

Generación de Certificados para Producción

Publicación 1.0

AFIP/SDGSIT/DIOPIN/DESOTE

Índice general

1. Introducción
2. Solicitud del Certificado Digital 3
3. Generación de Solicitud de Certificado utilizando OpenSSL 9
4. Certificados digitales para Entorno de Testing 11

Introducción

El siguiente documento tiene como objetivo mostrar los distintos pasos para la obtención de un certificado digital válido solamente para el entorno de producción. Se presupone que ya se posee clave fiscal de nivel acorde a los servicios que se utilizan, tramitada en una dependencia de ARCA.

Este documento está dirigido a desarrolladores o contactos técnicos de las Empresas o Contribuyentes que necesiten consumir un Webservice provisto por ARCA.

Solicitud del Certificado Digital

Para ejemplificar el procedimiento se utilizará un caso ficticio. En este caso el usuario JOSE PEREZ ROMERO (CUIT 20120940288) es un técnico informático que trabaja para la empresa “EMPRESA DE FACTURACION S.A.” (CUIT 30710955057). La empresa es una firma que brinda servicio de facturación a otras empresas. A su vez factura electrónicamente a sus clientes.

El Administrador de Relaciones de la Empresa le ha delegado a JOSE PEREZ ROMERO el servicio “Administrador de Certificados Digitales”.

1. El Acceso al Sistema se hace ingresando por el portal institucional (<https://www.arca.gob.ar/landing/default.asp>). Deberá ubicar el enlace “Acceso con Clave Fiscal”



2. En la pantalla de autenticación con Clave Fiscal, deberá ingresar la CUIT/CUIL/CDI de su usuario (sin guiones ni separadores de ningún tipo) y a continuación la contraseña en el campo Clave.

 **Ingresar con Clave Fiscal**

CUIT/CUIL

Siguiente

[¿Olvidaste tu clave?](#)

Obtené tu Clave Fiscal

[¿Qué es la Clave Fiscal?](#)

[Ayuda](#)

3. Luego de ingresar se desplegará el listado de Servicios Administrativos habilitados para el usuario. Seleccionar “Ver todos”. El servicio a utilizar se denomina “Administración de Certificados Digitales”. En caso de contar con el servicio, hacer clic sobre el título para acceder.

 **Solicitud de Cuit**

 **Presentaciones Digitales**

 **Administrador de relaciones**

 **Domicilio Fiscal Electrónico**
No tenés notificaciones

¿Qué necesitás? | Buscá trámites y servicios 

Servicios | Más utilizados

Domicilio Fiscal Electrónico	Mis Facilidades	Monotributo	Mis Aplicaciones Web	Ver todos
------------------------------	-----------------	-------------	----------------------	---------------------------

La primera acción a realizar en el servicio, será determinar en nombre de quien se transaccionará.



Bienvenido Usuario JOSE PEREZ ROMERO [20-12094028-8]

Autoridad de Aplicación

Por favor seleccione el contribuyente para el que va a operar este servicio

- Seleccione -

El sistema presenta la pantalla con un desplegable conteniendo todas las personas que han autorizado al usuario para Administrar sus Certificados Digitales. Para más información acerca de la Delegación de este y cualquier otro servicio, remitirse al instructivo de utilización del Administrador de Relaciones.

En este ejemplo la empresa “EMPRESA DE FACTURACION S.A.” es la empresa que utilizará los Webservices, por lo tanto es la empresa que solicitará el Certificado Digital. Se deberá seleccionar entonces a “EMPRESA DE FACTURACION S.A.” del desplegable.

NOTA: En el caso de que el mismo usuario sea el que solicita el certificado digital, y ninguna otra persona le hubiera delegado el servicio, esta pantalla es omitida por el sistema, ya que el usuario solo podría seleccionarse a sí mismo.

5. Inicialmente la pantalla se presenta vacía, ya que la persona no tiene Certificados Digitales habilitados. Para solicitar un nuevo certificado digital, deberá presionar el botón “Agregar Alias”

Usted está solicitando un certificado con las siguientes características

CUIT 30-71095505-7	←	El certificado es solicitado por esta persona.
---------------------------	---	--

Alias

Para obtener un nuevo certificado, debe subir un CSR (Certificate Signing Request) en formato PKCS#10.

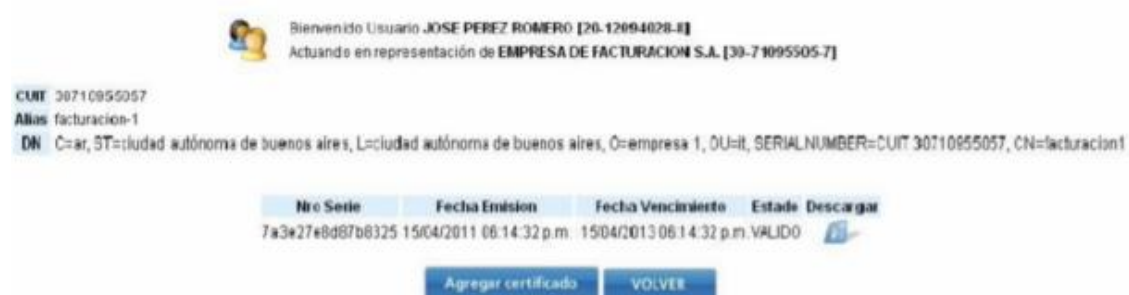
6. La solicitud de un nuevo certificado le requiere que ingrese dos datos. El Alias del certificado y un archivo CSR. El alias es el nombre descriptivo que la persona quiera para distinguir sus certificados. Internamente ARCA asociará al Alias del certificado, la CUIT de la persona solicitante.

