face
PUNTO GENERAL DE ENTRADA
DE FACTURAS ELECTRÓNICAS

Documentación de integración y recomendaciones de uso en FACe

Equipo de desarrollo de la plataforma FACe

Versión 1.0.2

Esta página se ha dejado vacía a propósito

Índice de contenidos

Esta página se ha dejado vacía a propósito

Capítulo 1

Introducción

1.1 Historial de versiones del documento

Versión	Fecha	Descripción de los cambios
1.0.0	24/ 11/ 2014	Inicio del documento
1.0.1	22/ 12/ 2014	Se incluyen los certificados clase 3 para WS
1.0.2	26/ 01/ 2015	Modificacion de los limites de POST e indicacion de los atributos necesarios para emision de certificados correctos para fima de factura

1.2 Objetivo de este documento

Este documento tiene como objetivo informar sobre ciertos aspectos que se deben cumplir para una integración y uso correcto.

Esta página se ha dejado vacía a propósito

Capítulo 2

Comunicación e integración con los Web Services de FACe.

2.1 Protocolos SSL y TLS

El unico protocolo admitido es TLS>=1.0

NOTA: para aquellos integradores en Java 6, por defecto usa SSLv3 y el handshake falla. Especificar en el arranque la opcion -Dhttps.protocols="TLSv1"

2.2 Server Name Indication (SNI)

El único acceso permitido es por nombre, no es posible acceso únicamente por ip. SNI es una extensión del protocolo TLS.1. Se requiere soporte de la extensión SNI en el navegador o cliente. Los usuarios cuyos navegador no soporte SNI podrán recibir advertencias de seguridad por no coincidencia de nombre de certificado con el de servicio. La mayor parte de los sistemas operativos, navegadores y clientes actuales, soportan SNI, en caso de duda, puede comprobar la compatibilidad de su cliente o navegador en wikipedia articulo sobre SNI (http://es.wikipedia.org/wiki/Server_Name_Indication) .

A partir de noviembre de 2012, los únicos grandes bases de usuarios cuyos navegadores no soportan SNI son de Android 2.x (navegador predeterminado), Internet Explorer en Windows XP y versiones de Java antes de 1.7 en cualquier sistema operativo.

2.3 Confianza en Certifcados FNMT Clase 2 CA

Los certificados empleados por el servicio son "FNMT Clase 2 CA". Para evitar problemas con los certificados, se requiere que el navegador o cliente, confíe en los certificados emitidos por dicha CA. Por defecto, algunos navegadores, no confían en este certificado, por lo que ha de añadirse manualmente. Si el cliente es Java, este certificado hay que añadirlo al correspondiente truststore.

Puede obtenerse este certificado en (https://www.sede.fnmt.gob.es/documents/11614/116099/FNMTClase2CA.cer/29de1646-675e-49b3-bd8e-0ff6ca02cb66) . Además de este certificado, y en previsión de su sustitución, se recomienda añadir el certificado "AC Raíz FNMT-RCM (SHA2)", descargable en (https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Raiz_FNMT-RCM_SHA256.cer/b1447e06-9927-45b7-92cc-8690edd7562d) ya que los certificados más recientes se vienen emitiendo desde esta CA.

En ambos casos, ya sea en navegador o en cliente, la confianza requerida para estos certificados es como CA ("raíz de confianza" o "autoridad", en algún navegador, como Firefox, se requiere además, indicar que el certificado puede emplearse para "identificar sitios web").

En caso de no instalar dichos certificados, el acceso al servicio podrá ser limitado o con advertencias de seguridad.

2.4 Envío de peticiones

Las peticiones que no cumplan estos requisitos podrán ser rechazadas.

2.4.1 Cabeceras HTTP

Por motivos de seguridad se requiere en la cabecera de las peticiones esté presente la definicion **Content-Length** con el valor correcto en bytes.

Se recomienda también la definicion del charset sea en UTF-8. Ejemplo:"Content-Type: text/xml;charset=UTF-8".

2.4.2 Tamaños de las peticiones

Se admiten solicites POST con un tamaño máximo de 8M.

2.5 Integración en Java

Para aquellos integradores que decidan usar Java se recomienda usar la version >= 1.7. Esta versión soporta TLS y SNI por defecto.

2.5.1 Librerías recomendadas

Esta es la relación de librerías java recomendadas para la integración con las distintas codificaciones wsdl.

Entorno de Staging o Test

Codificación	Librerias Java recomendadas	Url
RPC/ Encoded	Axis 1.4	WS Proveedores https://se-face-webservice.redsara.es/sspp?wsdl
RPC/ Encoded	Axis 1.4	WS Organismos https://se-face-webservice.redsara.es/srcf?wsdl
RPC/ Encoded	Axis 1.4	WS Gestion Unidades https://se-face-webservice.redsara.es/gestionUnidades?wsdl
RPC/ Literal	Axis 2 sobre xmlbeans	WS Proveedores https://se-face-webservice.redsara.es/sspp2?wsdl
RPC/ Literal	Axis 2 sobre xmlbeans	WS Organismos https://se-face-webservice.redsara.es/srcf2?wsdl
RPC/ Literal	Axis 2 sobre xmlbeans	WS Gestion Unidades https://se-face-webservice.redsara.es/gestionUnidades2?wsdl

Entorno de Producción

Codificación	Librerias Java recomendadas	Url
RPC/ Encoded	Axis 1.4	WS Proveedores https://webservice.face.gob.es/sspp?wsdl
RPC/ Encoded	Axis 1.4	WS Organismos https://webservice.face.gob.es/srcf?wsdl

