



Manual del Usuario del WSASS

Publicación 19.10.1

soporte-ws-testing@afip.gob.ar





1. INTRODUCCIÓN	1
2. FUNCIONALIDADES DISPONIBLES	3
3. CONCEPTOS BÁSICOS	5
3.1. Autoservicio de certificados.....	5
3.2. Gestión de acceso a servicios.....	5
3.3. Delegación de representación.....	6
4. CÓMO GENERAR UNA SOLICITUD DE CERTIFICADO(CSR)	7
4.1. Generación de la clave privada.....	7
4.2. Generación del CSR.....	7
5. CÓMO CREAR UN CERTIFICADO NUEVO	9
5.1. Cómo crear un archivo PFX con clave privada.....	10
6. CÓMO CREAR UNA AUTORIZACIÓN DE ACCESO	11
7. CÓMO AGREGAR UN CERTIFICADO A UN ALIAS	13
8. CÓMO VER LOS SERVICIOS DISPONIBLES	15
9. CÓMO VER LOS CERTIFICADOS GENERADOS	17
10. CÓMO VER LAS AUTORIZACIONES REALIZADAS	19
11. CÓMO ELIMINAR UNA AUTORIZACIÓN	21
12. FAQ (PREGUNTAS/RESPUESTAS FRECUENTES)	23
12.1. Cómo hago para adherirme al servicio WSASS ?.....	23
12.2. Cuando trato de adherirme veo el error “El servicio no es delegable”.....	23
12.3. Cómo hago para generar un certificado para la CUIT de una empresa?.....	23
12.4. Al crear un certificado en el WSASS veo el error “Error creando certificado”.....	23
12.5. Quiero eliminar un certificado que creé, cómo hago eso?.....	24





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).

Los pasos para adherirse al servicio WSASS se explican en el manual “WSASS: Cómo adherirse al servicio” publicado en http://www.afip.gob.ar/ws/WSASS/WSASS_como_adherirse.pdf

Por comentarios o preguntas acerca de este manual, por favor contactar asoporte-ws-testing@afip.gob.ar



FUNCIONALIDADES DISPONIBLES

WSASS Autoservicio de Acceso a WebServices (TESTING/HOMOLOGACIÓN)

TAREAS QUE SE PUEDEN HACER EN ESTE SITIO

En este sitio los programadores de aplicaciones pueden solicitar acceso a los diversos webservices (denominados "servicios") que están disponibles en el ambiente de test AFIP. **No son de aplicación para el ambiente de Producción.**

Para poder acceder a un servicio, la aplicación a programar debe utilizar un certificado de seguridad, que se obtiene en este sitio. Entre otras cosas, el certificado contiene (CN) que incluye una CUIT. Cada DN será identificado por un "alias" o "nombre simbólico", que actúa como una abreviación.

Autoservicio de certificados

Para obtener el certificado, distinguimos dos casos según si el DN ya fue creado de alta (DN existente) o si aún no existe. Según sea el caso, utilice uno de los formularios:

- Formulario para obtener el certificado por primera vez
- Formulario para obtener otro certificado adicional (para un DN existente)

Tareas relacionadas:

- Ver los certificados emitidos para una CUIT

Gestión de accesos a servicios

Una vez generado el DN y obtenido el certificado, se puede solicitar autorización de acceso a los servicios de AFIP:

- Ver el catálogo de servicios disponibles
- Formulario de solicitud de autorización de acceso a servicio

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.

FINALIZAR SESION

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.





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). Los pasos son:

4.1 Generación de la clave privada

La clave privada de 2048 bits se genera con OpenSSL.

```
openssl genrsa -out MiClavePrivada.key 2048
```

IMPORTANTE

Conserve el archivo de su clave privada en un lugar seguro. La clave privada va a ser necesaria, junto con el certificado creado a partir de ella, para firmar los mensajes.

