Tutorial para la solicitud de certificados de aplicación

AC ONTI

Por favor lea atentamente el instructivo completo antes de comenzar el procedimiento

1. Objetivo

Describir el proceso necesario para generar un CSR, realizar la solicitud y obtener un Certificado de Aplicación ante la AC ONTI.

2. Definiciones

AC ONTI: Autoridad Certificante de la Oficina Nacional de Tecnologías de Información. También referido como "Certificador".

PUC: Política Única de Certificación.

KEY: Se llama así a la clave privada necesaria para firmar.

CSR: Certificate Signing Request. Se utiliza para solicitar un certificado digital a una Autoridad Certificante. Contiene la clave pública asociada a la clave privada y la información que irá en el certificado.

AVISO

Realizar la presentación del CSR y la nota de solicitud no implica obligación de emisión por parte de la AC ONTI.

La emisión de todos los certificados de aplicación será sujeta a revisión y aprobación por parte de la Dirección Nacional de Firma Digital e Infraestructura Tecnológica.

Al realizar la solicitud de un certificado de aplicación el responsable del área solicitante acepta y se compromete a utilizar el certificado de acuerdo con los términos y condiciones establecidos en la Política Única de Certificación V4.0 de AC ONTI, el Acuerdo con Suscriptores v4.0 de AC ONTI y documentos vigentes complementarios.

3. Desarrollo

Etapa 1: Creación de la Key y el CSR

Para generar la clave y la CSR necesarias para realizar la solicitud, deberá utilizar una herramienta capaz de generar claves públicas, claves privadas y solicitudes de certificado.

En este tutorial, utilizaremos la aplicación de código abierto "OpenSSL" (https://www.openssl.org/) en su versión v1.1.1, aunque puede emplear la versión que prefiera. Tenga en cuenta que si utiliza otro software, los comandos pueden variar.

Si necesita un instalador simple para Windows, puede descargarlo desde el siguiente enlace (la versión Light es suficiente):
https://slproweb.com/products/Win32OpenSSL.html

No es obligatorio utilizar dicho instalador.

Para que su solicitud sea considerada y aprobada por el certificador, debe cumplir con el Perfil de Certificado de Aplicaciones de la Política Única de Certificación v4.0 de AC ONTI. El tamaño de las claves debe ser RSA de 2048 bits (Subject Public Key Info, pág. 54) y la información contenida en el CSR debe respetar los puntos indicados en Subject DN (campos 2.5.4.3, 2.5.4.5, 2.5.4.6, 2.5.4.10 y 2.5.4.11, pág. 54).

Consideraciones sobre el procedimiento:

- Se sugiere escribir manualmente los comandos. Algunas versiones de OpenSSL presentan inconvenientes al copiar y pegar comandos
- Cada campo de la solicitud no debe superar los 64 caracteres.
- Al seleccionar la ruta para la creación de KEY y CSR, asegúrese de que las carpetas de dicha ruta estén previamente creadas antes de ejecutar el comando. Elija rutas que no contengan espacios para minimizar posibles errores
- El certificado no debe incluir campos adicionales a los especificados en el perfil de certificado de aplicaciones de la PUC v4.0 de AC ONTI

Utilice la siguiente línea de comandos, adaptándola para indicar la ruta donde se guardarán los archivos generados y completando los datos del certificado:

> OpenSSL req -newkey rsa:2048 -nodes -keyout C:\Nombre_Carpeta\Nombre_Archivo.key -subj "/CN=Nombre o uso de la aplicacion/O=Nombre organismo solicitante/OU=Unidad del Organismo responsable del certificado/serialNumber=CUIT XXXXXXXXXXX/C=AR" -out C:\Nombre_Carpeta\Nombre_Archivo.csr

Dónde:

Req: Indica que se realizará una solicitud de certificado (CSR).

-newkey rsa:2048: Genera un nuevo par de clave pública/privada RSA de 2048 bits.

-nodes: Opcional. Indica que la clave privada no debe cifrarse con una contraseña.

-keyout C:\Nombre_Carpeta\Nombre_Archivo.key: Especifica la **carpeta** y el **nombre del archivo** donde se guardará la clave privada generada. Ambos son a elección del usuario.

-subj: Declara los valores de la aplicación y el organismo responsable:

CN = Debe poder identificarse claramente el nombre de la aplicación o el uso que tendrá el certificado.

