDSs5
31EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FEl
THVf/ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6
WEj7yoNQzsBrcMV3</ds:X509Certificate>
                            </ds:X509Data>
                        </ds:KeyInfo>
                        <ds:Object Id="TSTInfo-Id-c2b194d1-6757-4dbc-ad75-a5e65ee5895a"
MimeType="application/xml">
                            <dss:TstInfo>
                                <dss:SerialNumber>1413526075818100008</dss:SerialNumber>
                                <dss:CreationTime>2014-10-17T08:13:22.450+02:00</dss:CreationTime>
                                <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                <dss:Ordered>true</dss:Ordered>
                                <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                            </dss:TstInfo>
                        </ds:Object>
                    </ds:Signature>
                </dss:Timestamp>
            </dss:SignatureObject>
        </dss:SignResponse>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


A.3.3 Ejemplos de Renovación de Sello de Tiempo

Servicio discontinuado (deprecated).

Ejemplo 7. Solicitud de Renovación de Sello de Tiempo XML

Petición:

- Securización de la Cabecera SOAP: SAML 1.0 (Método de Confirmación del Sujeto – Holder of Key)
- InputDocument: DocumentHash (Con Transformada)
- Petición Encriptada con Clave Simétrica: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413535934083-1071201767">
                <wsu:Created>2014-10-17T08:52:14.150Z</wsu:Created>
                <wsu:Expires>2014-10-17T08:57:14.150Z</wsu:Expires>
            </wsu:Timestamp>
            <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:exc14n="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:xs="http://www.w3.org/2001/XMLSchema" AssertionID="1413535934083" IssueInstant="2014-10-
17T10:52:14.083+02:00" Issuer="C=ES, O=Telvent, OU=Telvent Global Services, CN=AfirmaSubCA"
MajorVersion="1611735152734479641" MinorVersion="1">
                <saml:Conditions NotBefore="2014-10-17T09:52:14.083+02:00" NotOnOrAfter="2014-10-
17T11:52:14.083+02:00"/>
                <saml:AttributeStatement>
                    <saml:Subject>
                        <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=ES, O=Telvent, OU=Telvent Global Services,
CN=AfirmaSubCA</saml:NameIdentifier>
                        <saml:SubjectConfirmation>
                            <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-
key</saml:ConfirmationMethod>
                            <ds:KeyInfo xmlns:ns5="http://www.w3.org/2001/XMLSchema-instance"
ns5:type="keyInfo">
                                <ds:KeyValue>
                                    <ds:RSAKeyValue>

<ds:Modulus>kch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0ptsmAVJ9OJ7D2gMvPgQNJEOshdF
yG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MPxKb4NZm5fFd1LGApXNEPZ0OCOxpGkIMwn/Yk
HSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0aWqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u6+GuHKijZ5LUeVrSpjcRq9Nhp
+gVvqnaxVlmeRgG7C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQ==</ds:Modulus>
                                        <ds:Exponent>AQAB</ds:Exponent>
                                    </ds:RSAKeyValue>
                                </ds:KeyValue>
                            </ds:KeyInfo>
                        </saml:SubjectConfirmation>
                    </saml:Subject>
                </saml:AttributeStatement>
                <ds:Signature>
                    <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="#1413535934083">
                            <ds:Transforms>
                                <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                <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>bPx1AA/df7pN10cqZQxx9VE63jk=</ds:DigestValue>
                        </ds:Reference>
```

```
                    </ds:SignedInfo>

<ds:SignatureValue>BXgSdqvxZgEK8vzBWquU1BmDfVmCJE1UT3S9CCJdV169XODfbMOqulEnoOHD2edn/BUxmGVPGLHH
W99p/0tHfQKW1jC8B5MlwnhlwWKsF4lRuAZvUOf8jXVrzaVMDSH1iXqsUvTNKbDlPar80mSr9Xfv
mDrKSBnLIWJxBs/DZ31GqlTqQkWVpiZrFXNBQ5JCsXB8wBgQa3aODUh0+NSVC1NLtZmMDotoYWxF
K2JvTzGeIgZ7vylgNWB9sRW75qT7VWrkqK9HOry/0jrghInrhCcBi2eMbjTbtlZWnIIqtdQbz6Uj
Pj6D3dIchwranry1QoY99LuJoCSYhlX8i8w0sQ==</ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:KeyValue>
                            <ds:RSAKeyValue>

<ds:Modulus>kch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0ptsmAVJ9OJ7D2gM
vPgQNJEOshdFyG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MP
xKb4NZm5fFd1LGApXNEPZ0OCOxpGkIMwn/YkHSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0a
WqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u6+GuHKijZ5LUeVrSpjcRq9Nhp+gVvqnaxVlmeRgG7
C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQ==</ds:Modulus>
                                <ds:Exponent>AQAB</ds:Exponent>
                            </ds:RSAKeyValue>
                        </ds:KeyValue>
                    </ds:KeyInfo>
                </ds:Signature>
            </saml:Assertion>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-
14135359340821650609394">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413535934118761397927">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>cRmHoGQS88YgWuixYmAHV5wQbeQ=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>GcTTjtTT7TPJVFHhhCv73CY5bvApeubxq+6WK7x0Lwl+EbzLdHNO9kwNsJxEXfj3MN3hBIBkUjVf
45kl95S7gxx+aCeLRMnzriLgICCPflz4D/ouRCLmV92nijS0ZYYSd9Qr+KM711bp/KI5NZOtNyK2
awB5biLor/hMnXJczSYIJBKu4LNuhpBmprgGwT+QMnF1dOFtZL2RcMN+RURg1VF+ZPiR6yiiXV5V
4vYkttsqaxOhH6z0htieF+YyblmyYxaxabAbTWRWWaOYviovMxfCwcnpCY3R3Q6+HUjyqTIW9wUm
IQAHlqFOv8gK8wx/NiyjPRqNqlEuwJZCjrlx2Q==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-
wss-wssecurity-secext-1.1.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLV1.1" wsu:Id="XWSSGID-1413535934117184581945O">
                        <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-
saml-token-profile-1.0#SAMLAssertionID">1413535934083</wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413535934118761397927">
        <dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:dst="urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema#"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
            <dss:OptionalInputs>
                <dst:RenewTimestamp>
                    <dst:PreviousTimestamp>
                        <dss:Timestamp>
                            <ds:Signature Id="Id-a9698375-ea34-42f1-a96f-f6772a5cc8e9">
                                <ds:SignedInfo Id="Id-ede3c3d7-e671-4ffa-92b6-20f8c4f3da24">
                                    <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 Id="Id-9b68dbaf-2b06-4cf4-818e-e8987685ea93">
                                        <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>+VbKci2rOHmHZfsQwmqYKBC1d/Y=</ds:DigestValue>
                                    </ds:Reference>
                                    <ds:Reference Id="Id-bac13f23-6cb5-47ba-956c-2cd03b05600c"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-37ced97a-520b-4812-
81f6-2b2e35ccc9a0">
                                        <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>fT0zwOb/2XwPFHLzbAyb+ehNVvI=</ds:DigestValue>
                                    </ds:Reference>
                                </ds:SignedInfo>

<ds:SignatureValue>ebfVTDThpllxNJzJvlpdkbfvv5E5Sb/fXqlAD+agKZ1F1q1e3UIo/vBBqcd+gET/WP4zqUUBzQ6Rorad7
bXPYo9bSwfHg1pIW3uT2cAWKMI+OGedEgPNSivdJ2yGH7FqDRNGtTGHMWaepEAcZE7SXqhU6s9mgP6j+ByPfS8m6kTpbDOykxRPB
rQ+aLU29MGQ8Iq5Vjbh/uX1jpkbvmru1xT87EobcZKnWB9Feioacdfekig+1ZNP+n5qQZsdvtfu1aE8xAVI74NfyEeX0V9vI22ur
9Vhp54O7p6cDSsY9ggP1h57NcvwZpre+pi9WB3ZvwcbpjBybYorMDVug4XI3w==</ds:SignatureValue>
                                <ds:KeyInfo>
                                    <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3Vi
Q0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEy
MDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ251cldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAw
HgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebqz4t
4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh5
4cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMo182o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jD
BMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwggHO
MIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlz
dC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZp
Y2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEGDAW
gBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAv
ZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVu
dCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4rvVH
7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE0
7uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfC
lWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/ivH
ByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3</ds:X509Certifi
cate>
                                    </ds:X509Data>
                                </ds:KeyInfo>
                                <ds:Object Id="TSTInfo-Id-37ced97a-520b-4812-81f6-2b2e35ccc9a0"
MimeType="application/xml">
                                    <dss:TstInfo>
                                        <dss:SerialNumber>1413530041215100056</dss:SerialNumber>
                                        <dss:CreationTime>2014-10-
17T10:52:13.949+02:00</dss:CreationTime>
                                        <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                        <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                        <dss:Ordered>true</dss:Ordered>
                                        <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                                    </dss:TstInfo>
                                </ds:Object>
                            </ds:Signature>
                        </dss:Timestamp>
                    </dst:PreviousTimestamp>
                </dst:RenewTimestamp>

<dss:SignatureType>urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken</dss:SignatureType>
                <dss:ClaimedIdentity>
                    <dss:idAplicacion>appPrueba</dss:idAplicacion>
                </dss:ClaimedIdentity>
            </dss:OptionalInputs>
            <dss:InputDocuments>
                <dss:DocumentHash>
                    <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>+VbKci2rOHmHZfsQwmqYKBC1d/Y=</ds:DigestValue>
                </dss:DocumentHash>
            </dss:InputDocuments>
        </dss:SignRequest>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <dss:SignResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-b67b815d-4146-4cc2-8da7-
d909204a9f67">
            <dss:Result>
                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            </dss:Result>
            <dss:SignatureObject>
                <dss:Timestamp>
                    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Id-2ec6245f-
596c-4bb9-8636-ca7f9d9463d4">
                        <ds:SignedInfo Id="Id-41d1577b-8048-48e2-83a5-cee00eded02e">
                            <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 Id="Id-2a6dd767-78fd-446b-b153-9daea8fc15d5">
                                <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>+VbKci2rOHmHZfsQwmqYKBC1d/Y=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-3cae2e82-a0e0-44b6-a2b7-096cd2cf37dd"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-4bc07a6c-eee7-4bf0-
bf1f-139871b603e0">
                                <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>Wne7PwXi2mdsEkWGrm3/VvM3v+o=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-c7ef9bae-798c-4470-8cbc-c5fd340635ec"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-8f0902ab-2211-42ae-
8ac2-7d5faaa864ca">
                                <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>ey3KI0d4MVMeGEEauCA1aM3QmPw=</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>

<ds:SignatureValue>PjyFLjTzVnzSuXn8xnYDQ5CtnW1fXuGayiqQTYG9mQjbqLRSxCUJQmzWMkbvuRiuRxQ0YSQwgsE1
At6NDgsPy3wS5dXiXJco98dYLEP7YaoTSpKmXP4mMPfl0GlxpnNzm2cYUu2VhMPfaNuCpdnAH6G4
```