4.2 Generación del CSR

El CSR se genera a partir de la clave privada, usando OpenSSL.

```
openssl req  
-new  
-key MiClavePrivada.key  
-subj "/C=AR/O=Empresa/CN=Sistema/serialNumber=CUIT nnnnnnnnnnnn"  
-out MiPedidoCSR.csr
```

donde hay que reemplazar:

- *MiClavePrivada.key* por nombre del archivo elegido en el primer paso.
- *Empresa* por el nombre de su empresa
- *Sistema* por el nombre de su sistema cliente
- *nnnnnnnnnnnn* por la CUIT (sólo los 11 dígitos, sin guiones) de la empresa o del programador ■ (persona jurídica)
- *MiPedidoCSR.csr* por el nombre del archivo CSR que se va a crear



IMPORTANTE

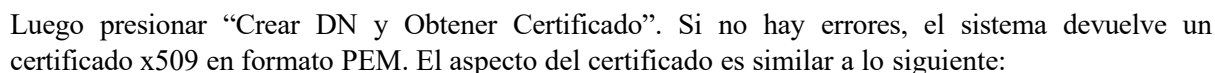
Observar que en el serialNumber se escribe “CUIT” seguido de un espacio en blanco y a continuación los 11 dígitos de la CUIT sin separadores.

Por ejemplo, para una empresa llamada “MiEmpresa”, un sistema llamado “TestSystem”, la CUIT 20123456789, con un archivo de clave privada llamado *TestSystem.key*, así se crearía el CSR:

```
openssl req -new -key TestSystem.key
-subj "/C=AR/O=MtEmpresa/CN=TestSystem/serialNumber=CUIT 20123456789"
-out TestSystem.csr
```