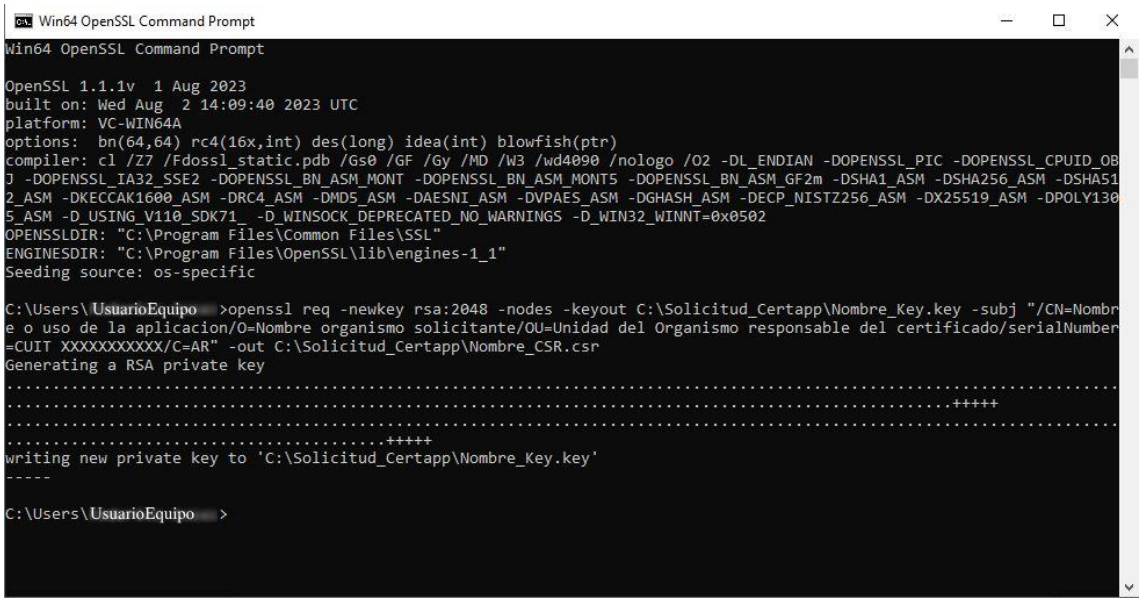
serialNumber = CUIT del organismo solicitante. Separado con espacio de la sigla "CUIT" y sin guiones.

O = Nombre del organismo solicitante. Debe coincidir con la razón social asociada al CUIT ingresado en "serialNumber".

OU = Nombre legal del área dentro del organismo responsable del certificado. La nota de solicitud deberá ser firmada digitalmente por el responsable del área o superior.

C= Debe contener "AR".

-out C:\Nombre_Carpeta\Nombre_Archivo.csr: Especifica la **ruta** y el **nombre del archivo** donde se guardará la solicitud de certificado (CSR) generada. Ambos son a elección del usuario.



Cuando haya modificado el comando y revisado la información de solicitud, busque el Command Prompt de OpenSSL y ejecútelo.

Una vez finalizado, se habrán generado dos archivos en la carpeta especificada como ruta: uno con extensión ".key" (clave privada) y otro con extensión ".csr" (solicitud de certificado). El archivo ".csr" es el que deberá enviar en el siguiente paso.

Tenga en cuenta que, una vez que obtenga su certificado, la aplicación firmará con esa clave privada, por lo que **es de extrema importancia que el archivo ".key" no se comparta con absolutamente nadie para asegurar el uso exclusivo del certificado del organismo/área solicitante.**

IMPORTANTE

NO comparta su clave privada (KEY) con NADIE, ni siquiera con AC ONTI.
Solo envíe la solicitud de certificado (CSR).

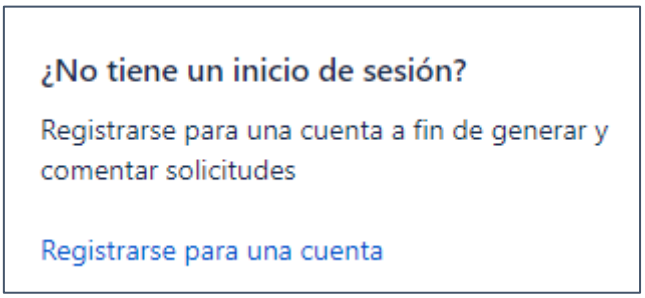
Etapa 2: Solicitud de certificado a la AC ONTI

2.1 – Presentación de CSR a través de JIRA

Al generar el CSR, tendrá la mitad de la solicitud completada. Solo falta enviarlo para su revisión a la AC ONTI junto con una nota de solicitud. Si todo es correcto y resulta aprobado, se emitirá su certificado.

