Manual del Usuario del WSASS

Publicación 1.1

AFIP/SDGSIT/DIOPIN/DESOTE/DVSHYS

12 de January de 2017

Índice general

CAPÍTULO 1

INTRODUCCIÓN

Para los desarrolladores que deseen implementar aplicaciones que consuman de los webservices de AFIP, se dispone de la herramienta WSASS (Autogestion de certificados para Servicios Web en los ambientes de homologacion). WSASS ES una aplicacion online que permite al usuario gestionar sus certificados digitales para el Entorno de Testing exclusivamente.

Para usar el WSASS el usuario debe adherirse al servicio, ingresando con su clave fiscal al portal de AFIP. El servicio WSASS no es delegable, esto significa que para adherirse al servicio WSASS el usuario debe acceder con su clave fiscal de persona física (no de persona jurídica o empresa).

CAPÍTULO 2

FUNCIONALIDADES DISPONIBLES

2.1 Menú

Las funcionalidades disponibles en el menú del WSASS son:

- Introducción: Muestra una guía rápida de tareas que se pueden hacer en el WSASS.
- Servicios: Muestra el catálogo de servicios disponibles.
- Certificados: Muestra la lista de certificados que ha creado el usuario.
- Nuevo Certificado: Formulario para crear un certificado nuevo.
- Autorizaciones: Muestra la lista de autorizaciones creadas por el usuario.
- Crear autorización a servicio: Formulario para crear una autorización para que un certificado pueda utilizar un servicio representando a un contribuyente.
- Eliminar autorización a servicio: Formulario para eliminar una autorización de acceso a servicio por parte de un certificado.
- Agregar certificado a alias: Formulario para solicitar la creación de un certificado adicional asociado.

2.2 Fin de sesión

Para finalizar la sesión pulsar el botón “Cerrar sesión” que está en la parte superior derecha. Para iniciar una nueva sesión hay que reingresar la clave fiscal en el portal de AFIP.

CAPÍTULO 3

CONCEPTOS BÁSICOS

Usando el WSASS los programadores de aplicaciones pueden solicitar acceso a los diversos webservices (denominados "servicios") que están disponibles en el ambiente de testing/homologación de la AFIP. Básicamente, el WSASS genera certificados digitales para testing. Dichos certificados digitales no son de aplicación para el ambiente de producción.

Para poder acceder a un servicio en ambiente de testing, la aplicación a programar debe utilizar el certificado generado en el WSASS. Entre otras cosas, el certificado contiene un Distinguished Name (DN) que incluye una CUIT. Cada DN será identificado por un "alias" o "nombre simbólico", que actúa como una abreviación.

3.1 Autoservicio de certificados

Para obtener el certificado, distinguimos dos casos según si el DN ya fué dado de alta (DN existente) o si aún no existe. Para eso utilizar uno de los formularios siguientes:

- Formulario para obtener el certificado por primera vez (menú: Nuevo Certificado).
- Formulario para obtener otro certificado adicional para un DN existente (menú: Agregar Certificado a Alias).
- Ver los certificados emitidos para una CUIT (menú: Certificados).

3.2 Gestión de accesos a servicios

Una vez generado el DN y obtenido el certificado, se puede gestionar la autorización de acceso a los servicios de AFIP, utilizando los siguientes formularios:

- Formulario de solicitud de autorización de acceso a servicio (menú: Crear Autorización a Servicio).
- Formulario para eliminar una autorización de acceso a servicio (menú: Eliminar Autorización a Servicio).
- Ver el catálogo de servicios disponibles (menú: Servicios).

3.3 Delegación de representación

Una vez obtenido el certificado, se puede delegar la representación mediante la opción del menú Crear Autorización a Servicio, donde en el campo “CUIT representado” se debe colocar la CUIT a representar y además se debe seleccionar el servicio deseado.

CÓMO GENERAR UNA SOLICITUD DE CERTIFICADO (CSR)

Para obtener el certificado por primera vez, hay que dar de alta al DN. Para esto hay que presentar una "solicitud de certificado" o "Certificate Signing Request" (CSR). El CSR se genera en su computadora, usando la herramienta OpenSSL (disponible para Windows, UNIX/Linux y MacOSX). Primero hay que generar una clave privada en formato PKCS10 con un mínimo de 2048 bits:

```
openssl genrsa -out MiClavePrivada 2048
```

IMPORTANTE

Conserve el archivo de su clave privada en un lugar seguro.