```
ag6xh28uksgiKObrNl1XrcZ2ReGtnG7Ran1K/pkwlM5ctX18GrHGe1FaWqOTdNl/pTmAbfHbz8qK
7P85U2NwzKdSAKJymAjmTmVmR07O9XnMgVkhtqAZ0Cjs+29XqKuiqlHOTCr0mEbGSbF7XPaX3uEO
3LH/ZMY9nXOn+Z7g/0C2PiJCqwpZrtq1Rw7BUQ==</ds:SignatureValue>
                        <ds:KeyInfo>
                            <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1h
U3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50
MQswCQYDVQQGEwJFUzAeFw0xMjEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMM
EVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAwHgYDVQQLDBdUZWx2ZW50IEds
b2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4H
lyxktK6uz6ArGjFM5Bebqz4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/
G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh54cAMZGllNVBbZEHjgBqS9THNO673
GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jDBMPG
V8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+a
WP8CAwEAAaOCAdIwggHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0
My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwm
aXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZpY2VzJTJj
TyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcD
CDAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGR
hoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2Vy
dGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwr
U2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYE
FPW/tms4rvVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabt
w/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6
HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfClWAznM2nejANDSs5
31EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FEl
THVf/ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6
WEj7yoNQzsBrcMV3</ds:X509Certificate>
                            </ds:X509Data>
                        </ds:KeyInfo>
                        <ds:Object Id="TSTInfo-Id-4bc07a6c-eee7-4bf0-bf1f-139871b603e0"
MimeType="application/xml">
                            <dss:TstInfo>
                                <dss:SerialNumber>14135300412151000 58</dss:SerialNumber>
                                <dss:CreationTime>2014-10-17T10:52:14.246+02:00</dss:CreationTime>
                                <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                <dss:Ordered>true</dss:Ordered>
                                <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                            </dss:TstInfo>
                        </ds:Object>
                        <ds:Object Id="TSTInfo-Id-8f0902ab-2211-42ae-8ac2-7d5faaa864ca"
MimeType="application/xml">
                            <dst:PreviousTimestamp
xmlns:dst="urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema#">
                                <dss:Timestamp>
                                    <ds:Signature Id="Id-a9698375-ea34-42f1-a96f-f6772a5cc8e9">
                                        <ds:SignedInfo Id="Id-ede3c3d7-e671-4ffa-92b6-20f8c4f3da24">
                                            <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 Id="Id-9b68dbaf-2b06-4cf4-818e-
e8987685ea93">
                                                <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>+VbKci2rOHmHZfsQwmqYKBC1d/Y=</ds:DigestValue>
                                            </ds:Reference>
                                            <ds:Reference Id="Id-bac13f23-6cb5-47ba-956c-
2cd03b05600c" Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-
37ced97a-520b-4812-81f6-2b2e35ccc9a0">
                                                <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>fT0zwOb/2XwPFHLzbAyb+ehNVvI=</ds:DigestValue>
                                                </ds:Reference>
                                            </ds:SignedInfo>

<ds:SignatureValue>ebfVTDThpllxNJzJvlpdkbfvv5E5Sb/fXqlAD+agKZ1F1q1e3UIo/vBBqcd+gET/WP4zqUUBzQ6Rorad7
bXPYo9bSwfHg1pIW3uT2cAWKMI+OGedEgPNSivdJ2yGH7FqDRNGtTGHMWaepEAcZE7SXqhU6s9mgP6j+ByPfS8m6kTpbDOykxRPB
rQ+aLU29MGQ8Iq5Vjbh/uX1jpkbvmru1xT87EobcZKnWB9Feioacdfekig+1ZNP+n5qQZsdvtfu1aE8xAVI74NfyEeX0V9vI22ur
9Vhp54O7p6cDSsY9ggP1h57NcvwZpre+pi9WB3ZvwcbpjBybYorMDVug4XI3w==</ds:SignatureValue>
                                            <ds:KeyInfo>
                                                <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3Vi
Q0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEy
MDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ251cldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAw
HgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebqz4t
4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh5
4cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jD
BMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwggHO
MIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlz
dC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZp
Y2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEGDAW
gBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAv
ZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVu
dCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4rvVH
7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE0
7uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfC
lWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/ivH
ByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3</ds:X509Certifi
cate>
                                                </ds:X509Data>
                                            </ds:KeyInfo>
                                            <ds:Object Id="TSTInfo-Id-37ced97a-520b-4812-81f6-
2b2e35ccc9a0" MimeType="application/xml">
                                                <dss:TstInfo>

<dss:SerialNumber>14135300412151000 56</dss:SerialNumber>
                                                    <dss:CreationTime>2014-10-
17T10:52:13.949+02:00</dss:CreationTime>
                                                    <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                                    <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                                    <dss:Ordered>true</dss:Ordered>
                                                    <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                                                </dss:TstInfo>
                                            </ds:Object>
                                        </ds:Signature>
                                    </dss:Timestamp>
                                </dst:PreviousTimestamp>
                            </ds:Object>
                        </ds:Signature>
                    </dss:Timestamp>
                </dss:SignatureObject>
            </dss:SignResponse>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Ejemplo 8. Solicitud de Renovación de Sello de Tiempo XML

Petición:

- Securización de la Cabecera SOAP: SAML 1.0 (Método de Confirmación del Sujeto – Sender Vouches)
- InputDocument: TransformedData
- Petición Encriptada con Clave Simétrica: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413536531268-425179357">
                <wsu:Created>2014-10-17T09:02:11.309Z</wsu:Created>
                <wsu:Expires>2014-10-17T09:07:11.309Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" 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="XWSSGID-
14135365312687936680 23">MIIFRTCCBC2gAwIBAgIIFl4IlQK/pRkwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1h
U3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0x
MjEwMjMxMzAwMjJaFw0xNTEwMjYxNTA0MThaMHMxEzARBgNVBAMMClNvYXBTaWduZXIxEDAOBgNVBAsMB1RlbHZlbnQxIDAeBgNV
BAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRswGQYDVQQKDBJTY2huZWlkZXIgRWxlY3RyaWMxCzAJBgNVBAYTAkVTMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0pts
mAVJ9OJ7D2gMvPgQNJEOshdFyG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MPxKb4NZm5fFd1
LGApXNEPZ0OCOxpGkIMwn/YkHSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0aWqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u6
+GuHKijZ5LUeVrSpjcRq9Nhp+gVvqnaxVlmeRgG7C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQIDAQABo4IB9zCCAfMwga0G
A1UdLgSBpTCBojCBn6CBnKCBmYaBlmh0dHA6Ly8xNzIuMjEuMjQzLjEwMjo4MDgwL2VqYmNhL3B1YmxpY3dlYi93ZWJkaXN0L2Nl
cnRkaXN0P2NtZD1kZWx0YWNybCZpc3N1ZXI9Q04lM2RBZmlybWFTdWJDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2Vydmljc XMl
MmNPJTNkVGVsdmVudCUyY0MlM2RFUzAMBgNVHRMBAf8EAjAAMDsGA1UdJQQ0MDIGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUH
AwQGCCsGAQUFBwMIBggrBgEFBQcDCTAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGU
oIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZp
c3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2Vydmljc XMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAO
BgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFAIYOhNZWFgafngAgs9tQ74e2yeYMA0GCSqGSIb3DQEBBQUAA4IBAQBmeMs+UdPMWY5I
cyn97ZR//LOfk6ElAfgxRs1y6DH1oJdiWUnVkHmSgGNY+Y4j4y74TMiH25naizyyKQzmGoHw7KOgTxxqUEwlEHZPuf5GIJxc+/a0
askEItRRgf9pozjL2+RS4YMU33xJlyBZNQ4nrvlKyNx50favpiKD2kOuHFqu3CypQzEvWw8uW5RY6Vvmujc3pztwjZtMeatWTbxM
S8+c4wfT7N5bgRFCH3t/Wu/yhKQlnfkXGLdpOeIt2pxIKH15UR7ODMmlNcIIRJQPoCPm5PWPmo24BkTb5U+nr1y4I5yY/gkIOamm
YYORPb10i1vx9bRX1llTnWg4/YNX</wsse:BinarySecurityToken>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-
14135365312684698529 22">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413536531272-2069059990">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>/JYNYFpHotT1WvX+rH7LWUit684=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="SV-123">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#STR-Transform">
                                <wsse:TransformationParameters>
                                    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                </wsse:TransformationParameters>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>m9iA5Y6SVtgqAEm+X0Ve9bx8MBk=</ds:DigestValue>
```

```
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>NIODTx4qN8/ZQKlkU40nTIBNaQix+JGTnIdqVBeLzw/wpeSAWrWMZ4kmQqvd1Nqxc5v4f6zDEVAw
cUjdjkxzdaDhWwRWl7f1pcOdYCDZ3D0PRllLmcsnnt8WGxuVGCXujsoM928OE8ibZ/gGA/xI9PzT
4hBYG9JwTevI/8bArVInQ5FEGOUSOvSFYcPEEWcg0PDMyBzu7CCDDd8VhWeuOy/fDWXrDZ42PlsM
GNOiDTqh6xqROeopatIYi6fguSwYqzLYnQ3fE1g8Yf4N/vdqt9D3DhJ1gLPqM2/EeT6UijFR5HP8
ZXKbbe7s64K4YOT2AJdAeNKFF0+Qqa9UongxJg==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413536531272-
752528016">
                        <wsse:Reference URI="#XWSSGID-141353653126879366802 3"
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:SecurityTokenReference xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-
wssecurity-secext-1.1.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLV1.1" wsu:Id="SV-123">
                <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">1413536531269</wsse:KeyIdentifier>
            </wsse:SecurityTokenReference>
            <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:exc14n="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:xs="http://www.w3.org/2001/XMLSchema" AssertionID="1413536531269" IssueInstant="2014-10-
17T11:02:11.269+02:00" Issuer="C=ES, O=Telvent, OU=Telvent Global Services, CN=AfirmaSubCA"
MajorVersion="1611735152734479641" MinorVersion="1">
                <saml:Conditions NotBefore="2014-10-17T10:02:11.269+02:00" NotOnOrAfter="2014-10-
17T12:02:11.269+02:00"/>
                <saml:AttributeStatement>
                    <saml:Subject>
                        <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=ES, O=Telvent, OU=Telvent Global Services,
CN=AfirmaSubCA</saml:NameIdentifier>
                        <saml:SubjectConfirmation>
                            <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:sender-
vouches</saml:ConfirmationMethod>
                        </saml:SubjectConfirmation>
                    </saml:Subject>
                </saml:AttributeStatement>
            </saml:Assertion>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413536531272-2069059990">
        <dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:dst="urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema#"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
            <dss:OptionalInputs>
                <dst:RenewTimestamp>
                    <dst:PreviousTimestamp>
                        <dss:Timestamp>
                            <ds:Signature Id="Id-15b1caf6-e402-4330-84c5-6beec607db89">
                                <ds:SignedInfo Id="Id-4fed4aed-ec59-4c43-84b0-f85c2cc59cea">
                                    <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 Id="Id-444686e0-2621-45d3-9e82-11dc67f08bd9">
                                        <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>+VbKci2rOHmHZfsQwmqYKBC1d/Y=</ds:DigestValue>
                                    </ds:Reference>
                                    <ds:Reference Id="Id-3a73d231-7582-4841-874a-7b40fa631346"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-9cb852b7-3eb8-44e2-
b533-fa02b0aa2b48">
```

```
                                        <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>u61X/xEWOFTa9owozu/LU33vzW8=</ds:DigestValue>
                                    </ds:Reference>
                                </ds:SignedInfo>

<ds:SignatureValue>NAm+QvZ1+J+iS6b5fo4wc3L1zOxpDItUS9gfzw0DvbrjoCV6EK+yJBGQuXq1JKD8by68x4P5yLWYtz/i9
EoFVWJljR9uBDitt/wnBpr/AeU6Uuu8X2snGBwYQmJU8dEAxLWezBY+CitpBWT52yA1qNHe08Y3pwUf6xZpnmLE1ssaRT4giHmzb
h34huPPcWIgo/iXmZBZAfjtszQUWcXJFAQdR9Wy59PlBd6lrWpXlWC1ApTVe/gz6gGB0JkPauUl7Ows7qRjO7rIhtNb2pemtEA/6
nmqrCiFf5u2iAUWka3xcgVBUR3DasUFC/KCCLWVvzLP2rMkvboSo+MKHycRyA==</ds:SignatureValue>
                                <ds:KeyInfo>
                                    <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3Vi
Q0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEy
MDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAw
HgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebqz4t
4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh5
4cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jD
BMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwggHO
MIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlz
dC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZp
Y2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEGDAW
gBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAv
ZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVu
dCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4rvVH
7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE0
7uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfC
lWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/ivH
ByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3</ds:X509Certificate>
                                    </ds:X509Data>
                                </ds:KeyInfo>
                                <ds:Object Id="TSTInfo-Id-9cb852b7-3eb8-44e2-b533-fa02b0aa2b48" MimeType="application/xml">
                                    <dss:TstInfo>
                                        <dss:SerialNumber>1413530041215100066</dss:SerialNumber>
                                        <dss:CreationTime>2014-10-17T11:02:11.071+02:00</dss:CreationTime>
                                        <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                        <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                        <dss:Ordered>true</dss:Ordered>
                                        <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                                    </dss:TstInfo>
                                </ds:Object>
                            </ds:Signature>
                        </dss:Timestamp>
                    </dst:PreviousTimestamp>
                </dst:RenewTimestamp>

