



---

# FACeB2B

Punto de entrada de facturas electrónicas entre empresas

## Integración y recomendaciones

---

*Versión*

**1.0**

*Fecha de revisión*

**26/09/2017**

*Realizado por*

**Equipo DTI**

# ÍNDICE

1.1.	¿Qué es FACeB2B? .....	3
1.2.	Web Services FACeB2B .....	4
1.3.	Comunicación e integración con los Web Services FACeB2B .....	6
1.3.1.	Protocolos SSL y TLS .....	6
1.3.2.	Server Name Indication (SNI) .....	6
1.3.3.	Confianza en Certificados FNMT Clase 2 CA .....	6
1.3.4.	Envío de peticiones .....	7
1.3.5.	Integración en Java .....	7
1.4.	Uso de certificados en FACeB2B .....	9
1.4.1.	Clasificación de certificados por Afirma .....	9
1.4.2.	Uso de Certificados en FACeB2B .....	10

## 1.1. ¿Qué es FACeB2B?

Dado el éxito de la implantación de la factura electrónica en el Sector Público en el año 2015, se creó un grupo de trabajo entre miembros del Sector Privado y del Sector Público para tratar la implantación de la factura electrónica en las relaciones entre empresas.

Este grupo de trabajo estudia las medidas de éxito del modelo de facturación electrónica del Sector Público, para tratar de trasladar e impulsar aquellas que sean necesarias y viables al Sector Privado en las relaciones de facturación entre empresas.

Primero, para fomentar la facturación electrónica globalmente y que llegue a todos los sectores industriales sin importar el tamaño de la organización, sector o grado de informatización. Y segundo para generar nuevos modelos que permitan solventar los problemas que la facturación electrónica actualmente pueda producir a empresas de determinados sectores, tamaño o grado de informatización.

Por todo ello se han creado un conjunto de Web Services que permitirán a las entidades integrar en sus sistemas la remisión de facturas y su gestión, así como la gestión de sus usuarios y unidades contables.

## 1.2. Web Services FACeB2B

A continuación se detallan los diferentes Web Services que engloban toda la actividad prevista para FACe B2B:

### GESTIÓN DE FACTURAS (facturasspp):

Este Web Service engloba todos los métodos necesarios para el proveedor para remitir y consultar facturas:

- Enviar factura. Se divide en tres grupos: información del proveedor, fichero de la factura y ficheros anexos.
- Anular factura.
- Consultar estados.
- Consultar factura.
- Consultar listado de facturas.
- Consultar Unidades por Empresas.
- Consultar Empresas.
- Consultar NIFs.
- Consultar NIFs por Empresa.

### NOTIFICACIONES DE FACTURA para los proveedores (notificasspp):

Este Web Service engloba todos los métodos necesarios para la gestión de notificaciones para los proveedores:

- Obtener Tipos Notificación activos en FACe B2B.
- Creación Tipos de Notificación.
- Obtener Tipos Notificación activos configurados en Sistema Proveedor.

### **GESTIÓN DE FACTURAS para las empresas (facturasrcf)**

Este Web Service engloba todos los métodos necesarios para el gestor para evolucionar sus facturas:

- Solicitar nuevas facturas.
- Solicitar nuevas anulaciones.
- Descargar factura.
- Confirmar descarga de factura.
- Cambiar estado de facturas.
- Consultar estados.
- Consultar unidades.
- Gestionar solicitud de anulación de facturas.
- Consultar factura.
- Consultar listado de facturas.
- Cambiar estado listado de facturas.
- Gestionar solicitud anulación listado facturas.
- Cambio código RCF.
- Consultar código RCF (estas dos últimos se usarán si la empresa llevan un registro contable).

### **GESTIÓN DE DIRECTORIO para las empresas (directoriosrcf)**

Este Web Service engloba todos los métodos necesarios para la gestión del directorio de los gestores de facturas:

- Consultar Unidad.
- Gestión Número de Identidad.
- Gestión de Relación.
- Gestión de Rol.

## 1.3. Comunicación e integración con los Web Services FACeB2B

### 1.3.1. Protocolos SSL y TLS

El único protocolo admitido es TLS $\geq$ 1.0

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

### 1.3.2. Server Name Indication (SNI)

El único acceso permitido es por nombre, no es posible el 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 cuyo navegador no soporten 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, se puede comprobar la compatibilidad de su cliente o navegador en wikipedia artículo sobre SNI ([http://es.wikipedia.org/wiki/Server\\_Name\\_Indication](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.

### 1.3.3. Confianza en Certificados FNMT Clase 2 CA

Los certificados empleados por el servicio son "FNMT Clase 2 CA". Para evitar problemas 7 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](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.

### 1.3.4. Envío de peticiones

Las peticiones que no cumplan estos requisitos podrán ser rechazadas.

#### 1.3.4.1. Cabeceras HTTP

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

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

#### 1.3.4.2. Tamaños de las peticiones

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

### 1.3.5. Integración en Java

Para aquellos integradores que decidan usar Java se recomienda usar la versión  $\geq 1.7$ . Esta versión soporta TLS y SNI por defecto.