Si no hay errores, el archivo *TestSystem.csr* 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-----
MIIC1TCCAX0CAQAwUDELMAkGA1UEBhMCQVixEjAQBgNVBAoTCVNPUE9SVEVXUzE
S
MBAGA1UEAxMJU09QT1JURVdTMRkwFwYDVQQFExBDVU1UIDIwMTkwMTc4MTU0MII
B
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYu7TZTjKEdXEZPR4wIhFOW1
S
...
QMNYAgJ/J2Zyy2JzxtsHzZDN1oM1SJbG9KyA5Rp02QZMMsMWIIYKQLsoM5QAPQ
```

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

El DN del certificado creado tiene el formato “SERIALNUMBER=CUIT nnnnnnnnnnnn, CN=xxxxx”, donde ‘nnnnnnnnnnnn’ es el número de la CUIT y ‘xxxxx’ es el alias que se indicó. Este formato es por diseño y no puede modificarse.

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

El formato PFX o PKCS#12 es un formato binario para almacenar el certificado, los certificados inter-medios 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.

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

— AFIPComunica      



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 listadesplegable.
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 autorización. 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

WSASS Autoservicio de Acceso a WebServices (TESTING/HOMOLOGACIÓN)

Autogestión de servicios

- Introducción
- Servicios
- Certificados
- Nuevo Certificado
- Crear autorización a servicio
- Eliminar autorización a servicio
- Autorizaciones
- Agregar certificado a alias**
- Contactenos

Agregar certificado

Formulario para solicitar la creación de un certificado adicional asociado a un DN existente.

1. Nombre simbólico del DN	SERIALNUMBER=CJIT 20190178154, CN=demo1	Es el alias o nombre simbólico del DN
2. CUIT del DN	20190178154	Es la CUIT del DN
3. Nueva solicitud de certificado en formato PKCS10	Es la solicitud de certificado (Certificate Signing Request, CSR) en formato PKCS10. Copiar y Pegar en este campo el contenido del CSR.	

Crear certificado adicional para el DN

Resultado

-----BEGIN CERTIFICATE REQUEST-----
MIICDCCAYACAQAwZEEUMAKGAIUEBHMICVixEJAQgNVBAoMCDQVJSSUYSQTE
VMBMGA1UEAwMRBxBLJ3RV3BU11TRKwFwYDVQQFEExBDVU1U1DIwRTkwMTc4MTU
0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQAMIBcKKAQEAsHmY18k1558H394DTjb
1FIV3jrfb+SdwLAvhfzEdXa51u0EY3QsqGfVtlyJAjXK8R0rcpJk1xgqn8d17Th
EAX8Cw15VW7QA4Uz91/PH0yFeLa++LwFVYpx397g/RTLRQe9B186IEqu6KfzU
GKxYfIg5xTbnQT63G8Env1BGCPuXR45ybQ/7LPoS5G5/Ba7Q5rAXAdH+AnA8uz4I
M-----

Si no hay errores:
El sistema entrega un nuevo certificado x509v2 en formato PEM. Copiar y Pegar en este campo, para grabar el certificado en su disco local.

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 computadora 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

**WSASS Autoservicio de Acceso a WebServices
(TESTING/HOMOLOGACIÓN)**
[Cerrar Sesión](#)

Autogestión de servicios

- Introducción
- Servicios**
- Certificados
- Nuevo Certificado
- Crear autorización a servicio
- Eliminar autorización a servicio
- Autorizaciones
- Agregar certificado a alias
- Contáctenos

Servicios

Catálogo de servicios disponibles.
Actualmente hay 167 servicios disponibles en el catálogo.

	Id	Descripción	URL
Ver	ws_exp_simp	Régimen de Exportación Simplificada "EXPORTA SIMPLE"	https://treshomo.afip.gov.ar/WSExpSimp/ExpSimpServ
Ver	ws_pdf_librosueldos	Servicio diseñado para el envío de los pdf de libro de sueldos a otras entidades gubernamentales	https://webserviceshomext.afip.gob.ar/misimplificas/wsPdfLibroDeSueldos.aspx
Ver	ws_sr_constancia_inscripcion	Web service de Consulta de la Constancia de Inscripción de Padrón	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA5
Ver	ws_sr_padron_a10	Servicio de consulta Padrón a10	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA10
Ver	ws_sr_padron_a100	Servicio de consulta de parámetros de padrón	https://awshomo.afip.gov.ar/sr-parametros/webServiceA100
Ver	ws_sr_padron_a13	WS de consulta padrón A13	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA13
Ver	ws_sr_padron_a4	Servicio Consulta Padrón A4	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA4
Ver	ws_sr_padron_a5	WS de Consulta Padrón A5	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA5
Ver	ws_sr_padron_a6	Servicio Consulta y actualización Padrón A6	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA6