<dss:SignatureType>urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken</dss:SignatureType>
                <dss:ClaimedIdentity>
                    <dss:idAplicacion>appPrueba</dss:idAplicacion>
                </dss:ClaimedIdentity>
            </dss:OptionalInputs>
            <dss:InputDocuments>
                <dss:TransformedData>
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    </ds:Transforms>

<dss:Base64Data>PERvY3VtZW50IHhtbG5zPSJodHRwOi8vNHRpYy5jb20vZm91cnNpZ24vc2lnbnN0b3JlL2RlZmluaXRpb25z
Ij48RGVzY3JpcHRpb24+RG9jdW1lbnRvIDwvRGVzY3JpcHRpb24+PFNlcnZlclNpZ25hdHVyZT5mYWxzZTwvU2VydmVyU2lnbmF0
dXJlPjxGb3JtYXQ+SlgKQURFUzwvRm9ybWF0PjxJc3N1ZXI+RmlybWEgYXV0b21hdGljYTwvSXNzdWVyPjxTaWduYXR1cmVUeXBl
PjxDb2RlPm9wZW5zYXQ8L0NvZGU+PC9TaWduYXR1cmVUeXBlPjxDb250ZW50VHlwZT50ZXh0L3htbDwvQ29udGVudFR5cGU+PEZp
bGVOYW1lPmluLXhhZGVzLnhtbDwvRmlsZU5hbWU+PERhdGE+UEQ5NGJXd2dkbVZ5YzJsdmJqMGlNUzR3SWlCbGJtTnZaR2x1Clp6
MGlWVlJHTFRnaVB6NEtQRk5wWjI1bFpUnZZeUJtYjNKdFlYUTlJa1JKUjBsRVQwTXRXRTFNSWlCMlpYSnphVzl1UFNJeExqTWlJ
```

SGh0Ykc1elBTSm9kSFJ3T2k4dmQzZDNMbk5yTG1WbEwwUnBaMmxFYjJNdmRqRXVNeTR3SXlJK0NqeEVZWFJoUm1sc1pTQjRiV3h1
Y3owaWFIUjBjRG92TDNkM2R5NXpheTVsWlM5RWFXZHBSRzlqTDNZeExqTXVNQ01pSUVOdmJuUgpsYm5SVWVYQmxQU0pGVFVKRlJF
UkZSRjlDUVZORk5qUWlJRVpwYkdWdVlXMWxQU0owYjFOcFoyNHhNalF3TmpBME1qazJORFV4TnpVNE1EVTNMbmh0YkNJZ1NXUTlJ
a1F3SWlCTmFXMWxWSGx3WlQwaWRHVjRkQzk0Yld3aUlGTnBlbVU5SWpNM01USWlQbEJFT1RSaVYzZG5aRzFXZVdNeWJIWmlhakJw
VFZNMGQwbHBRbXhpYlU1M1drZHNkVnA2TUdsV1ZsSkhURlJuYVYKQjZORTVEYW5oUVkwZFdkVlV3UmxWUWFuaEdZa2RXZEZwWE5U
QlFhbmhyWXpBMWFHSlhWU3RSVlRWSVVsVjNaMVJHVmtwVmVVSkxVMVV4UmxSclZtRkpSVEZDVld4U1NsUnJWbUZRUXpscll6QTFh
R0pYVlN0UVNFcHNZek5XYzJSSFJtdGlNRnB3WW0xR2MxQnFkM1pqYlZaNlpGZDRNRmxYVW5aU2JXeDFXVmQzSzFCSFJuZGFWM2h6
WVZkU2RrMXNTbXhqUkRWT1VWWktWClZOVk5VWlhhbmQyV1ZoQ2JHSkhlSEJhUnpoNVZXMVdkMUJxZUhSYVYxSndZak5PUmxreU9Y
VmlNakZ3V1RJNWVsQnFkM1ppVjFacllWYzVlbEpYVG5aaWJUbDBZVmRPZG1ONk5EaGhWekZ1VkZkR2NHSnFOVzlrU0ZKM1QyazRk
bUpIT1dwWlYzaHZZak5PTUU5cWEzZE5SRUYyWWpOQ2JHSnVUbWhrUXpreldsZEpkbUZYTVdoYU1sWjZURExXZWxrelZtdGlNVGw1
V2xoQwpkbU51VVhWYU1teHRVRU01Y0dKWFpFNVpWMngxVUdwNGExcFhUbk5UYmxaNVdWZFNhRk51VmpaYU1rWnJZak5OSzFCRE9X
dGFWMDV6VTI1V2VWbFhVbWhUYmxZMldqSkdhMkl6VFN0UVIxSnNXVEo0UzJSWVNtaGFSMFpDV1ROU01WbFhlSEJsYlVacVlWYzVk
VkJ0T1hWUVF6bHJXbGRPYzFOdVZubFpWMUpvVVZkT01HUlhSbk5oV0hCb1dUSnNkbUpxTkRoa1IyeDNZakYKU2VWbFhOWHBqUnps
NVpFZFZLMUJET1RCaFdFSjJWa2hLYUdKdVRuZGlNMG93V2xRME9GcHRSalJRYW1zeVRrUlZNVTVxV1ROT2VuZDJXbTFHTkZCcWVH
MWlNMUoyV1RJNWQyRlhSa1ZVYTJ4SFlWaE9jRmt5UlN0UVF6bHRZak5TZGxreU9YZGhWMFpGVkd0c1IyRllUbkJaTWtVclVFZHNh
MUJxUlRWTlJFRTFUa1JOTVZKNmQzWmhWMUVyVUVoT2JHSkhWbXBrUjFaclVWCmRPTUdGWE9YVlFibEpzWTIweFZHRlhaSFZhVjFF
NFRETk9iR0pIVm1wa1IxWnJVVmRPTUdGWE9YVlFhbmg2WVZka2RWVnRPWE5hVkRRNFRETk9jRm95TlZOaU1uaHNVR3A0YUdOSFZu
TmlSMnhyWW5wRksxQkRPV2hqUjFaellrZHNhMko2UlN0UVJ6VXhZbFZXTkdOR1NteFpWM2NyVFVSM2RtSnVWblJTV0doM1ZXMVdh
R0pFTkRoaWJsWjBVbGhvZDFCcVFUaE1NalV4WQpsVldOR05FTkRoa01qbDVZVEphYzJJell5dGlSMnhxWVZoU2FGcEhPWGxhV0Ux
MFRWTTBNVXhYZUhCWk1td3dXVmRTZG1OdFZucE1WRVYxVGxOUmVFOVVkM1prTWpsNVlUSmFjMkl6WXl0UVIxSjJXVE5XVjJGWFZq
TlFhbmQyV2tjNWFtUldXbkJhV0dNclVFZEdhbVJIYkRKaFdGSTFVRzVPZG1KSGJHcGhXRkl4V2tSM2RsbFhUakJoV0Zwd1pFaHJL
MUJIVW5aWk0xWjAKV2xjMU1GRllVakJaVjA1dldsZFNUMWxYTVd4UWFuZDJXa2M1YW1SWE1XeGlibEpDWkVoU2FGa3lhR3hhUlRW
b1lsZFZLMUJIVG5OWldFNTZVRzFPYzFsWVRucEpSMDUyWWxNMWJXSXpWbmxrUjJ4cVRHMDVkMXBYTlhwWldGRjFZek5TZVdSWVVu
cE1iVnAyWTIweGVreHVRbmxpTWs1c1l6STVla3h0ZUhCWk1td3dXVmRTZG1OdFZucE1iRTUyWWtkc2FtRllVakZhUlZwCjJZMjB3
T0V3eVRuTlpXRTU2VUdwNGRXRlhXbE5hV0VFclRWUnJkMDFFYXpCTmVsWklVRU01ZFdGWFdsTmFXRUVyVUVkc2ExUkhPV3BaVjNo
d1drZEdhMUJxVVhkUVF6bHdXa1Y0ZGxreVJuTmhWMUpvV2tRME9HTnRWbTVoV0U0d1kyMDVVV050T1cxYVdFNXdZakkxYUdKRU5E
aE1NMHBzV2pKc2VtUklTblpWU0VwMldtMVdlbUZYT1hWWlYzY3JVRWRrZVdGWFVsRlpVQpvd1lWZE9NV0pIUm5sWU1qbHJaRVEx
V0Vrd1ZXcFZhVTVWVUVNNWJtTnRiR3RWUjBaNVpFZHNhbVJYZUdoamJEbDJXa2hSSzFCSFVucFdSMVp6V2xkWksxQkRPV3RqTVZK
c1lrZFdiVkJxZUhCYVJVWXhaRWM1YzJGWVJqRmhWMUpvV1RKc2RtSnFORGhNTW14clVWaFdNR0l5ZUhCaldGWndXa2RHYW1GWE9Y
VlFhbmhxV1ZoU2JGb3lPWGxoVjBaRVlrZEdlbUZYV25CWk0Ka1pxWVZjNWRWQnNTVGhNTWs1b1pFZFdibUl6U25CWlZVNXpXVmhP
Y0ZwdGJHcFpWMDV3WWpJMEsxQkhVblpaTTFaaFlWaEJLMlZYVm5wUVF6bHJZakpPTVZkdGJIZFFhbmh3WW0xYWRtTnRNV3hVVjJ4
NllWYzVkVkpIYkhkaVJ6bDBXVmhTY0ZreVJTdFFRemx3WW0xYWRtTnRNV3hVVjJ4NllWYzVkVkpIYkhkaVJ6bDBXVmhTY0ZreVJT
dFFTRUoyV2tkV2VWcFlUU3RRClF6bDNZakpTYkdOdFZucFFhbmh3WWxoQ2VWSkhPV3BrVkRVd1kyNVdiRkJET1hCaVdFSjVVa2M1
YW1SVU5EaGliV3h0VUdwRk5VMUVRVFZPUkUweFVucDNkbUp0YkcxUWFuaHJXbGhPYWxaSGJIZGlNVTUyWWtkc2FtRllVakZhUlU1
M1lsZEtkbEJxZDNaYVIxWjZXVEZTY0dOSE9WUmlNbmh3V1RKc01HUlhVa1JpTWpGcFlubzBPRnBJVGtabFNFSnNXa2RzYkdKdVVt
eApWYlZab1lrUTBkMUJET1d0ak1GWTBZMGRXYTJGWFZuVmtSMVpUV2xkR2MxQnFlSFJhVjFKd1lqTk9WVnBYVG5WaFYwNTJZM28w
T0V3eU1XeGFSMngyWXpGU2JGa3lOWEJaTWpsNlVHcDRhMk13VmpSalIxWnJZVmRXZFdSSFZTdE5SSGQyV2toT1JtVklRbXhhUjJ4
c1ltNVNiRkJxZUhsYVYwNTJZMjFSSzAxWWVHeGlbEo1WlZoNGVtSXllSEJaTW13d1pGZFJPRXd6U20KeFpNamw1V2tRME9Gb3pT
bkJhUmtwc1l6TkNkbUp1VG1oWmJYaHNZekU1ZGxwSVVTdFJWV