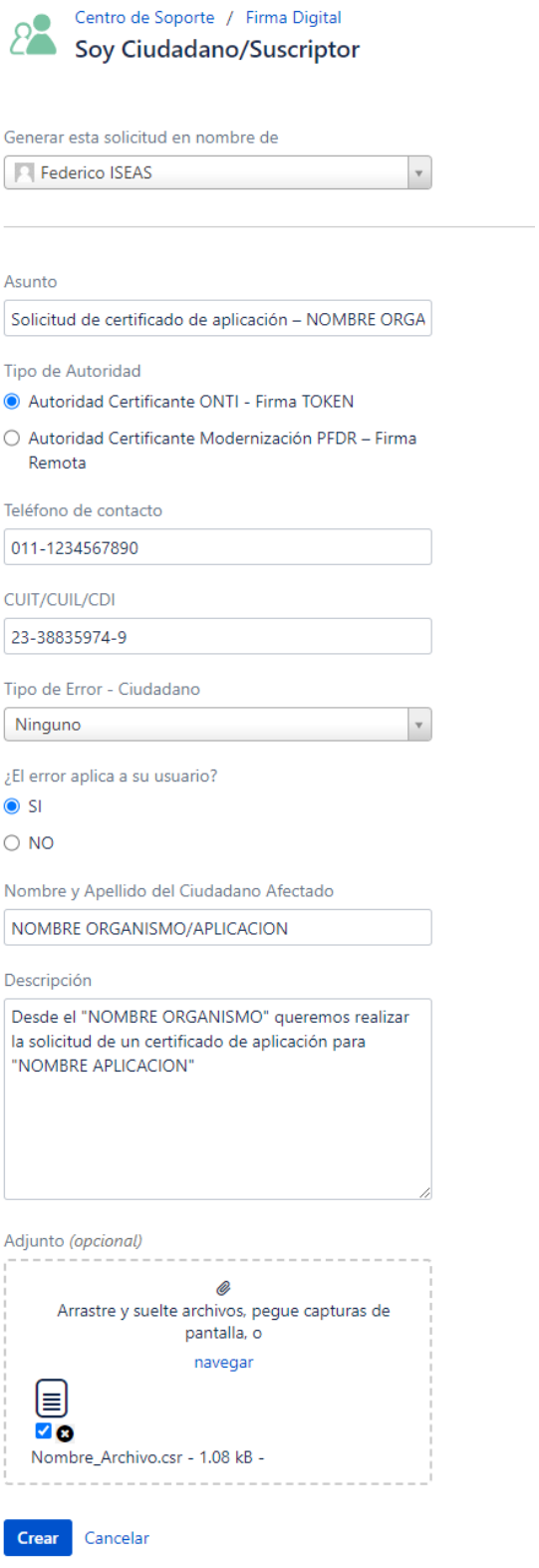
La presentación debe realizarse a través del sistema de incidencias JIRA que proporciona la AC ONTI para comunicarse con el certificador. Puede acceder a través del siguiente enlace: https://incidencias.innovacion.gob.ar/servicedesk/customer/portal/16.

Para cargar una nueva incidencia, deberá crear un usuario en la plataforma por única vez haciendo clic en **"Registrarse para una cuenta"**.

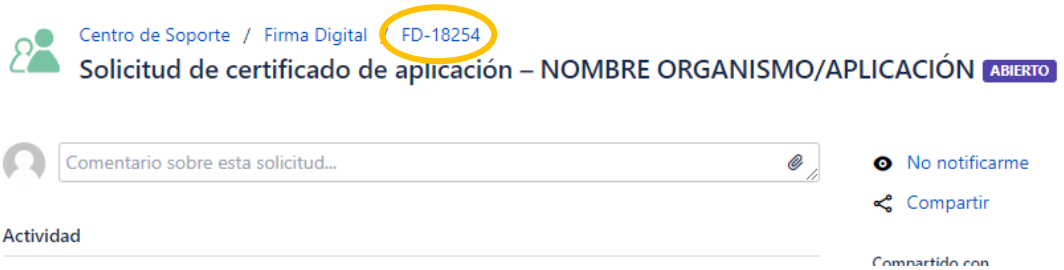


Una vez que ingrese con su usuario, el sistema le permitirá comenzar la carga. Seleccione **"Soy Ciudadano/Suscriptor"** o **"Sugerencias"** para proceder.

