AFIP-SDG SIT

Facturación Electrónica

Especificación de establecimiento de canal de comunicación

Administración Federal de Ingresos Públicos
Subdirección General de Sistemas y Telecomunicaciones
Buenos Aires
11 de enero de 2007

1.1 Objetivo

El presente documento esta dirigido a quienes tengan que desarrollar el cliente consumidor de los WebServices correspondientes al servicio de Facturación Electrónica (WSFE).

1.2 Alcance

Este documento brinda las especificaciones técnicas para el establecimiento de la comunicación segura entre el cliente consumidor (CEE) y el WSFE. Debe complementarse con los documentos relativos a: Servicio de Autenticación y Autorización y Manual para el desarrollador.

1.3 Descripción general

La comunicación entre el CEE y el WSFE se realizara a través de HTTP sobre protocolo SSL v3.0 estándar (HTTPS). Esto involucra tanto la comunicación desde el CEE hacia el WebService de Autenticación y Autorización (WSAA) como así también el WebService de Negocio (WSN).

En el momento de establecerse el canal encriptado SSL (Handshake), el WSFE presentara el certificado X509 (Server Certificate) correspondiente al WS involucrado (WSAA o WSN dependiendo de la URL invocada por el CEE) indicando la identidad del servidor al cual se ha establecido la comunicación.

El certificado estará firmado por una Autoridad Certificante (CA) conocida permitiendo al CEE confirmar la identidad del servidor al cual se ha conectado.

Es importante aclarar que este mecanismo de presentación de certificado por parte del WSFE no esta relacionado con los métodos de Autenticación y Autorización implementados en el WSAA para el propio servicio de WSFE.

1.4 Establecimiento e invocación

La utilización de protocolo SSL para HTTP no requiere ningún tipo de establecimiento previo de las partes ni clave precompartida. Únicamente es necesario especificar su uso en el momento de invocación del método del servicio de WS.

Ejemplo:

https://wsw.afip.gov.ar/wsfe/service.asmx

El indicador HTTPS es el encargado de establecer el canal seguro de comunicación, previa negociación automática entre los extremos sobre algoritmos de encripcion y digesto a utilizar en la comunicación. Una vez establecida, se genera la llamada al método invocado.

1.5 Requerimientos

Al usar especificaciones y protocolos estándares el cliente puede ser desarrollado con cualquier lenguaje de programación que posea librerías o métodos para establecimiento de conexiones a través de SSL.

No existen requerimientos en cuanto al tipo de conectividad a la red para el funcionamiento del mecanismo de establecimiento de comunicación segura, es decir, es compatible con las utilizaciones de Proxys (transparentes y no transparentes) como así también para ambientes que utilicen direcciones IP dinámicas.

Las habilitaciones necesarias para su utilización a través de firewalls son:

Protocolo TCP

Port 443