```
SjRNbHBYTldwaFYwWlZXbGRPZFdGWFRtaFFhbmQyWXpJNWMyUnRWblZaTW14b1ZrZFdhbUp0YkdwWlZEUTRaRWRzZDJJd05YWmtS
Mnh0WVZkT2FGa3liSFppYWpWMVlqTlNjRnB0YkdwWlZIZDJaRWRzZDJJd05YWmtSMnh0WVZkT2FGa3liSFppYWpRNFdWaENiR0pI
ZUhCYVJ6aDRWVzFXZDFCcmNFcFVWVlpQVWxadk9Fd3lSbmRhVjNoellWZFNkazFXU214alJEUTRXa2hPUldGWVNteFpNMUp3WWpJ
MEsxQkRPV3RqTUZKd1kyMVdhbVJIYkhaaWFqUTRXbGhPYW1OdGJEQmtXRXBvWTNvME9Fd3lWbnBaTTBwd1pFaFdlVmxZVFN0UVIx
cHNXVEpvYUZWdFZtcGlNMHByVUdwQmVrbEdUbXhqUTBGNVRVUkZkMGxFUlRCUGFrVjVUMnBKZWtsRlpFNVdSSGQyV20xV2FtRkhS
bE5hVjA1MlkyMVJLMUJIVW5wVVJ6bHFXVmQ0Y0dSSWF5dFFRemxyWXpCNGRsa3lSbk5oV0ZJMVVHcDRiVnBYVG05WlZWSnNXVE5L
YkdSSE9DdFFRemx0V2xkT2IxbFZVbXhaTTBwc1pFYzRLMUJJVW5CalJ6bFRZMGRTZGxCdGNERmpiV3hyWVZkT2FGQkRPVEJoV0VK
MlZXNUNhMko2TkRoak1qbHpaRzFXZFZreWJHaFNWMDUyWW0wNWRHRlhUbWhRYW5kMll6STVjMlJ0Vm5WWk1teG9VbGRPZG1KdE9Y
UmhWMDVvVUdwNGRsbHRjR3hrUnpsVVlqSk9jRmxYZHl0VFZ6VnRZak5LZEZsWVVuQlpNa1U0VERJNWFXRnRWakJpTVU1MldUSnNh
R0pFTkRoaWJUbDBXVzVLYkZCc1FubGtWMVpwV1ZOQmVsQkRPWFZpTWpGcFkyMVZLMUJIYkd0VlNFcDJaRzFzZFZreWJHaFFha1Y1
VUVNNWNGcEdRbmxpTTFwd1ltMU9jRmxVTkRoYVIxWjZXVEI0ZGxreVJuTmhWMUpvV2tRMVJGRldUbFZTVlhoT1ZEQTBaMUpGVldk
VVJVVm5WVVY0UWxSclJYWlJNRVpVVmtWV1RWUkZPR2RTU1ZWblZFVkZaMVZGZUVKVWEwVTRURVpTYkdNeVRrMWlNazVvWWtkc2Ex
bFhVU3RRUjJSNVpGaENkbEV5ZUdoak1teHRZVmRPYUZreWJIWmlhalZZVUVNNWJtTnVWbmRpTUU1eldWaE9jRnB0YkdwWlYwNXdZ
akkwSzFCSFVucFNSMVpxWTIxV01HSjZORGhNTWxKNlVrZFdhbU50VmpCaWVqUTRXbGN4YUdGWGR5dGpNamsxV1ZjMWJscFhlRUZh
TWpGb1lWZDNkVmt5T1hSUVF6bHNZbGRHY0dKRU5EaGFSMng1V2xkT2FtRlhPWFZRYkVwc1dWZDNaMkpxT0dkTmFrazRUREpTY0dO
dFZtcFpNbXgyWW1vME9HUnRiRzVhVnpWcVlWZEdSR0pIUm5waFYxcHdXVEpHYW1GWE9YVlFiRkU0VEROYWNGb3lWblZaTW14b1VU
SjRhR015YkcxaFYwNW9XVEpzZG1KcU5EaGhWMUp3WWpJeGFGUnRPVEJoVjFwd1dUSkdhbUZYT1hWUWJWWjZVRU01Y0ZwSGJIWmlW
MFpQWWpOU2NGcHRiR3BaVjA1d1lqSTBLMUJET1VaaVIxWjBXbGMxTUZCcWQzWlVNMEpzWW14T1FsWkVORTVEWnowOVBDOUVZWFJo
Um1sc1pUNEtQRVJoZEdGR2FXeGxJSGh0Ykc1elBTSm9kSFJ3T2k4dmQzZDNMbk5yTG1WbEwwUnBaMmxFYjJNdmRqRXVNeTR3SXlJ
Z1EyOXVkR1Z1ZEZSNWNHVTlJa1JGVkVGVVEwaEZSQ0lnUkdsblpYTjBWSGx3WlQwaWMyaGhNU0lnUkdsblpYTjBWbUZzZFdVOUlr
VmpXRTVoU1RSd1QwVnpSMnR0WTAxU2RreHJZek50Y1hwRU9EMGlJRVpwYkdWdWlXMWxQU0pQUTFSdGNEUXhNRFF3TXprNE1UY3pN
RFV5TVRBNE5Ua3ViMlIwSWlCSlpEMGlSREVpSUUxcGJXVlVlWEJsUFNKaGNIQnNNV05oZEdsdmJpOTJibVF1YjJGemFYTXViM0Js
Ym1SdlkzVnRaVzUwTG5SbGVIUWlJRk5wZW1VOUlqVXhNak14SWo0OEwwUmhkR0ZHYVd4bFBnb0tQQzlUYVdkdVpXUkViMk0rPC9E
YXRhPjxTaWduZXI+PFNpZ25lclJvbGU+PENvZGU+RmlybWEgYXV0b21hdGljYTwvQ29kZT48L1NpZ25lclJvbGU+PFNpZ25lcj5G
aXJtYSBhdXRvbWF0aWNhPC9TaWduZXI+PE9yZGVyPjEwPC9PcmRlcj48L1NpZ25lcj48L0RvY3VtZW50Pg==</dss:Base64Data
>
                </dss:TransformedData>
            </dss:InputDocuments>
        </dss:SignRequest>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: Sí (Token de Seguridad – X509IssuerSerial)

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14135365314371124270532">
                <wsu:Created>2014-10-17T09:02:11.438Z</wsu:Created>
                <wsu:Expires>2014-10-17T09:07:11.438Z</wsu:Expires>
            </wsu:Timestamp>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1413536531437-
673913072">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-14135365314413174758 60">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="SOAP-ENV dss ds dst"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>kC+fQ7RcW+6OPuJSx3eeCDv8BT0=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-14135365314371124270532">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
```

```
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsu wsse SOAP-ENV"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>GVUU5zYBZE5R/3skjgv3Laf0mi0=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>NKQfWXfPIeFhdFftz3KUz9cITNLv4d0gt6CX6RANBZ5e2BVvCvpAHPMpNcnJ0wocPgWJdVmMzp9L
nNwTVfR3dzwydqO8y1qelYBnwOCaU0nrfBzExa6/7Q0/oLy/mpbtMl3Dyq/YZkjIZTflUrLE+hBn
Z/4s9jpL+npAv8oA96Cb1G6Z73BB7rQO9Q4FbxpdlC7he7FC98jegaI9Epi5wPiUTWZPR732Nj7c
m4+knDz6Ya3af6vfmz2qq9CA9I+Wu/0y5xVk7/Ckjyb7qh45C7RuNmMTHw7QKPzfTb61U4KfvPkq
p13oKtTdTfV1G4ntLc+7PX4cWIG/xx4s7cTyCQ==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-
14135365314381881305182">
                        <ds:X509Data>
                            <ds:X509IssuerSerial>
                                <ds:X509IssuerName>CN=AfirmaSubCA,OU=Telvent Global
Services,O=Telvent,C=ES</ds:X509IssuerName>
                                <ds:X509SerialNumber>1611735152734479641</ds:X509SerialNumber>
                            </ds:X509IssuerSerial>
                        </ds:X509Data>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-141353653144131747586O">
        <dss:SignResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-52f34e01-41b6-4762-8fee-
6375808eba36">
            <dss:Result>
                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            </dss:Result>
            <dss:SignatureObject>
                <dss:Timestamp>
                    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Id-6d07f306-
d090-4a5e-bb2c-233b3968b17b">
                        <ds:SignedInfo Id="Id-a6b13606-2612-4c6c-8d6d-5e071bb37d92">
                            <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 Id="Id-c00a50b0-c05b-40c9-8a74-d35cc0f4ef10">
                                <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>+VbKci2rOHmHZfsQwmqYKBC1d/Y=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-f42f956f-1f62-480c-8f7e-b4c64a2b1f02"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-afbe4f25-e441-401c-
97bd-54b45498a837">
                                <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>eOou9jPYdFqsAgnJA+/yRLNWeAI=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-b6a514e2-e8a3-4c53-a159-635ce5668bc8"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-b814e7d5-66bb-4b23-
93b0-7e4392622237">
                                <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>sw3S1nc0XWdvtC/q4w5drMwc+ZI=</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>

<ds:SignatureValue>TxNDq0ip4LjldxlQde7mZgLsKbpFqhHwk4q1ZOcbH69nGfhDGHiU8tk6n4hAIvsiCIrb5PdZ6krN
nVy3DTxUVhaTY6iujxKOP35qpfR6qkacIgmc0pHjcDtaN5lmSs6zFGBeVsdN3M9wn1x2Vd+neJg7
Y/1BFzKbObJiegalJqe2x7UPgwnUTAjwdHKZhGYHxhhxdikATXtTodSVJkfZ+TwIAogDyN8CAH6k
cmRrTpCecM8kqG0skG84TWXJILA2GBTeQafqK1/pbjaaRWzagG9DBJRHAjuytoLOjQdVYG+W7l9M
03mAWdJ3O3RTvYiJS99kSBVn4V6ESQMCI/dgFg==</ds:SignatureValue>
                        <ds:KeyInfo>
                            <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1h
U3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50
MQswCQYDVQQGEwJFUzAeFw0xMjEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMM
EVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAwHgYDVQQLDBdUZWx2ZW50IEds
b2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4H
lyxktK6uz6ArGjFM5Bebqz4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/
G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh54cAMZGllNVBbZEHjgBqS9THNO673
GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jDBMPG
V8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+a
WP8CAwEAAaOCAdIwggHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0
My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwm
aXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZpY2VzJTJj
TyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcD
CDAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGR
hoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2Vy
dGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwr
U2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYE
FPW/tms4rvVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabt
w/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6
HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfClWAznM2nejANDSs5
31EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FEl
THVf/ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6
WEj7yoNQzsBrcMV3</ds:X509Certificate>
                            </ds:X509Data>
                        </ds:KeyInfo>
                        <ds:Object Id="TSTInfo-Id-afbe4f25-e441-401c-97bd-54b45498a837"
MimeType="application/xml">
                            <dss:TstInfo>
                                <dss:SerialNumber>1413530041215100068</dss:SerialNumber>
                                <dss:CreationTime>2014-10-17T11:02:11.396+02:00</dss:CreationTime>
                                <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                <dss:Ordered>true</dss:Ordered>
                                <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                            </dss:TstInfo>
                        </ds:Object>
                        <ds:Object Id="TSTInfo-Id-b814e7d5-66bb-4b23-93b0-7e4392622237"
MimeType="application/xml">
                            <dst:PreviousTimestamp
xmlns:dst="urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema#">
                                <dss:Timestamp>
                                    <ds:Signature Id="Id-15b1caf6-e402-4330-84c5-6beec607db89">
                                        <ds:SignedInfo Id="Id-4fed4aed-ec59-4c43-84b0-f85c2cc59cea">
                                            <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 Id="Id-444686e0-2621-45d3-9e82-
11dc67f08bd9">
                                                <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>+VbKci2rOHmHZfsQwmqYKBC1d/Y=</ds:DigestValue>
                                            </ds:Reference>
```