Codificación	Librerias Java recomendadas	Url
RPC/ Encoded	Axis 1.4	WS Gestion Unidades https://webservice.face.gob.es/ gestionUnidades?wsdl
RPC/ Literal	Axis 2 sobre xmlbeans	WS Proveedores https://webservice.face.gob.es/ sspp2?wsdl
RPC/ Literal	Axis 2 sobre xmlbeans	WS Organismos https://webservice.face.gob.es/ srcf2?wsdl
RPC/ Literal	Axis 2 sobre xmlbeans	WS Gestion Unidades https://webservice.face.gob.es/ gestionUnidades2?wsdl

NOTA: Se está estudiando la posibilidad de crear una tercera codificación Document/Literal que está en estudio de viabilidad no existiendo por ahora una fecha para su puesta en producción.

NOTA: para aquellos integradores en Java 6, por defecto usa SSLv3 y el handshake falla. Especificar en el arranque la opcion -Dhttps.protocols="TLSv1"

Capítulo 3

Uso de certificados en FACe.

3.1 Clasificación de certificados por Afirma

La plataforma @firma, a través del campo "clasificación" de la respuesta de la herramienta validae (https://valide.redsara.es/valide/inicio.html) , proporciona una clasificación básica del tipo de certificado que se trata.

Los tipos son los que se incluyen a continuación:

- Clasificación = 0 – Persona física según la ley 59/2003
- Clasificación = 1 – Persona jurídica según la ley 59/2003
- Clasificación = 2 – Componente/SSL/no reconocido/sello de empresa
- Clasificación = 3 – Sede según la ley 11/2007
- Clasificación = 4 – Sello según la ley 11/2007
- Clasificación = 5 – Empleado Público según la ley 11/2007
- Clasificación = 6 – Entidad sin personalidad jurídica según la ley 59/2003

Las clasificaciones devueltas por @firma coinciden con las clasificaciones de los certificados indicados por el MINETUR. Pueden consultar todos los certificados incluidos en @firma y su clasificación en el ANEXO PSC's de la Declaración de Practicas de validación de @firma: documento (http://forja-ctt.administracionelectronica.gob.es/webdav/site/ctt-map/users/soporte_afirma/public/@FirmaV5p0_ANEXO_PSC.pdf)

Certificados publicados en la web del MINETUR como reconocidos:

- Certificados de Persona Física (tipo 0 en @firma).
- Certificados de Persona Jurídica – Legal Person (tipo 1 en @firma).
- Certificados de Empleado Público (tipo 5 en @firma).
- Certificados de Sello Electrónico (tipo 4 en @firma).
- Certificados de Entidad Sin Personalidad Jurídica (tipo 6 en @firma).

Certificados publicados en la web del MINETUR como no reconocidos / Certificados de componente / Certificados de aplicación / Certificados SSL / Certificados de TSA (tipo 2 en @firma).

Certificados publicados en la web de MINETUR como de Sede Electrónica (tipo 3 en @firma)

Otros.

- Certificados de Empleado Nivel Alto, propósito de Autenticación (tipo 5 en @firma).
- Certificados de Empleado Nivel Alto, propósito de Cifrado (tipo 5 en @firma)

Certificados reconocidos de PSC's extranjeros según Directiva de Firma Electrónica (tipo 0 en @firma)

3.2 Uso de certificados en FACe

En FACe se pueden usar certificados para varios propósitos que enumeramos a continuación:

Firma de comunicación por Web Services tipo SOAP

Este uso comprende la firma de xml en cualquiera de los formatos XMLDsig o XAdES en cualquiera de sus variantes. Los certificados admitidos para ese uso son:

- Clasificación = 0 – Persona física según la ley 59/2003
- Clasificación = 1 – Persona jurídica según la ley 59/2003
- Clasificación = 2 – Componente/SSL/no reconocido/sello de empresa
- Clasificación = 3 – Sede
- Clasificación = 4 – Sello según la ley 11/2007

- Clasificación = 5 – Empleado Público según la ley 11/2007

Firma de la factura electrónica

Este uso comprende la firma de la factura en xml en cualquiera de los formatos XMLDsig o XAdES en cualquiera de sus variantes. Los certificados admitidos para ese uso son:

- Clasificación = 0 – Persona física según la ley 59/2003
- Clasificación = 1 – Persona jurídica según la ley 59/2003
- Clasificación = 4 – Sello según la ley 11/2007
- Clasificación = 5 – Empleado Público según la ley 11/2007

Se han encontrado algunos casos de certificados validos emitidos incorrectamente. Para la firma de facturas FACe requiere que el certificado aporte DNI y nombre y apellidos del responsable.

Para certificados de clase 0 y 5 se requiere que el certificado tenga los atributos "Nombre-Responsable","PrimerApellidoResponsable" y "NIFResponsable" Para certificados de clase 1 se requieren los atributos "NIF-CIF" y "RazónSocial". Para certificados de clase 4 se requieren los atributos "NIFEntidadSuscriptora" y "entidadSuscriptora".

Logeado en FACe con certificado

Este uso es para identificar personas físicas por lo que los certificados aceptados son:

- Clasificación = 0 – Persona física según la ley 59/2003
- Clasificación = 5 – Empleado Público según la ley 11/2007

Firma de justificantes dentro del portal de FACe

La firma de documentos o justificantes deben ser por personas físicas por lo que los certificados aceptados son:

- Clasificación = 0 – Persona física según la ley 59/2003
- Clasificación = 5 – Empleado Público según la ley 11/2007