Ver	ws_sr_padron_a7	Servicio Consulta y actualización Padrón A7	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA7
Ver	ws_sr_padron_a9	WS de consulta Padrón A9	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA9
Ver	wsagr	Archivo de Proveedores - Reproweb	https://wsinhomo.afip.gov.ar/wsagr/wsagr.aspx
Ver	wsavt	Combustibles	https://efscihomo.afip.gob.ar/pls/combust/pckcombust

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.

**WSASS Autoservicio de Acceso a WebServices
(TESTING/HOMOLOGACIÓN)**
[Cerrar Sesión](#)

Autogestión de servicios

- Introducción
- Servicios**
- Certificados
- Nuevo Certificado
- Crear autorización a servicio
- Eliminar autorización a servicio
- Autorizaciones
- Agregar certificado a alias
- Contáctenos

Información del servicio

Información detallada del servicio.



Servicio	ws_sr_constancia_inscripcion	Nombre que identifica al servicio
Descripción	Web service de Consulta de la Constancia de Inscripción de Padrón	Descripción del servicio
URL	https://awshomo.afip.gov.ar/sr-padron/webservices/personaServiceA5	URL del servicio
Tipo	ws	Tipo de servicio (ws: WebService)
Buscable	True	Indica si se puede dar la baja del servicio.
Texto bin	WS de Consulta de la Constancia de Inscripción	Texto a usarse en interfaz al usuario
Delegable	True	Indica si se puede delegar a otra CUIT
DN		DN del servicio
Filtro	False	Indica si hay filtros para autorizar/representar
Organismo	afip	Organismo dueño
Predible	True	Indica si es posible adherirse al servicio
Presencial	False	Indica si es presencial
Version ticket	2.0	Indica la versión del token de acceso
Visible	True	Indica si es visible
Nivel	3	Nivel mínimo de acceso requerido
Clave pública		Clave pública del servicio

Acciones posibles

Crear autorización para acceder a este servicio



CÓMO VER LOS CERTIFICADOS GENERADOS

**WSASS Autoservicio de Acceso a WebServices
(TESTING/HOMOLOGACIÓN)**
[Cerrar Sesión](#)

- Autogestión de servicios
 - Introducción
 - Servicios
 - Certificados**
 - Nuevo Certificado
 - Crear autorización a servicio
 - Eliminar autorización a servicio
 - Autorizaciones
 - Agregar certificado a alias
 - Contáctenos

Certificados

Actualmente hay 18 certificados para la CUIT 20190178154. [Selecciona un certificado para ver más detalles.](#)

	cuit	alias	dn
Ver	20190178154	20190510c	SERIALNUMBER=CUIT 20190178154, CN=20190510c
Ver	20190178154	demo1	SERIALNUMBER=CUIT 20190178154, CN=demo1
Ver	20190178154	glarriera20160930	SERIALNUMBER=CUIT 20190178154, CN=glarriera20160930
Ver	20190178154	glarriera20161118	SERIALNUMBER=CUIT 20190178154, CN=glarriera20161118
Ver	20190178154	glarriera2017	SERIALNUMBER=CUIT 20190178154, CN=glarriera2017
Ver	20190178154	glarriera20170825	SERIALNUMBER=CUIT 20190178154, CN=glarriera20170825
Ver	20190178154	glarriera20181029	SERIALNUMBER=CUIT 20190178154, CN=glarriera20181029
Ver	20190178154	glarriera20190510	SERIALNUMBER=CUIT 20190178154, CN=glarriera20190510
Ver	20190178154	glarriera20190513b	SERIALNUMBER=CUIT 20190178154, CN=glarriera20190513b
Ver	20190178154	glarriera20190903	SERIALNUMBER=CUIT 20190178154, CN=glarriera20190903
Ver	20190178154	soportews1	SERIALNUMBER=CUIT 20190178154, CN=soportews1
Ver	20190178154	soportews20161013	SERIALNUMBER=CUIT 20190178154, CN=soportews20161013
Ver	20190178154	soportews20161118	SERIALNUMBER=CUIT 20190178154, CN=soportews20161118
Ver	20190178154	test_1807160815_test	SERIALNUMBER=CUIT 20190178154, CN=test_1807160815_test
Ver	20190178154	test1pc1	C=ar, O=test1, SERIALNUMBER=CUIT 20190178154, CN=test1
Ver	20190178154	test1pc2	C=ar, O=supersistemas corp, SERIALNUMBER=CUIT 20190178154, CN=supersistema negriazu
Ver	20190178154	test2pc1	C=ar, O=empresapueba, SERIALNUMBER=CUIT 20190178154, CN=testsystem
Ver	20190178154	test3	CN=glarriera, SERIALNUMBER=CUIT 20190178154, O=glarriera, C=ar

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.



Autogestión de servicios

- Introducción
- Servicios
- Certificados
- Nuevo Certificado
- Crear autorización a servicio
- Eliminar autorización a servicio
- Autorizaciones
- Agregar certificado a alias
- Contáctenos

Información del DN

Alias del DN demo1
CUIT 20190178154
DN SERIALNUMBER=CUIT 20190178154, CN=demo1

Certificados asociados

	Emisión	Vencimiento	estado	serial
Ver	30/09/2019 02:59:43 p.m.	29/09/2021 02:59:43 p.m.	VALIDO	304a75d3d66030ee1