```
                                        <ds:Reference Id="Id-3a73d231-7582-4841-874a-
7b40fa631346" Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-
9cb852b7-3eb8-44e2-b533-fa02b0aa2b48">
                                            <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>u61X/xEWOFTa9owozu/LU33vzW8=</ds:DigestValue>
                                        </ds:Reference>
                                    </ds:SignedInfo>

<ds:SignatureValue>NAm+QvZ1+J+iS6b5fo4wc3L1zOxpDItUS9gfzw0DvbrjoCV6EK+yJBGQuXq1JKD8by68x4P5yLWYtz/i9
EoFVWJljR9uBDitt/wnBpr/AeU6Uuu8X2snGBwYQmJU8dEAxLWezBY+CitpBWT52yA1qNHe08Y3pwUf6xZpnmLE1ssaRT4giHmzb
h34huPPcWIgo/iXmZBZAfjtszQUWcXJFAQdR9Wy59PlBd6lrWpXlWC1ApTVe/gz6gGB0JkPauUl7Ows7qRjO7rIhtNb2pemtEA/6
nmqrCiFf5u2iAUWka3xcgVBUR3DasUFC/KCCLWVvzLP2rMkvboSo+MKHycRyA==</ds:SignatureValue>
                                    <ds:KeyInfo>
                                        <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3Vi
Q0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEy
MDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ251cldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAw
HgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebqz4t
4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh5
4cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jD
BMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwggHO
MIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlz
dC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZp
Y2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEGDAW
gBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAv
ZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVu
dCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4rvVH
7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE0
7uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfC
lWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/ivH
ByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3</ds:X509Certificate>
                                        </ds:X509Data>
                                    </ds:KeyInfo>
                                    <ds:Object Id="TSTInfo-Id-9cb852b7-3eb8-44e2-b533-
fa02b0aa2b48" MimeType="application/xml">
                                        <dss:TstInfo>

<dss:SerialNumber>14135300412151000 66</dss:SerialNumber>
                                            <dss:CreationTime>2014-10-
17T11:02:11.071+02:00</dss:CreationTime>
                                            <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                            <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                            <dss:Ordered>true</dss:Ordered>
                                            <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                                        </dss:TstInfo>
                                    </ds:Object>
                                </ds:Signature>
                            </dss:Timestamp>
                        </dst:PreviousTimestamp>
                    </ds:Object>
                </ds:Signature>
            </dss:Timestamp>
        </dss:SignatureObject>
    </dss:SignResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Ejemplo 9. Solicitud de Renovación de Sello de Tiempo XML

Petición:

- Securización de la Cabecera SOAP: Usuario y Contraseña
- InputDocument: EscapedXML
- Petición Encriptada con Clave Simétrica: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14135368635176649558 53">
                <wsse:Username>a</wsse:Username>
                <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
username-token-profile-1.0#PasswordDigest">****</wsse:Password>
                <wsse:Nonce EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary">CZcHdxpkPjwkBJzxAX1NbIs6</wsse:Nonce>
                <wsu:Created>2014-10-17T09:07:43.518Z</wsu:Created>
            </wsse:UsernameToken>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body>
        <dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:dst="urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema#"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
            <dss:OptionalInputs>
                <dst:RenewTimestamp>
                    <dst:PreviousTimestamp>
                        <dss:Timestamp>
                            <ds:Signature Id="Id-b4af67d3-a0a3-4cea-8e21-6529fb56f06c">
                                <ds:SignedInfo Id="Id-3bce21ae-5df6-40ee-833e-cb188e54d345">
                                    <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 Id="Id-278d411f-56d6-4b6f-b4e4-0710276a8d61">
                                        <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>o/VcDXzRLrDKv4rrh14fDOLbyVY=</ds:DigestValue>
                                    </ds:Reference>
                                    <ds:Reference Id="Id-d3a221fe-5207-4b86-a541-64d95dbd14f6"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-229e48da-7821-4e58-
bb2c-2b38aa88a5ed">
                                        <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>mFHGiuFu4fQdPTy905EOIo8nTzI=</ds:DigestValue>
                                    </ds:Reference>
                                </ds:SignedInfo>

<ds:SignatureValue>ZlWogxdGnCxf2EAUjMYBH69W3AuNIBsXGliSZyK2BcSbM4eqB+9STNLbfJGInY9ztuYYXEvxj2ZqBLM1X
X9GrnnhyP5t08+UXXO1iSKh29FkjhxTO9udoj+VPMWqJw1a9PTJ+sxA3o1F6rLKAKCmcmBV5NAtVi7+KE7dChCM2pa+RqeU4oqUc
DHFmFBXl0vCo0SCKVLfeD1HoWuc5v5vps6t3ZldXsxmiH7V4bTZ3eLHAyytAK1OvHK2iiRECrgIYFBgcCaZWJQMkmlHTpubuQ0p9
sopUAYAWGHC78yqx9vGjk5Sgmx4ME/F3ILzkpxvL1zVN1VLeB3tx3PSp9CyPw==</ds:SignatureValue>
```

```
                                <ds:KeyInfo>
                                    <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3Vi
Q0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEy
MDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAw
HgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebqz4t
4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh5
4cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jD
BMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwggHO
MIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlz
dC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZp
Y2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEGDAW
gBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAv
ZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVu
dCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4rvVH
7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE0
7uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfC
lWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/ivH
ByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3</ds:X509Certifi
cate>
                                    </ds:X509Data>
                                </ds:KeyInfo>
                                <ds:Object Id="TSTInfo-Id-229e48da-7821-4e58-bb2c-2b38aa88a5ed"
MimeType="application/xml">
                                    <dss:TstInfo>
                                        <dss:SerialNumber>1413530041215100072</dss:SerialNumber>
                                        <dss:CreationTime>2014-10-
17T11:07:42.954+02:00</dss:CreationTime>
                                        <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                        <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                        <dss:Ordered>true</dss:Ordered>
                                        <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                                    </dss:TstInfo>
                                </ds:Object>
                            </ds:Signature>
                        </dss:Timestamp>
                    </dst:PreviousTimestamp>
                </dst:RenewTimestamp>

<dss:SignatureType>urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken</dss:SignatureType>
                <dss:ClaimedIdentity>
                    <dss:idAplicacion>appPrueba</dss:idAplicacion>
                </dss:ClaimedIdentity>
            </dss:OptionalInputs>
            <dss:InputDocuments>
                <dss:Document>
                    <dss:EscapedXML>&amp;lt;SOAP-ENV:Envelope xmlns:SOAP-
ENV=&amp;quot;http://schemas.xmlsoap.org/soap/envelope/&amp;quot;&amp;gt;
&amp;lt;SOAP-ENV:Header/&amp;gt;
&amp;lt;SOAP-ENV:Body xmlns:wsu=&amp;quot;http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd&amp;quot; wsu:Id=&amp;quot;XWSSGID-
1389871328322112515102&amp;quot;&amp;gt;
&amp;lt;dss:SignResponse xmlns:dss=&amp;quot;urn:oasis:names:tc:dss:1.0:core:schema&amp;quot;
Profile=&amp;quot;urn:oasis:names:tc:dss:1.0:profiles:timestamping&amp;quot; RequestID=&amp;quot;Id-
1669b7bc-5600-4b8a-9022-29be4f619c9e&amp;quot;&amp;gt;
&amp;lt;dss:Result&amp;gt;
&amp;lt;dss:ResultMajor&amp;gt;urn:oasis:names:tc:dss:1.0:resultmajor:Success&amp;lt;/dss:ResultMajo
r&amp;gt;
&amp;lt;/dss:Result&amp;gt;
&amp;lt;dss:SignatureObject&amp;gt;
&amp;lt;dss:Timestamp&amp;gt;
&amp;lt;dss:RFC3161TimeStampToken&amp;gt;MIAGCSqGSIb3DQEHAqCAMIIHxAIBAzELMAkGBSsOAwIaBQAwZgYLKoZIhvc
NAQkQAQSgVwRVMFMCAQEGBSoDBAUGMCEwCQYFKw4DAhoFAAQUxIiWj/4wjlnkV7FNphsHBW8u9U4CCAHtx3K78/01GA8yMDE0MDE
xNjExMjIwOFowCQIBAoABAYEBAaCCBSswggUnMIIED6ADAgECAggcbqJjqBfPZTANBgkqhkiG9w0BAQUFADBXMRQwEgYDVQQDDAt
BZmlybWFTdWJDQTEgMB4GA1UECwwXVGVsdmVudCBHbG9iYWwgU2VydmljZXMxEDAOBgNVBAoMB1RlbHZlbnQxCzAJBgNVBAYTAkV
TMB4XDTEyMTIwNDEwMDgyMFoXDTE1MTAyNjE1MDQxOFowejEaMBgGA1UEAwwRVHNhU2lnbmVyV2l0aEVLVVQxEDAOBgNVBAsMB1R
lbHZlbnQxIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRswGQYDVQQKDBJTY2huZWlkZXIgRWxlY3RyaWMxCzAJBgN
VBAYTAkVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAh19v59Uvnfvbrtimqf5T4uAMgWT+juc6LgeXLGS0rq7PoCs
aMUzkF5urPi3gaiNZmvAyCvg8k75/Pj7dNH8pN7ivRpFe1UDFUCVBI8Ufu/OqXn8bZ6znD9F3H1f1Sd/rlfZ1z7uGuCunIFglBHf
SEVmoiPcV6HnhwAxkaWU1UFtkQeOAGpL1Mc07rvcZ4pZBkoJ144z0gWSEyiXzaj8R15euaSQ8gEL3BpLDtaahkvYw11p1pKLutCg
+RlYmcWCLmMMEw8ZXyXUHDj1kmoAFtcn5OPvuYrzLeLL0JKDvkiedAPQX2nAr1m/ODkNhJqfJexdXUULyt+alsc9N/5pY/wIDAQA
```