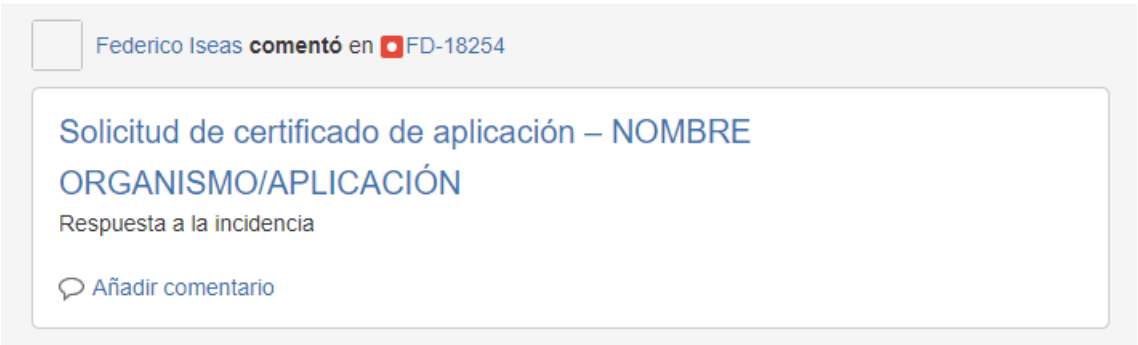
En “Asunto” / “Resumen”, escriba “Solicitud de certificado de aplicación – NOMBRE ORGANISMO/APLICACIÓN” y cargue sus datos. Al final del formulario, podrá añadir como adjunto el archivo CSR que generó en la **Etapa 1**.



Al hacer clic en “Crear”, se cargará la incidencia y deberá aguardar una respuesta. La misma tendrá un código identificador que comienza con “FD-XXXXX”, donde X representa el número de la incidencia. Guarde este dato, ya que será importante para realizar la nota de solicitud.



Cuando su solicitud sea atendida y el encargado de atención le responda, recibirá otro correo notificándolo. Para responder **no lo haga por correo electrónico**; debe hacerlo ingresando nuevamente a JIRA. Para ello, haga clic en el título de la incidencia o en **“Añadir comentario”:**



2.2 – Presentación de nota de solicitud

Puede solicitar el modelo de nota de solicitud a través de la incidencia o utilizar el siguiente:

XX(DIA), de XX(MES) de XXXX(AÑO)

REF: SOLICITUD DE EMISIÓN DE CERTIFICADO DE APLICACIÓN.

AL RESPONSABLE DE LA AUTORIDAD CERTIFICANTE DE LA

OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN

S / D

Tengo el agrado de dirigirme a Ud. en relación a la solicitud de un certificado de aplicación para XXXXXXXXXXXX(Nombre aplicación y organismo), cuyo CSR (Certificate Signing Request) se adjunta en la incidencia FD-XXXXX y cuyo digesto SHA256 es: "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

Sin otro particular, saludo a usted atentamente.

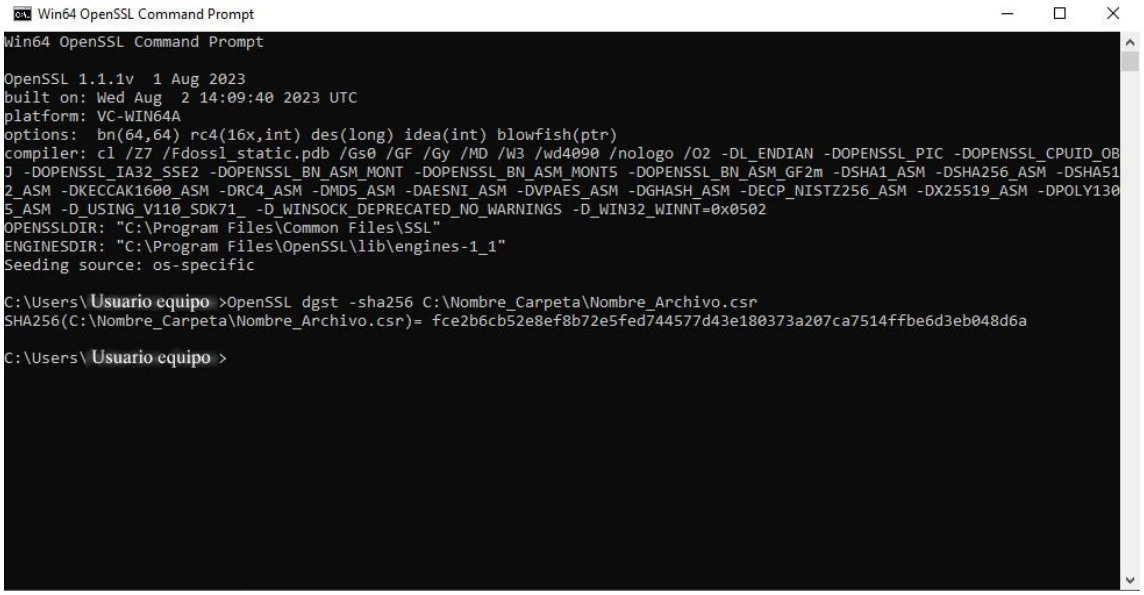
.....