```
-----BEGIN CERTIFICATE-----
MIIDBTCCAi2gAwIBAgIIMEPl:09SiC*suDQVJFkoZlIwbnNAQENhQAwOCEaIMgGA1UEAwwRQ299tcRUV0
YWRvcmVzIHRlci03QmDTALBgNVBAQwMBEFGSVUAcCaA7BgNVBAYTAkFBRzB4XDESMGkkaMDEONTkzMlloK
DTIwMjIyOTQwMTk0MTEuR2EOMGAwGA1UEAwwRFGVUbnEwGTAXBgNVBAUTENUSVUQ2g6fjAeOTAAQgAg
MTQyggEAMGAOGCCqgSIlzIQEBAQUAA4IBDwAwggEgFAIIBAQCOWeZkXyTULneen3QW0NwVU8hXaCeSuf
JlYsC+EXGRldzm97QTI1CyoI+SW1TikAnErxHStykmSLGCqeF2LoOGADEETCLlVotAAdnTMGX8wo?
IV6xz7iuvu226VinHn3u097hXFB70GUMogSgjoqaW'e2NEU1DnFMGdSFrcoQSa+IEYFLRdHhLJcD/
ss+jFIhbn5FxtDmeScB0f4CcDS7FggycX/1*KhEdEzR3eTIS11reGZLxmkbv83UY9cb4B+ZRMcuGm
IOXV2uVGO9523uh462jG06p0Cf1M2nJEagtbU2e;M75GOWISVs06yqcWg4UQ2fj2QnqXfseH3ex
FgCoFRB/AgIEAAjYUSeIAw6A1UsEwES/wQCGAAnfwIDVR0jSBgwfoAUeLT//8put7eja8RIIaW
THlyT2iwGUFUROCBSYEIIFH9Poe30VsdL198anFfa0AS0jyGA4GAIUdMEB/wQEhWIT4DAMBgAq
hkiG9wEBAQOFAAOCAQEAf2obyKj483kbEM62aK11u12e9IteUWSETbu391u4d4ykh1NYq8ngVjo2g
Xia6FUjNk02JZcL9CXt9+u81VteALq0LhCoqu4P63bS0j/VOUuo4MeEFAgossax;37mXK6T28Ba
nVp1Hus+Jl+bdpT+2NM1Tb9n1FlvGF2S6B4Hs4khH9dql4RYeoi4hSeauFHEPFcLehNWEzPYT8
kiNUQaioVzAkQ2d5m4pAdnTvpqihaUkCWCsAF22UvULom4Ko+3QFFe93U+uQqiJ+I3mA7mS2Ec4T
3JVIULW27E7iCqenkaTkmq+/q8CWtDGekYNkmTUPR86fUWk1IGSa2XwQ==
-----END CERTIFICATE-----
```

Acciones posibles

Agregar Autorizaciones a este alias de DN



CÓMO VER LAS AUTORIZACIONES REALIZADAS

WSASS Autoseguro de Acceso a WebServices (TESTING/HOMOLOGACIÓN)

Autorizaciones

Actualmente hay 25 certificados para la CUIT 20190178154. Seleccione un certificado para ver más opciones.

	Dador	Alias	Representado	Servicio
Eliminar	20190178154	termo1	20190178154	ws.pdf.librosueltos
Eliminar	20190178154	glarriers2017	20190178154	sud.contrataciones
Eliminar	20190178154	glarriers2017	20190178154	sud.restricciones
Eliminar	20190178154	glarriers2017	20190178154	ws.sr.constancia.inscripcion
Eliminar	20190178154	glarriers2017	20190178154	ws.sr.padron.a10
Eliminar	20190178154	glarriers2017	20190178154	ws.sr.padron.a100
Eliminar	20190178154	glarriers2017	20190178154	ws.sr.padron.a1
Eliminar	20190178154	glarriers2017	20190178154	ws.sr.padron.a5
Eliminar	20190178154	glarriers2017	20190178154	ws.sr.padron.a9
Eliminar	20190178154	glarriers2017	20190178154	wsct
Eliminar	20190178154	glarriers2017	20190178154	wsctg
Eliminar	20190178154	glarriers2017	30709014370	wsctg
Eliminar	20190178154	glarriers2017	20190178154	wsfe
Eliminar	20190178154	glarriers2017	20190178154	wsfex
Eliminar	20190178154	glarriers2017	20190178154	wsmtxca
Eliminar	20190178154	glarriers2017	20190178154	wsremcarne
Eliminar	20190178154	glarriers2017	20190178154	wsstabaco
Eliminar	20190178154	glarriers20181029	20190178154	ws.sr.constancia.inscripcion
Eliminar	20190178154	glarriers20181029	20190178154	ws.sr.padron.a13
Eliminar	20190178154	glarriers20181029	20190178154	ws.sr.padron.a4

MENU

Opción: “Autorizaciones” para ver las autorizaciones realizadas.

De cada autorización se muestra:

- 1.Dador. Es la CUIT de quien realizó la autorización.
- 2.Alias. Es el alias del certificado autorizado.
- 3.Representado. Es la CUIT que puede acceder al servicio.