```
Bo4IB0jCCAc4wga0GA1UdLgSBpTCBojCBn6CBnKCBmYaBlmh0dHA6Ly8xNzIuMjEuMjQzLjEwMjo4MDgwL2VqYmNhL3B1YmxpY3dlYi93ZWJkaXN0L2NlcnRkaXN0P2NtZD1kZWx0YWNybCZpc3N1ZXI9Q041M2RBZmlybWFTdWJDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAMBgNVHRMBAf8EAjAAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMB8GA1UdIwQYMBaAFJllOlt2vbfdiw4iwnmMO/ciD1H1MIGlBgNVHR8EgZ0wgZowgZeggZSggZGGgY5odHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlzdC9jZXJ0ZGlzdD9jbWQ9Y3JsJmlzc3Vlcj1DTiUzZEFmaXJtYUNBJTJjT1UlM2RUZWx2ZW50K0dsb2JhbCtTZXJ2aWNlcyUyY08lM2RUZWx2ZW50JTJjQyUzZEVTMA4GA1UdDwEB/wQEAwIE8DAdBgNVHQ4EFgQU9b+2aziu9Ufv7Sk24EUgp0wc2jcwDQYJKoZIhvcNAQEFBQADggEBAGwh3tG8cDixMsjQdWWNpu3D9KE50k4xa5PAJgS+LeueEptWhzs2GkAHATTu5aKIwDTqtaMCSA82zWbi+ocmHRccShEnCXfAq7ofBaVfC/0h+RjewHuCaleiTrO/aqS4ZHot+V53YdvD0TlUf1+TeHYSJY/ql8KVYDOczad6MA0NKznfUSZbtDcKzTZ/zU0EdOOT6ZtilqBPSPAMD0HkFFw3FX5qBfqLsX6IDuV0WGAnpp6bthZiAFzcUSVMdV/+K8cHIJoyjuEMoY+fZm/2+yeuoU+teJLKOyBL+Qp/vxCt/YKQS8PtkrtdFBrqisOXrPO9CbpYSPvKg1DOwGtwxXcxggIZMIICFQIBATBjMFcxFDASBgNVBAMMC0FmaXJtYVN1YkNBMSAwHgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEQMA4GA1UECgwHVGVsdmVudDELMAkGA1UEBhMCRVMCCBxuomOoF891MAkGBSsOAwIaBQCggYwwGgYJKoZIhvcNAQkDMQ0GCyqGSIb3DQEJEAEEMBwGCSqGSIb3DQEJBTEPFw0xNDAxMTYxMTIyMDhaMCMGCSqGSIb3DQEJBDEWBBSvXeJCaTDeBCysifBtTs8iaIetETArBgsqhkiG9w0BCRACDDEcMBowGDAWBBQLLY7tmlbZK+j+cVm+dl2veO92MDANBgkqhkiG9w0BAQEFAASCAQA+hJzYvq+J5VRkyEQjHbLhIrIg4W6YtWwDfWk+a/u0FkHQCoEhsuxNPXFXFh8QWVk/pOe2YosRAxIzM5jMBwTpFOiPAc0/MUP8DXtRFW9+EnqgTj5yEFlbfiYgu+ozAC++oX5K4BfqPDFOmxFtwPdY6uogjCkkSljnQhMyxn+++ZMeo0nWLMNxMzTawOE06mUJaGLpio38GN7ngNgXcBW5SqmtRfzDhXMiJxCFiLCAVhn8vRs1IG9MNSqBwxJLKShib/qhfGKgQe2s96R2Q8F3edyONYpZKajZh6TDnm/SbuhIEMrzJlZnJjM9jMy94bjOo4zygiNrYMtjK8/xwLjEAAAAAA==&amp;lt;/dss:RFC3161TimeStampToken&amp;gt;
&amp;lt;/dss:Timestamp&amp;gt;
&amp;lt;/dss:SignatureObject&amp;gt;
&amp;lt;/dss:SignResponse&amp;gt;
&amp;lt;/SOAP-ENV:Body&amp;gt;
&amp;lt;/SOAP-ENV:Envelope&amp;gt;
                    </dss:EscapedXML>
                </dss:Document>
            </dss:InputDocuments>
        </dss:SignRequest>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: Sí (Token de Seguridad – SAMLToken)


```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413536863642-1827872867">
                <wsu:Created>2014-10-17T09:07:43.716Z</wsu:Created>
                <wsu:Expires>2014-10-17T09:12:43.716Z</wsu:Expires>
            </wsu:Timestamp>
            <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:exc14n="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:xs="http://www.w3.org/2001/XMLSchema" AssertionID="1413536863643" IssueInstant="2014-10-17T11:07:43.643+02:00" Issuer="CN=AfirmaSubCA,OU=Telvent Global Services,O=Telvent,C=ES" MajorVersion="1" MinorVersion="1">
                <saml:Conditions NotBefore="2014-10-17T10:07:43.643+02:00" NotOnOrAfter="2014-10-17T12:07:43.643+02:00"/>
                <saml:AttributeStatement>
                    <saml:Subject>
                        <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">CN=AfirmaSubCA,OU=Telvent Global Services,O=Telvent,C=ES</saml:NameIdentifier>
                        <saml:SubjectConfirmation>
                            <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-key</saml:ConfirmationMethod>
                            <ds:KeyInfo xmlns:ns5="http://www.w3.org/2001/XMLSchema-instance" ns5:type="keyInfo">
                                <ds:KeyValue>
                                    <ds:RSAKeyValue>

<ds:Modulus>kch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0ptsmAVJ9OJ7D2gMvPgQNJEOshdFyG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MPxKb4NZm5fFd1LGApXNEPZ0OCOxpGkIMwn/Yk
```

```
HSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0aWqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u6+GuHKijZ5LUeVrSpjcRq9Nhp
+gVvqnaxVlmeRgG7C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQ==</ds:Modulus>
                                        <ds:Exponent>AQAB</ds:Exponent>
                                    </ds:RSAKeyValue>
                                </ds:KeyValue>
                            </ds:KeyInfo>
                        </saml:SubjectConfirmation>
                    </saml:Subject>
                </saml:AttributeStatement>
                <ds:Signature>
                    <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="#1413536863643">
                            <ds:Transforms>
                                <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                <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>f/qeTs/SnbshJbCuNmrzlWP4a2o=</ds:DigestValue>
                        </ds:Reference>
                    </ds:SignedInfo>

<ds:SignatureValue>ej23Ddgezbr8d76U1LYrShnaKMTLSF5HOvEjZoO+hKOpPdv7zQft4Zc9+xn8GyfjGBPaeyZCBd81
69yLUx96ycKvE/s6DrrnC2isIFQgupCAclTNQmUakxpifvXmUs+XBuJAu/xvcsvjElaZADts6aLJ
KVHiK9ou0b/MAcxx4zepLP2bVUDVO8p71ba/qNjo5lOfKAfA5qDSI9CtBIBL8IQFp3L3jkaDKW1v
obm+sGSdoMDRfmMaHdntI3NhtWPjfWGqcwjjBJ5PilqC7/klzowpnr+ReaLfWLyqC8Ym6qBNnLOC
isVLNDKRQ54epy/rOCrazuQCYM0iwuEvD41LIQ==</ds:SignatureValue>
                    <ds:KeyInfo>
                        <ds:KeyValue>
                            <ds:RSAKeyValue>

<ds:Modulus>kch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0ptsmAVJ9OJ7D2gM
vPgQNJEOshdFyG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MP
xKb4NZm5fFd1LGApXNEPZ0OCOxpGkIMwn/YkHSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0a
WqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u6+GuHKijZ5LUeVrSpjcRq9Nhp+gVvqnaxVlmeRgG7
C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQ==</ds:Modulus>
                                        <ds:Exponent>AQAB</ds:Exponent>
                                    </ds:RSAKeyValue>
                                </ds:KeyValue>
                            </ds:KeyInfo>
                </ds:Signature>
            </saml:Assertion>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-
14135368636424049616 73">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413536863681-1512947811">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>ygutKGZDj0RWAFoZh7aK5HaFvbk=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>gecbz2/EFDrcUtHMDDS0ej3DRqI1ORAj4PXv1009WEADm9XAHavMyUTN8XNUu1KJ0Z0g6v4zxp2z
oEZE/YYj1BtP89bhn23QzlkaCQwb40RMsEzXcdztiliRkGvOLQt4ULDtr7MlPOg1y1V/wlN1/+6o
WJjpudHv3m7bsOAnr9yw53Nr/f8KjnBNRyKk7L2rFp7ASj2+gNqAIw+GQ6dq0+Maa24BSrbWE2MN
WCQGr+npQ6pVpWF/KLIfaPnWmHOOp45g0FP0o3S8jCiFWa1ggzvzqqKsHY33hpjoyNrF0IfgsyFc
c5aIYGlDn2ER9WzL1tqBzpbGui2diPRzrDXqmA==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-
wss-wssecurity-secext-1.1.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.1#SAMLV1.1" wsu:Id="XWSSGID-1413536863680189893976">
                        <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-
saml-token-profile-1.0#SAMLAssertionID">1413536863643</wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
                </ds:KeyInfo>
            </ds:Signature>
```

```
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413536863681-1512947811">
        <dss:SignResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema" Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-8ebb407d-b512-4237-9050-1dece39319a8">
            <dss:Result>
                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            </dss:Result>
            <dss:SignatureObject>
                <dss:Timestamp>
                    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Id-e58c9a93-21b8-4008-94d2-ebf435c7a8b0">
                        <ds:SignedInfo Id="Id-7eed2c2d-01b9-447c-b734-dbabb0601e78">
                            <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 Id="Id-a6719e5e-73ec-4e4e-960d-323dfca9f3ab">
                                <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>o/VcDXzRLrDKv4rrh14fDOLbyVY=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-946197e8-96f4-4d18-bc84-01d20f619d61" Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-1bf9ad15-534d-4fb6-a0d1-94221972cb2c">
                                <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>BvAoj92p2M15sMLJgjHgWJpL8JU=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-3145dabd-81df-44bc-9e63-061b3577fd72" Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-2e1ea419-c425-45fe-afb3-08499823d12b">
                                <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>8RBqmv0LdUVUKZksaMDjwdSxcpY=</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>

<ds:SignatureValue>T61CAXrem3nslcrW487tOkmX88KrNK4r7jI8Indh/yNyOTwybwuZTaFAE6VwScoxQZkhKmX55HCw
8w0a9lcthrBR6gieoPK6u/AuPNbJ8KK8wNR32dfhwD0AJsQwZVeg7AmtLVf0TVHQWs2rrmhXMpCm
HkEnIrhUGb/7R+oivnLv5Dofmzm0gEwv/c1KMLPwlIDiL624ceuS9IP1Q2mjFprmSTyaTarhkxmW
R77Wk5BdxRvh8Aui/6T0qXgdQ7OZVJpAJds/CQHZpK5ToELOFuYSSKnozv7+gDa1TWJs+/XMZnnB
ve1ftPLATpwRZqaR/zBE+a3qfwS5hZSUiX0N6A==</ds:SignatureValue>
                        <ds:KeyInfo>
                            <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1h
U3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50
MQswCQYDVQQGEwJFUzAeFw0xMjEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMM
EVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAwHgYDVQQLDBdUZWx2ZW50IEds
b2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4H
lyxktK6uz6ArGjFM5Bebqz4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/
G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh54cAMZGllNVBbZEHjgBqS9THNO673
GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jDBMPG
V811Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+a
WP8CAwEAAaOCAdIwggHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0
My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwm
aXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZpY2VzJTJj
TyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcD
```

```
CDAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGR
hoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2Vy
dGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwr
U2VydmljZXMlMnNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYE
FPW/tms4rvVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabt
w/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6
HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfClWAznM2nejANDSs5
31EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FEl
THVf/ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6
WEj7yoNQzsBrcMV3</ds:X509Certificate>
                        </ds:X509Data>
                    </ds:KeyInfo>
                    <ds:Object Id="TSTInfo-Id-1bf9ad15-534d-4fb6-a0d1-94221972cb2c"
MimeType="application/xml">
                        <dss:TstInfo>
                            <dss:SerialNumber>14135300412151000074</dss:SerialNumber>
                            <dss:CreationTime>2014-10-17T11:07:43.601+02:00</dss:CreationTime>
                            <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                            <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                            <dss:Ordered>true</dss:Ordered>
                            <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                        </dss:TstInfo>
                    </ds:Object>
                    <ds:Object Id="TSTInfo-Id-2e1ea419-c425-45fe-afb3-08499823d12b"
MimeType="application/xml">
                        <dst:PreviousTimestamp
xmlns:dst="urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema#">
                            <dss:Timestamp>
                                <ds:Signature Id="Id-b4af67d3-a0a3-4cea-8e21-6529fb56f06c">
                                    <ds:SignedInfo Id="Id-3bce21ae-5df6-40ee-833e-cb188e54d345">
                                        <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 Id="Id-278d411f-56d6-4b6f-b4e4-
0710276a8d61">
                                            <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>o/VcDXzRLrDKv4rrh14fDOLbyVY=</ds:DigestValue>
                                        </ds:Reference>
                                        <ds:Reference Id="Id-d3a221fe-5207-4b86-a541-
64d95dbd14f6" Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-
229e48da-7821-4e58-bb2c-2b38aa88a5ed">
                                            <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>mFHGiuFu4fQdPTy905EOIo8nTzI=</ds:DigestValue>
                                        </ds:Reference>
                                    </ds:SignedInfo>

<ds:SignatureValue>ZlWogxdGnCxf2EAUjMYBH69W3AuNIBsXGliSZyK2BcSbM4eqB+9STNLbfJGInY9ztuYYXEvxj2ZqBLM1X
X9GrnnhyP5t08+UXXO1iSKh29FkjhxTO9udoj+VPMWqJw1a9PTJ+sxA3o1F6rLKAKCmcmBV5NAtVi7+KE7dChCM2pa+RqeU4oqUc
DHFmFBXl0vCo0SCKVLfeD1HoWuc5v5vps6t3ZldXsxmiH7V4bTZ3eLHAyytAK1OvHK2iiRECrgIYFBgcCaZWJQMkmlHTpubuQ0p9
sopUAYAWGHC78yqx9vGjk5Sgmx4ME/F3ILzkpxvL1zVN1VLeB3tx3PSp9CyPw==</ds:SignatureValue>
                                    <ds:KeyInfo>
                                        <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU3Vi
Q0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xMjEy
MDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ251cldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAw
HgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebqz4t
4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh5
4cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jD
```

```
BMPGV8l1Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwggHO
MIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlz
dC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZp
Y2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEGDAW
gBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAv
ZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVu
dCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4rvVH
7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE0
7uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfC
lWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/ivH
ByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3</ds:X509Certificate>
                                        </ds:X509Data>
                                    </ds:KeyInfo>
                                    <ds:Object Id="TSTInfo-Id-229e48da-7821-4e58-bb2c-2b38aa88a5ed" MimeType="application/xml">
                                        <dss:TstInfo>

<dss:SerialNumber>14135300412151000 72</dss:SerialNumber>
                                            <dss:CreationTime>2014-10-17T11:07:42.954+02:00</dss:CreationTime>
                                            <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                            <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                            <dss:Ordered>true</dss:Ordered>
                                            <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                                        </dss:TstInfo>
                                    </ds:Object>
                                </ds:Signature>
                            </dss:Timestamp>
                        </dst:PreviousTimestamp>
                    </ds:Object>
                </ds:Signature>
            </dss:Timestamp>
        </dss:SignatureObject>
    </dss:SignResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Ejemplo 10. Solicitud de Renovación de Sello de Tiempo ASN.1

Petición:

- Securización de la Cabecera SOAP: Usuario y Contraseña
- InputDocument: Base64Data
- Petición Encriptada con Clave Simétrica: No

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413537282938147750192 7">
                <wsse:Username>a</wsse:Username>
                <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
username-token-profile-1.0#PasswordDigest">****</wsse:Password>
                <wsse:Nonce EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary">16x6ypCEb8Ru2SFjeqfBuG+w</wsse:Nonce>
                <wsu:Created>2014-10-17T09:14:42.939Z</wsu:Created>
            </wsse:UsernameToken>
        </wsse:Security>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body>
        <dss:SignRequest xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:dst="urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema#"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping">
            <dss:OptionalInputs>
                <dst:RenewTimestamp>
                    <dst:PreviousTimestamp>
                        <dss:Timestamp>

<dss:RFC3161TimeStampToken>MIAGCSqGSIb3DQEHAqCAMIIHyAIBAzELMAkGBSsOAwIaBQAwagYLKoZIhvcNAQkQAQSgWwRZM
FcCAQEGBSoDBAUGMCEwCQYFKw4DAhoFAAQUySErJYEqdFwOFyp2icgkiDF/MiQCCBOd3hVR+CStGBMyMDE0MTAxNzA5MTQ0Mi42N
jZaMAkCAQKAAQGBAQGgggUrMIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU
3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xM
jEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50M
SAwHgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFU
zCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebq
z4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3F
eh54cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi
5jDBMPGV8llBw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwg
gHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZ
GlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1Nlc
nZpY2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEG
DAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwO
DAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q041M2RBZmlybWFDQSUyY09VJTNkVGVsd
mVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4r
vVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpAB
wE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6
pfClWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA71dFhgJ6aem7YWYgBc3FElTHVf/
ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3MYICGTCCAhUCA
QEwYzBXMRQwEgYDVQQDDAtBZmlybWFTdWJDQTEgMB4GA1UECwwXVGVsdmVudCBHbG9iYWwgU2VydmljZXMxEDAOBgNVBAoMB1Rlb
HZlbnQxCzAJBgNVBAYTAkVTAggcbqJjqBfPZTAJBgUrDgMCGgUAoIGMMBoGCSqGSIb3DQEJAzENBgsqhkiG9w0BCRABBDAcBgkqh
kiG9w0BCQUxDxcNMTQxMDE3MDkxNDQyWjAjBgkqhkiG9w0BCQQxFgQUDS3RtI3l8qZlzg2rA+lWrHxmxyswKwYLKoZIhvcNAQkQA
gwxHDAaMBgwFgQUCy2O7ZpW2Svo/nFZvnZdr3jvdjAwDQYJKoZIhvcNAQEBBQAEggEACAVX0G6bTN6krMdd/iJV4R8LPnmJGoWig
bReJ5M+UubHKXgFqmAmeX/+a7Ru9EeyOOTwZNwhjmr8sbFuFplIicOKukdNrYAPurDD+CAIYqeIcxcmO7y8Q20UeifSi/vxNCZv8
ZhWPrQPwv2AQJ4gECHyomUZ3B1AeEtUwbZgGVZSrGO7f+x2ADw1HGA7Wn9qUIKsu5SjUY2+vUWxWp2ffhQn1K/QS3wD4LAY+2DHX
vAb9ftq1RFFBgW4mUQZbHQnm3P6Uc8wtt3h70y7LRMgbAd/8vcaRbsSLqZNR4WYChgkcZGiqoVb0iZroC5idSWv0Ky2fbs/6GLTe
U0XwCogAgAAAAA=</dss:RFC3161TimeStampToken>
                        </dss:Timestamp>
                    </dst:PreviousTimestamp>
                </dst:RenewTimestamp>

<dss:SignatureType>urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken</dss:SignatureType>
```

```
            <dss:ClaimedIdentity>
                <dss:idAplicacion>appPrueba</dss:idAplicacion>
            </dss:ClaimedIdentity>
        </dss:OptionalInputs>
        <dss:InputDocuments>
            <dss:Document>

<dss:Base64Data>RmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFu
IG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNl
cnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVh
bGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRp
bGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmlj
aGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywg
byBjb3VudGVyLg0KR
```