Firma, Aclaración y DNI

(Cargo del responsable del área que solicita el certificado de aplicación)

Puede calcular el digesto SHA256 de la CSR con la aplicación que prefiera. En este caso, lo calcularemos desde OpenSSL con el siguiente comando:

> OpenSSL dgst -sha256 C:\Nombre_Carpeta\Nombre_Archivo.csr



Una vez completado, adjunte el borrador de la nota (sin firmar) a la incidencia para que sea revisado por el responsable de atención de AC ONTI.

Sólo cuando el responsable de atención confirme que la información es correcta, la nota deberá ser **firmada digitalmente por el responsable del área solicitante** (Campo “2.5.4.11” o “OU” de la información colocada en el CSR).

Si el responsable del área o superior **tiene firma digital** (de persona humana, NO con otro certificado de aplicación) puede:

- **Firmar y subir la nota:** Convertir la nota a PDF, firmarla digitalmente con la aplicación de su preferencia y cargarla a la incidencia JIRA.
- **Presentarla por GDE:** Generar una Nota a través del módulo de Comunicaciones Oficiales de GDE firmada digitalmente con **firma token** o **firma remota** por la autoridad del área responsable de la aplicación o superior. El destinatario de la nota debe ser Federico Iseas (FISEAS DNFDEIT#JGM). Esto les devolverá un número de GDE que deberán guardar y **comunicarlo en la incidencia JIRA**.

Si el responsable del área o superior **no tiene firma digital**:

- Deberá ingresar al siguiente trámite: https://tramitesadistancia.gob.ar/tramitesadistancia/detalle-tipo?id=2050 e iniciar sesión con su clave fiscal de **AFIP** o credenciales de **miArgentina**. Allí deberá adjuntar un escaneo o foto de la nota de solicitud, la cual debe incluir la firma, aclaración, cargo y DNI del responsable de área. Una vez presentada la documentación, **informe a través**

de JIRA el número de expediente generado. También puede descargar la nota y adjuntarla a la incidencia.

Etapa 3: Emisión y recepción de certificado

Si su solicitud recibe la aprobación por parte de la Dirección Nacional de Firma Digital e Infraestructura, la AC ONTI emitirá el certificado y el mismo será enviado en un archivo comprimido a través de la incidencia JIRA generada. No se envían certificados por otro medio.

Una vez obtenga su certificado, el procedimiento ante AC ONTI se da por **finalizado**.

Para usar mi certificado necesito crear un PFX, ¿Cómo lo genero?

Este procedimiento ya no corre por responsabilidad de la AC ONTI sino del área solicitante. Sólo figura en este tutorial a raíz de las consultas comunes luego de obtener el certificado.

Una vez que obtenga su certificado cópielo en la misma carpeta que contiene la clave privada (key) que generó al comienzo del tutorial. Luego ejecute la siguiente línea de comandos en OpenSSL:

```
OpenSSL pkcs12 -export -out C:\Nombre_Carpeta\Nombre_Archivo.pfx -inkey
C:\Nombre_Carpeta\Nombre_Archivo.key -in C:\Nombre_Carpeta\Nombre_Archivo.cer
```

Dónde:

pkcs12 -export: Indica que se realizará una operación de exportación de un archivo PKCS#12.

-out C:\Nombre_Carpeta\Nombre_Archivo.pfx: Especifica la **carpeta** y el **nombre del archivo** con extensión ".PFX" que se exportará.

-inkey C:\Nombre_Carpeta\Nombre_Archivo.key: Especifica la **carpeta** y el **nombre del archivo** con extensión ".KEY" que contiene la clave privada.

-in C:\Nombre_Carpeta\Nombre_Archivo.cer: Especifica la **carpeta** y el **nombre del archivo** con extensión ".CER" que contiene el certificado emitido por AC ONTI.

Se le pedirá que indique una contraseña para proteger el certificado. Recuérdela.

Como resultado, se habrá generado en la carpeta indicada el archivo PFX que necesita para instalar y utilizar el certificado en su aplicación.