- 4.Servicio. Es el identificador del servicio autorizado.

Pulsar en el enlace “Eliminar” para mostrar los detalles de una autorización en particular, con opción a eliminarla. La eliminación de una autorización no elimina al certificado vinculado a la misma.



CÓMO ELIMINAR UNA AUTORIZACION

MENU

Opción: “Eliminar autorización a servicio” para acceder al formulario que permite eliminar una autorización.

Los campos a ingresar en el formulario son:

1. Nombre simbólico del DN autorizado. Es el alias o nombre simbólico del DN. Debe haberse creado previamente. Elegir el alias de la lista desplegable. Al seleccionar el alias, automáticamente se cargan los datos de los demás campos del formulario.
2. CUIT del DN. Es la CUIT del DN al que se le eliminará la autorización de acceso al servicio. Este campo no puede modificarse.
3. CUIT representada. Es la CUIT representada por el DN. Este campo no debe modificarse.
4. CUIT de quien elimina la autorización. Es la CUIT de quien elimina esta autorización del DN para acceder al servicio (CUIT eliminante). Este campo no puede modificarse.
5. Nombre del servicio. Es el nombre del servicio al que accede el DN.

Pulsar en el enlace “Eliminar autorización” para eliminar la autorización. La eliminación de una autorización no elimina al certificado vinculado a la misma.



FAQ (PREGUNTAS/RESPUESTAS FRECUENTES)

12.1 Cómo hago para adherirme al servicio WSASS ?

Para adherirse al WSASS siga los pasos del manual “WSASS: Cómo adherirse al servicio”, publicado en http://www.afip.gob.ar/ws/WSASS/WSASS_como_adherirse.pdf

12.2 Cuando trato de adherirme veo el error “El servicio no es de- legable”

El servicio WSASS no es delegable. Esto significa que para adherirse al servicio WSASS el usuario debe acceder al portal de AFIP, CON SU CLAVE FISCAL DE PERSONA FISICA (no la CUIT de una empresa o persona jurídica).

12.3 Cómo hago para generar un certificado para la CUIT de una empresa?

Los certificados generados por WSASS siempre se emiten para la CUIT de una persona física. Para crear una autorización para una CUIT REPRESENTADA (por ejemplo, la de una empresa) hay que crear una autorización para el certificado, indicando como CUIT REPRESENTADA la de la empresa.

12.4 Al crear un certificado en el WSASS veo el error “Error crean- do certificado”

El error del WSASS “Error creando certificado” puede deberse a varios motivos. El más frecuente es que en el Campo 3 del formulario de creación de certificado nuevo haya pegado un texto que no corresponde a un CSR.

Otro error muy frecuente es que el alias elegido para el nuevo certificado sea el alias de un certificado ya existente. En este caso usted debería usar un alias nuevo.



12.5 Quiero eliminar un certificado que creé, cómo hago eso?

La version actual de WSASS no permite eliminar los certificados creados. Solamente se permite eliminar las autorizaciones de los certificados. De todas formas los mismos pueden permanecer en la base de datos sin inconvenientes, aún cuando hayan expirado.