IG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNl
cnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXIgZmlybWFzIHNl
bGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRp
bGl6YXLhIHBhcmEgcmVhbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmlj
aGVybyBxdWUgc2UgdXRpbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmlj
byBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFuIG5vcm1hbGVzLCBjbywg
IG5vcm1hbGVzLCBjbywgbyBjb3VudGVyLg0KRmljaGVybyBxdWUgc2UgdXRpbGl6YXIgZmlybWFzIHNlcnZpZG9yLCB5YSBzZWFu

Respuesta:

- Respuesta Encriptada con Clave Simétrica: No
- Respuesta Firmada: Sí (Token de Seguridad – BinarySecurityToken)

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">
            <wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-14135372830346068801 6">
                <wsu:Created>2014-10-17T09:14:43.034Z</wsu:Created>
                <wsu:Expires>2014-10-17T09:19:43.034Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:BinarySecurityToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" 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="XWSSGID-
14135372830341090173138">MIIFRTCCBC2gAwIBAgIIFl4IlQK/pRkwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1
hU3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0
xMjEwMjMxMzAwMjJaFw0xNTEwMjYxNTA0MThaMHMxEzARBgNVBAMMClNvYXBTaWduZXIxEDAOBgNVBAsMB1RlbHZlbnQxIDAeBgN
VBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRswGQYDVQQKDBJTY2huZWlkZXIgRWxlY3RyaWMxCzAJBgNVBAYTAkVTMIIBIjA
NBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkch+w0POYwAcqaOcmhm26pTnEdv6lS+dyQNZEXjeLGgGwrSJcMFB8MCwmsW+0pt
smAVJ9OJ7D2gMvPgQNJEOshdFyG6pal6EalEwLOtb81OM84MFoGY4xQrhrQY5uoVcGNZBi/c3FRZ3LndaYnBMV4MPxKb4NZm5fFd
1LGApXNEPZ0OCOxpGkIMwn/YkHSe4eGtnblzYpJdT2vhsp/YL2dQW4C79PGvgiI0aWqBRkZtLW43EwKbHA93J4g5RlypcP93dN8u
6+GuHKijZ5LUeVrSpjcRq9Nhp+gVvqnaxVlmeRgG7C9FYnEEukHmcT1Nt1vpoKjoPUp4W8l+o6cU5DQIDAQABo4IB9zCCAfMwga0
GA1UdLgSBpTCBojCBn6CBnKCBmYaBlmh0dHA6Ly8xNzIuMjEuMjQzLjEwMjo4MDgwL2VqYmNhL3B1YmxpY3dlYi93ZWJkaXN0L2N
lcnRkaXN0P2NtZD1kZWx0YWNybCZpc3N1ZXI9Q04lM2RBZmlybWFTdWJDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2Vydmljj ZXM
lMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAMBgNVHRMBAf8EAjAAMDsGA1UdJQQ0MDIGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQU
HAwQGCCsGAQUFBwMIBggrBgEFBQcDCTAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIG
UoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZ
pc3N1ZXI9Q04lM2RBZmlybWFFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwrU2Vydmlj ZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzA
OBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFAIYOhNZWFgafngAgs9tQ74e2yeYMA0GCSqGSIb3DQEBBQUAA4IBAQBmeMs+UdPMWY5
Icyn97ZR//LOfk6ElAfgxRs1y6DH1oJdiWUnVkHmSgGNY+Y4j4y74TMiH25naizyyKQzmGoHw7KOgTxxqUEwlEHZPuf5GIJxc+/a
0askEItRRgf9pozjL2+RS4YMU33xJlyBZNQ4nrvlKyNx50favpiKD2kOuHFqu3CypQzEvWw8uW5RY6Vvmujc3pztwjZtMeatWTbx
MS8+c4wfT7N5bgRFCH3t/Wu/yhKQlnfkXGLdpOeIt2pxIKH15UR7ODMmlNcIIRJQPoCPm5PWPmo24BkTb5U+nr1y4I5yY/gkIOam
mYYORPb10i1vx9bRX1llTnWg4/YNX</wsse:BinarySecurityToken>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="XWSSGID-1413537283034-
386534705">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsse SOAP-ENV"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#XWSSGID-1413537283036-1543069545">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="SOAP-ENV dss ds dst"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>SXQvt1f2hgeDZr8VifStlN2Srjw=</ds:DigestValue>
                    </ds:Reference>
                    <ds:Reference URI="#XWSSGID-14135372830346068801 6">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <InclusiveNamespaces xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="wsu wsse SOAP-ENV"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>ohzoua0k17VnS41GcUCWnD8cV78=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>

<ds:SignatureValue>ADAiJvDfjI8gxhFDbBny7kxgyPRV/EHKIQXGMq4FYImaNH6n0GqpnZDPtIYjkSGCLKIZKDvg+bKJ
wJeB0ski57kZOBj8VWS9W1ahFwIsVaerrl/pj3KurZ/yOqCmrOo34oXNATZU0ceUifszYFDOvfYL
Ml5Ed+75BzdP/eIJF/h8ANELj054am8t+uneSGy8vvGHZwRMQSe1jHUUZXdqMbrK1QHws5FgEmjJ
```