### 1.3.5.1. Librerías recomendadas

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

#### Entorno de Staging o Test (FALTA TABLA)

Codificación	Librerías Java recomendadas	URL
RPC/Encoded	Axis 1.4	WS Proveedores <a href="https://se-faceb2b-webservice.redsara.es/sspp?wsdl">https://se-faceb2b-webservice.redsara.es/sspp?wsdl</a>
RPC/Encoded	Axis 1.4	WS Organismos <a href="https://se-faceb2b-webservice.redsara.es/srcf?wsdl">https://se-faceb2b-webservice.redsara.es/srcf?wsdl</a>
RPC/Encoded	Axis 1.4	WS Gestion Unidades <a href="https://se-faceb2b-webservice.redsara.es/gestionUnidades?wsdl">https://se-faceb2b-webservice.redsara.es/gestionUnidades?wsdl</a>
RPC/Literal	Axis 2 sobre xmlbeans	WS Proveedores <a href="https://se-faceb2b-webservice.redsara.es/sspp2?wsdl">https://se-faceb2b-webservice.redsara.es/sspp2?wsdl</a>
RPC/Literal	Axis 2 sobre xmlbeans	WS Organismos <a href="https://se-faceb2b-webservice.redsara.es/srcf2?wsdl">https://se-faceb2b-webservice.redsara.es/srcf2?wsdl</a>
RPC/Literal	Axis 2 sobre xmlbeans	WS Gestion Unidades <a href="https://se-faceb2b-webservice.redsara.es/gestionUnidades2?wsdl">https://se-faceb2b-webservice.redsara.es/gestionUnidades2?wsdl</a>

#### Entorno de Producción (FALTA TABLA)

Codificación	Librerías Java recomendadas	URL
RPC/Encoded	Axis 1.4	WS Proveedores <a href="https://faceb2b-webservice.redsara.es/sspp?wsdl">https://faceb2b-webservice.redsara.es/sspp?wsdl</a>
RPC/Encoded	Axis 1.4	WS Organismos <a href="https://faceb2b-webservice.redsara.es/srcf?wsdl">https://faceb2b-webservice.redsara.es/srcf?wsdl</a>
RPC/Encoded	Axis 1.4	WS Gestion Unidades <a href="https://faceb2b-webservice.redsara.es/gestionUnidades?wsdl">https://faceb2b-webservice.redsara.es/gestionUnidades?wsdl</a>
RPC/Literal	Axis 2 sobre xmlbeans	WS Proveedores <a href="https://faceb2b-webservice.redsara.es/sspp2?wsdl">https://faceb2b-webservice.redsara.es/sspp2?wsdl</a>
RPC/Literal	Axis 2 sobre xmlbeans	WS Organismos <a href="https://faceb2b-webservice.redsara.es/srcf2?wsdl">https://faceb2b-webservice.redsara.es/srcf2?wsdl</a>
RPC/Literal	Axis 2 sobre xmlbeans	WS Gestion Unidades <a href="https://faceb2b-webservice.redsara.es/gestionUnidades2?wsdl">https://faceb2b-webservice.redsara.es/gestionUnidades2?wsdl</a>

**NOTA:** para aquellos integradores en Java 6, por defecto usa SSLv3 y el handshake falla. Hay que especificar en el arranque la opción `-Dhttps.protocols="TLSv1"`

## 1.4. Uso de certificados en FACeB2B

### 1.4.1. Clasificación de certificados por Afirma

La plataforma @firma, a través del campo "clasificación" de la respuesta de la herramienta Valide (<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.
- Clasificación = 7 – Empleado Público con Seudónimo.
- Clasificación = 8 – Cualificado de sello (UE 910/2014).
- Clasificación = 9 – Cualificado de autenticación de sitio web (UE 910/2014).
- Clasificación = 10 – Cualificado de sello de tiempo.
- Clasificación = 11 – Persona física representante ante las AAPP de persona jurídica.
- Clasificación = 12 – Persona física representante ante las AAPP de entidad sin persona jurídica.

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 Prácticas de validación de @firma:

[http://forjactt.administracionelectronica.gob.es/webdav/site/cttmap/users/soporte\\_afirma/public/@FirmaV5p0\\_ANEXO\\_PSC.pdf](http://forjactt.administracionelectronica.gob.es/webdav/site/cttmap/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).**

### **1.4.2. Uso de Certificados en FACeB2B**

En FACeB2B 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.
- Clasificación = 6 – Certificados de Entidad Sin Personalidad Jurídica.
- Clasificación = 7 – Empleado Público con Seudónimo.
- Clasificación = 8 – Cualificado de sello (UE 910/2014).
- Clasificación = 9 – Cualificado de autenticación de sitio web (UE 910/2014).
- Clasificación = 11 – Persona física representante ante las AAPP de persona jurídica.
- Clasificación = 12 – Persona física representante ante las AAPP de entidad sin persona jurídica.

### 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.
- Clasificación = 6 – Certificados de Entidad Sin Personalidad Jurídica.
- Clasificación = 8 – Cualificado de sello (UE 910/2014).
- Clasificación = 11 – Persona física representante ante las AAPP de persona jurídica.
- Clasificación = 12 – Persona física representante ante las AAPP de entidad sin persona jurídica.

Se han encontrado algunos casos de certificados válidos emitidos como seudónimos. Para la firma de facturas FACeB2B requiere que el certificado aporte NIF y nombre o razón social. En este caso un representante no será válido en tanto que no aporte dicha información.

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". Para certificados de clase 6 es necesario que la entidad emisora remitan los campos "NIF-CIF" y "RazónSocial" o "NombreResponsable" y "PrimerApellidoResponsable".