NOTA: El archivo CSR es un archivo de texto que puede ser generado con cualquier herramienta de algoritmos de Seguridad, como por ejemplo OpenSSL (<http://www.openssl.org>). En este caso el Alias elegido es "facturacion-1".

7. Luego de completar el alias y subir el archivo CSR, el sistema muestra la pantalla inicial, ahora con el nuevo certificado solicitado.



8. Al seleccionar la opción de Ver el detalle del certificado, el sistema trae la información que contenía la solicitud generada.



En la primera sección de la página muestra los datos identificatorios del Computador Fiscal: CUIT, Alias, y DN (Distinguish Name). La segunda tabla tiene el listado de certificados digitales asociados al computador. Utilizando el icono "Descargar" podrá obtener el certificado digital emitido (Archivo CRT), que en conjunto con la Clave Privada generada al momento de realizar la solicitud, podrá compilar para generar el Certificado Digital (Archivo PFX) instalable en su equipo.

Los certificados emitidos por AFIP tienen una vigencia establecida al momento de la emisión. Una vez vencidos ya no podrá operar más con ese certificado. Para continuar utilizándolo deberá solicitar un nuevo certificado asociado a ese computador fiscal. Para esto, deberá utilizar el botón "Agregar Certificado". Este botón lo remite a la pantalla de solicitud de Certificado, donde deberá consignar el mismo Alias y enviar un nuevo CSR para la generación de un nuevo certificado. Se sugiere verificar la fecha de vigencia del certificado emitido para planificar su renovación con anticipación.

Generación de Solicitud de Certificado utilizando OpenSSL

Básicamente, necesita usar el utilitario OpenSSL. Si tiene acceso a un servidor Unix/Linux, seguramente, ya lo tiene instalado. Si sólo tiene acceso a equipos Windows, puede bajar openssl de:

<http://www.slproweb.com/products/Win32OpenSSL.html>

<http://www.openssl.org>

1. Generar Clave Privada (Private Key) de 2048 bits. Desde la línea de comando, ubicado en el directorio de instalación de OpenSSL, ejecutar:

```
openssl genrsa -out privada 2048
```

Haga un backup de su clave privada para evitar futuros inconvenientes. Tenga en cuenta que la va a necesitar una vez que obtenga su certificado X.509, el cual no le va a servir de mucho si usted no dispone de la clave privada que le corresponde.

2. Generar el Pedido CSR (Certificate Signing Request). Desde la línea de comando, ubicado en el directorio de instalación de OpenSSL, ejecutar:

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

Para ejecutar el comando, deberá reemplazar: subj_o por el nombre de su empresa, subj_cn por su nombre o server hostname, y subj_cuit por la CUIT sin guiones de la empresa o programador.

IMPORTANTE: En el serialNumber se escribe el texto "CUIT", luego un espacio en blanco y a continuación el número de CUIT (sin guiones).

Según la tecnología que elija utilizar para llevar a cabo el desarrollo puede llegar a necesitar el certificado en formato pkcs12 (certificado x509 + clave privada). Por ejemplo, con para cliente en .NET. Para generarlo debe ejecutar desde la línea de comando:

```
openssl pkcs12 -export -inkey privada -in certificado.crt -out alias.p12
```


En algunos equipos Windows al invocar al WSAA para obtener su ticket de acceso puede llegar a obtener el siguiente mensaje de error: “La contraseña de red especificada no es válida”. Este error tiene que ver con el problema de que Windows parece no entender que el pkcs#12 generado con openssl no tiene password. La solución es importar el certificado al repositorio de Windows (Control panel/Internet Options/Contents/Certificates). Luego volver a exportarlo (hasta la versión 7 de Internet Explorer no es obligatorio ponerle password). Tener en cuenta que debe tildar la opción “Marcar esta clave como exportable”.

3. Utilizar el Certificado Digital. Una vez que haya generado correctamente su CSR, puede usarlo para obtener su certificado digital X.509, utilizando las instrucciones de este Documento Técnico. Luego deberá asociar el certificado al Web Service de Negocio que necesite, usando el servicio “Administrador de Relaciones de Clave Fiscal”. Para más información, por favor remitase al manual del Administrador de Relaciones.

Para los desarrolladores que deseen probar sus aplicaciones que consuman de los webservices de ARCA (en nuestro entorno de Testing), se dispone de la aplicación web WSASS (Autogestión de certificados para Servicios Web en los ambientes de homologación). WSASS permite al usuario gestionar sus certificados para el Entorno de Testing exclusivamente.

NOTA: Para poder acceder al WSASS, deberá solicitarse a través del sitio ARCA (www.arca.gob.ar) autenticándose con Clave Fiscal. Para más información dirigirse a nuestro micrositio <http://www.arca.gob.ar/ws/>