```
0MQy0mmi6F6b2d9WIqEz5JJA0Jb3Es70/TYfnx5XZMHRsIcgWZqx5IkPp2FoI09TMd+nTmMKelco
PNiRgYHEDCh1cyGhMZzMRKXtye5z2lna51JDJQ==</ds:SignatureValue>
                <ds:KeyInfo>
                    <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="XWSSGID-1413537283035-
1916754366">
                        <wsse:Reference URI="#XWSSGID-14135372830341090173138"
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>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="XWSSGID-1413537283036-1543069545">
        <dss:SignResponse xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"
Profile="urn:oasis:names:tc:dss:1.0:profiles:timestamping" RequestID="Id-90a8c734-eb35-4617-a7e8-
81ecf48bd13b">
            <dss:Result>
                <dss:ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</dss:ResultMajor>
            </dss:Result>
            <dss:SignatureObject>
                <dss:Timestamp>
                    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Id-af0d62c0-
128b-4fdf-b6c1-dd23a92714a5">
                        <ds:SignedInfo Id="Id-a749ef92-52fe-476b-8226-86b32808770e">
                            <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 Id="Id-1b76f8a5-644e-4704-b832-070dd3e3527b">
                                <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <ds:DigestValue>ySErJYEqdFwOFyp2icgkiDF/MiQ=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-84f3ea1b-f748-487d-a946-c74fbe7eebfe"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-eb2b9043-b5df-45ef-
a6d4-ac55c7e768b8">
                                <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>lq277xRqsDvQwjv2VIzJb7gvpAM=</ds:DigestValue>
                            </ds:Reference>
                            <ds:Reference Id="Id-65dfdfc9-174a-4072-a75f-4f6a48f1a2a9"
Type="urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken" URI="#TSTInfo-Id-30304b9f-3e95-4b62-
b813-181462225567">
                                <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>I1r+7I43FDpcvzjmZ0VWO9X4d/U=</ds:DigestValue>
                            </ds:Reference>
                        </ds:SignedInfo>

<ds:SignatureValue>cj3Gs/b/FFcVfiobZA0UL0xlp1FQYXm00w4AOlSqxHJBGvaxcuRFvzPJPA+/y4Btx/6HJR2g0XiR
fkYlbf1QIm9Yl9vT6uYR2nUbFPFByrZqDyTgV/Dtd1HyIF0V8p39TFeqTAScHEF156/fSdbM/Ffg
Kvto3SPPiFURCF7EvgCJh9q0N0Rf+toIcSubB2261yfDDd2rrZN960By0xjYFbA6xjDKmAZspK1X
sAggas9LwC9UekUBmnAdhHCkva+SqGPS4g9mU7iR4CBK7Mdmepy8Z27pcB1reUQ9u6XHDmhocMI0
o/DG8HjMJw2MVByOCWeBxk9V8xREgZlDwt6JJg==</ds:SignatureValue>
                        <ds:KeyInfo>
                            <ds:X509Data>

<ds:X509Certificate>MIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1h
U3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50
MQswCQYDVQQGEwJFUzAeFw0xMjEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMM
EVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50MSAwHgYDVQQLDBdUZWx2ZW50IEds
b2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFUzCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4H
lyxktK6uz6ArGjFM5Bebqz4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/
```

```
G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3Feh54cAMZGllNVBbZEHjgBqS9THNO673
GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi5jDBMPG
V811Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+a
WP8CAwEAAaOCAdIwggHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0
My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZGlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwm
aXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1NlcnZpY2VzJTJj
TyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcD
CDAfBgNVHSMEGDAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGR
hoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwODAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2Vy
dGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsdmVudCtHbG9iYWwr
U2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYE
FPW/tms4rvVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabt
w/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpABwE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6
HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6pfClWAznM2nejANDSs5
31EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FEl
THVf/ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6
WEj7yoNQzsBrcMV3</ds:X509Certificate>
                                </ds:X509Data>
                            </ds:KeyInfo>
                            <ds:Object Id="TSTInfo-Id-eb2b9043-b5df-45ef-a6d4-ac55c7e768b8"
MimeType="application/xml">
                                <dss:TstInfo>
                                    <dss:SerialNumber>14135300412151000079</dss:SerialNumber>
                                    <dss:CreationTime>2014-10-17T11:14:42.994+02:00</dss:CreationTime>
                                    <dss:Policy>urn:oid:1.2.3.4.5.6</dss:Policy>
                                    <dss:ErrorBound>PT2.001001S</dss:ErrorBound>
                                    <dss:Ordered>true</dss:Ordered>
                                    <dss:TSA Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">CN=Timestamp_Policy,O=RICOH,OU=ITA,ST=Sevilla,L=Sevilla,C=ES</dss:TSA>
                                </dss:TstInfo>
                            </ds:Object>
                            <ds:Object Id="TSTInfo-Id-30304b9f-3e95-4b62-b813-181462225567"
MimeType="application/xml">
                                <dst:PreviousTimestamp
xmlns:dst="urn:oasis:names:tc:dss:1.0:profiles:TimeStamp:schema#">
                                    <dss:Timestamp>

<dss:RFC3161TimeStampToken>MIAGCSqGSIb3DQEHAqCAMIIHyAIBAzELMAkGBSsOAwIaBQAwagYLKoZIhvcNAQkQAQSgWwRZM
FcCAQEGBSoDBAUGMCEwCQYFKw4DAhoFAAQUySErJYEqdFwOFyp2icgkiDF/MiQCCBOd3hVR+CStGBMyMDE0MTAxNzA5MTQ0Mi42N
jZaMAkCAQKAAQGBAQGgggUrMIIFJzCCBA+gAwIBAgIIHG6iY6gXz2UwDQYJKoZIhvcNAQEFBQAwVzEUMBIGA1UEAwwLQWZpcm1hU
3ViQ0ExIDAeBgNVBAsMF1RlbHZlbnQgR2xvYmFsIFNlcnZpY2VzMRAwDgYDVQQKDAdUZWx2ZW50MQswCQYDVQQGEwJFUzAeFw0xM
jEyMDQxMDA4MjBaFw0xNTEwMjYxNTA0MThaMHoxGjAYBgNVBAMMEVRzYVNpZ25lcldpdGhFS1VUMRAwDgYDVQQLDAdUZWx2ZW50M
SAwHgYDVQQLDBdUZWx2ZW50IEdsb2JhbCBTZXJ2aWNlczEbMBkGA1UECgwSU2NobmVpZGVyIEVsZWN0cmljMQswCQYDVQQGEwJFU
zCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIdfb+fVL537267Ypqn+U+LgDIFk/o7nOi4HlyxktK6uz6ArGjFM5Bebq
z4t4GojWZrwMgr4PJO+fz4+3TR/KTe4r0aRXtVAxVAlQSPFH7vzql5/G2es5w/Rdx9X9Unf65X2dc+7hrgrpyBYJQR30hFZqIj3F
eh54cAMZGllNVBbZEHjgBqS9THNO673GeKWQZKCdeOM9IFkhMol82o/EdeXrmkkPIBC9waSw7WmoZL2MNdadaSi7rQoPkZWJnFgi
5jDBMPGV811Bw49ZJqABbXJ+Tj77mK8y3iy9CSg75InnQD0F9pwK9Zvzg5DYSanyXsXV1FC8rfmpbHPTf+aWP8CAwEAAaOCAdIwg
gHOMIGtBgNVHS4EgaUwgaIwgZ+ggZyggZmGgZZodHRwOi8vMTcyLjIxLjI0My4xMDI6ODA4MC9lamJjYS9wdWJsaWN3ZWIvd2ViZ
GlzdC9jZXJ0ZGlzdD9jbWQ9ZGVsdGFjcmwmaXNzdWVyPUNOJTNkQWZpcm1hU3ViQ0ElMmNPVSUzZFRlbHZlbnQrR2xvYmFsK1Nlc
nZpY2VzJTJjTyUzZFRlbHZlbnQlMmNDJTNkRVMwDAYDVR0TAQH/BAIwADAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAfBgNVHSMEG
DAWgBSZZTpbdr233YsOIsJ5jDv3Ig9R9TCBpQYDVR0fBIGdMIGaMIGXoIGUoIGRhoGOaHR0cDovLzE3Mi4yMS4yNDMuMTAyOjgwO
DAvZWpiY2EvcHVibGljd2ViL3dlYmRpc3QvY2VydGRpc3Q/Y21kPWNybCZpc3N1ZXI9Q04lM2RBZmlybWFDQSUyY09VJTNkVGVsd
mVudCtHbG9iYWwrU2VydmljZXMlMmNPJTNkVGVsdmVudCUyY0MlM2RFUzAOBgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFPW/tms4r
vVH7+0pNuBFIKdMHNo3MA0GCSqGSIb3DQEBBQUAA4IBAQBsId7RvHA4sTLI0HVljabtw/ShOdJOMWuTwCYEvi3rnhKbVoc7NhpAB
wE07uWiiMA06rWjAkgPNs1m4vqHJh0XHEoRJwl3wKu6HwWlXwv9IfkY3sB7gmpXok6zv2qkuGR6Lfled2Hbw9E5VH9fk3h2EiWP6
pfClWAznM2nejANDSs531EmW7Q3Cs02f81NBHTjk+mbYpagT0jwDA9B5BRcNxV+agX6i7F+iA7ldFhgJ6aem7YWYgBc3FElTHVf/
ivHByCaMo7hDKGPn2Zv9vsnrqFPrXiSyjsgS/kKf78Qrf2CkEvD7ZK7XRQa6orDl6zzvQm6WEj7yoNQzsBrcMV3MYICGTCCAhUCA
QEwYzBXMRQwEgYDVQQDDAtBZmlybWFTdWJDQTEgMB4GA1UECwwXVGVsdmVudCBHbG9iYWwgU2VydmljZXMxEDAOBgNVBAoMB1Rlb
HZlbnQxCzAJBgNVBAYTAkVTAggcbqJjqBfPZTAJBgUrDgMCGgUAoIGMMBoGCSqGSIb3DQEJAzENBgsqhkiG9w0BCRABBDAcBgkqh
kiG9w0BCQUxDxcNMTQxMDE3MDkxNDQyWjAjBgkqhkiG9w0BCQQxFgQUDS3RtI3l8qZlzg2rA+lWrHxmxyswKwYLKoZIhvcNAQkQA
gwxHDAaMBgwFgQUCy2O7ZpW2Svo/nFZvnZdr3jvdjAwDQYJKoZIhvcNAQEBBQAEggEACAVX0G6bTN6krMdd/iJV4R8LPnmJGoWig
bReJ5M+UubHKXgFqmAmeX/+a7Ru9EeyOOTwZNwhjmr8sbFuFplIicOKukdNrYAPurDD+CAIYqeIcxcmO7y8Q20UeifSi/vxNCZv8
ZhWPrQPwv2AQJ4gECHyomUZ3B1AeEtUwbZgGVZSrGO7f+x2ADw1HGA7Wn9qUIKsu5SjUY2+vUWxWp2ffhQn1K/QS3wD4LAY+2DHX
vAb9ftq1RFFBgW4mUQZbHQnm3P6Uc8wtt3h70y7LRMgbAd/8vcaRbsSLqZNR4WYChgkcZGiqoVb0iZroC5idSWv0Ky2fbs/6GLTe
U0XwCogAgAAAAA=</dss:RFC3161TimeStampToken>
                                    </dss:Timestamp>
                                </dst:PreviousTimestamp>
                            </ds:Object>
                        </ds:Signature>
                    </dss:Timestamp>
                </dss:SignatureObject>
            </dss:SignResponse>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

A.4 Guía 807 del Esquema Nacional de Seguridad (ENS).

Les comunicamos que los productos de la Suite de @firma pueden contener entre los algoritmos disponibles, algunos no recomendados por la Guía 807 del Esquema Nacional de Seguridad (ENS; editada por el Centro Criptológico Nacional, CCN) vigente en el momento de publicación de este documento. Por lo que queda bajo la responsabilidad de las aplicaciones que hacen uso de estos productos el configurar adecuadamente las llamadas a los mismos para generar el resultado esperado, válido y adecuado para ese momento y el nivel de seguridad deseado, utilizando para ello algoritmos de la familia SHA-2 tal y como especifica dicha norma para la generación de firmas electrónicas.

Pueden consultar la norma vigente en el siguiente enlace:

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html