Luego hay que generar el CSR propiamente dicho:

```
openssl req
    -new
    -key MiClavePrivada
    -subj "/C=AR/O=subj_o/CN=subj_cn/serialNumber=CUIT subj_cuit"
    -out MiPedidoCSR
```

donde hay que reemplazar:

- MiClavePrivada por nombre del archivo elegido en el primer paso.
- subj_o por el nombre de su empresa
- subj_cn por el nombre de su sistema cliente
- subj_cuit por la CUIT (sólo los 11 dígitos, sin guiones) de la empresa o del programador (persona jurídica)
- MiClavePrivada por el nombre del archivo de la clave privada generado antes
- MiPedidoCSR por el nombre del archivo CSR que se va a crear

IMPORTANTE

Observar que en el serialNumber se escribe "CUIT" seguido de un espacio en blanco y a continuación los 11 dígitos de la CUIT sin separadores.

Por ejemplo, para una empresa llamada EmpresaPrueba, un sistema TestSystem, la CUIT 20123456789, con el archivo MiClavePrivada generado en el punto anterior:

```
openssl req
-new
-key MiClavePrivada
-subj "/C=AR/O=EmpresaPrueba/CN=TestSystem/serialNumber=CUIT 20123456789"
-out MiPedidoCSR
```

Si no hay errores, el archivo 'MiPedidoCSR' será utilizado al momento de obtener el DN y el certificado. El aspecto de un archivo CSR es similar a lo siguiente:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIClTCCAX0CAQAwUDELMAkGA1UEBhMCQVIxEjAQBgNVBAoTCVNPUE9SVEVXUzES
MBAGA1UEAxMJU09QT1JURVdTMRkwFwYDVQQFExBDVUlUIDIwMTkwMTc4MTU0MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyu7TZTjKEdXEZPR4wIhFOw1S
...
QMNYAgJ/J2Zyy2JzxtsHzZDN1oM1SJbG9KyA5Rp02QZMMMsMWIIYKQLsoM5QAPQH
DWxkDa8dm7tBylM3u5+XT5G+w1xH4WjRHViAmUH2U+hTmaVAj7qSxsQzR/5HWoKX
cnMXsTGvi/5Y9q9kuOw6csm43z5XvxT4BBBKZn6FqWqSwUKxVuaJU8Q=
-----END CERTIFICATE REQUEST-----
```

CAPÍTULO 5

CÓMO CREAR UN CERTIFICADO NUEVO

5.1 Obtención del certificado

MENU

Opción: "Nuevo Certificado" para acceder al formulario para crear un DN y el certificado inicialmente asociado al mismo.

Los campos a ingresar en el formulario son:

1. Nombre simbólico del DN. Es el alias o nombre simbólico del DN a crear. Este será el identificador por lo que debe ingresar un alias que no exista.
2. CUIT del contribuyente. Es la CUIT del contribuyente (persona física). Debe ser la mismo CUIT que se incluyó en la solicitud del certificado CSR (en el campo serialNumber del CSR). Este campo tiene automáticamente la CUIT del usuario conectado al WSASS y no puede editarse.
3. Solicitud de certificado en formato PKCS10. Es la solicitud de certificado (Certificate Signing Request, CSR) en formato PKCS10. El CSR debe contener en el SerialNumber el valor "CUIT nnnnn", donde nnnnn es el número de CUIT del usuario conectado al WSASS.

Luego presionar "Crear DN y Obtener Certificado". Si no hay errores, el sistema devuelve un certificado x509 en formato PEM. El aspecto del certificado es similar a lo siguiente:

```
-----BEGIN CERTIFICATE-----
MIIDSzCCAjOgAwIBAgIIS7JIkcfpQhswDQYJKoZIhvcNAQENBQAwMzEVMBMGA1UEAwwMQ29tcHV0
YWRvcmVzMQ0wCwYDVQQKDARBRklQMQswCQYDVQQGEwJBUjAeFw0xNjA5MzAxMTUzMjhaFw0xODA5
MzAxMTUzMjhaMDYxGTAXBgNVBAMMEENlcnRfZ2xhcnJpZXJhXzExGTAXBgNVBAUTEENVSVQgMjAx
OTAxNzgxNTQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDK7tNlOMoR1cRk9HjAiEU7
...
z2JEQXFPkcxcG6DE9v4Q/8WSaiPRxbzjOkC5+cEuEtqxlwGsCDeFjSRco05XFWmzXg8jLrJIEk8l
jFRvrIR9Shm/p6RxU6ZeBkyeNAu3c5ShTyL0tntIEoXDpx4wqZ2ZkA4tinmbbI7LnnCyaniKw27h
bkQkLybJPc1LIzJb9tRzFQUu9PreRj1ggnhzzo/qtCicv6oVoi7nZW05lO5mG8JxJQhEFfnVgZqw
0QRQQb4/Ouequfgw84C1/dD2TKH9RsjiJ8tiVvsCuz5tjkb727tH/ZW3ce2bG9t4QQ==
-----END CERTIFICATE-----
```

Luego hay que copiarlo y pegarlo en un editor de texto plano, para grabarlo en su disco duro local (por ejemplo, en un archivo *certificado.pem*).

NOTA

Los certificados creados no pueden ser eliminados, ni aún después de su fecha de expiración. El usuario puede crear todos los certificados que crea necesario.

5.2 Cómo crear un archivo PFX con clave privada

El formato PFX o PKCS#12 es un formato binario para almacenar el certificado del servidor, los certificados intermedios y la clave privada, todo en un único archivo encriptado. Los archivos PFX usualmente tienen la extensión *.pfx* o *.p12* y son típicamente usados en Windows para importar o exportar certificados y claves privadas.

Si se necesita crear un archivo PFX se puede usar OpenSSL. Por ejemplo:

```
openssl pkcs12
-export
-inkey MiClavePrivada
-in certificado.pem
-out certificado.pfx
```

donde *MiClavePrivada* es la clave privada usada cuando se generó el CSR, *certificado.pem* es el certificado x509 en formato PEM obtenido usando el WSASS y *certificado.pfx* será el nuevo archivo PFX conteniendo al certificado firmado.

CÓMO CREAR UNA AUTORIZACION DE ACCESO

MENU

Opción: “Crear Autorizacion a Servicio” para acceder al formulario para crear una autorización para que un DN pueda utilizar un servicio representando a un contribuyente.

Los campos a ingresar en el formulario son:

1. Nombre simbólico del DN a autorizar. Es el alias o nombre simbólico del DN a autorizar acceso al servicio. Debe haberse creado previamente. Elegir el alias de la lista desplegable.
2. CUIT del DN a autorizar. Es la CUIT del DN existente, que va a ser autorizado a usar el servicio en representación de un contribuyente. Este campo no puede modificarse.
3. CUIT representado. Es la CUIT representada por el DN. Ingresar la CUIT de una persona física o jurídica (empresa).
4. CUIT de quien genera la autorizacion. Es la CUIT de quien genera esta autorización (CUIT autorizante). Este campo tiene automáticamente la CUIT del usuario conectado al WSASS y no puede editarse.
5. Servicio al que desea acceder. Es el nombre del servicio al que el DN será autorizado a acceder, que se elige de la lista de servicios desplegable.

Luego presionar el botón “Crear Autorización de Acceso”.

CÓMO AGREGAR UN CERTIFICADO A UN ALIAS

MENU

Opción: “Agregar Certificado a Alias” para acceder al formulario para solicitar la creación de un certificado adicional asociado a un DN existente.

Los campos a ingresar en el formulario son:

1. Nombre simbólico del DN. Es el alias o nombre simbólico del DN. Debe haberse creado previamente. Elegir el alias de la lista desplegable.
2. CUIT del DN. Es la CUIT del DN seleccionado en el Campo 1.
3. Nueva solicitud de certificado en formato PKCS10. Es la solicitud de certificado (Certificate Signing Request, CSR) en formato PKCS10. Se ignora el campo DN del CSR. Copiar y pegar en este campo el contenido del CSR generado oportunamente en su computuadora local.

Luego presionar “Crear Certificado Adicional para el DN”. Si no hay errores, el sistema devuelve un certificado x509 en formato PEM. Luego hay que copiarlo y pegarlo en un editor de texto plano, para grabarlo en su disco duro local.

CÓMO VER LOS SERVICIOS DISPONIBLES

MENU

Opción: “Servicios” para ver el catálogo de servicios disponibles.

De cada servicio se muestra:

1. Id. Es el identificador interno del servicio.
2. Descripción. Una descripción del servicio.
3. Url. La dirección del servicio.

Pulsar en el enlace “Ver” para mostrar los detalles de un servicio en particular.

CÓMO VER LOS CERTIFICADOS GENERADOS

MENU

Opción: “Certificados” para ver el todos los certificados generados.

De cada certificado se muestra:

1. CUIT. Es la CUIT del usuario que generó el certificado.
2. Alias. Es el alias o nombre simbólico del DN, identifica al certificado.
3. DN. Es el DN del certificado.

Pulsar en el enlace “Ver” para mostrar los detalles de un certificado en particular.