Secretaría de Innovación, Ciencia y Tecnología
Jefatura de Gabinete de Ministros

Manual de Usuario para Oficiales de Registro y Responsables de Soporte Técnico

AC ONTI

Tabla de Contenidos

1. Glosario

Autoridad Certificante (AC): Organismo público o privado autorizado por el Ente Licenciante para emitir certificados digitales otorgando a estos validez legal.

Autoridad de Registro (AR): Oficina encargada de verificar la identidad de las personas solicitantes de un certificado digital y autorizar a la Autoridad Certificante para su emisión.

Oficial de Registro (OR): Responsable de validar la identidad de las personas, titularidad de la clave pública y aprobar y rechazar las solicitudes de certificados y su revocación.

Responsable de Soporte Técnico de Firma Digital (ST): Encargado de difundir el uso de la firma digital en el organismo, capacitar sobre buenas prácticas, verificar el cumplimiento técnico y reportar incidencias.

Responsable de Autoridad de Registro (RA): Responsable legal y nexo formal entre la Autoridad de Registro y la Autoridad Certificante. Supervisa el cumplimiento de la normativa e informa cualquier modificación.

Solicitante: Toda persona humana que realiza una solicitud de certificado a su nombre.

Suscriptor: Solicitante a cuyo nombre el certificador le emite un certificado, y que posee una clave privada que se corresponde con la clave pública contenida en el mismo.

Tercer usuario: Persona humana o jurídica que recibe un documento firmado digitalmente y verifica la validez del certificado para confirmar la autenticidad del documento.

Sitio web de la AC - ONTI: Consiste en la aplicación disponible en Internet provista por el Certificador destinada, principalmente, a la gestión de las solicitudes y revocación de certificados.

2. Introducción

El Sitio web de la AC - ONTI (https://pki.jgm.gov.ar/ar/default.aspx), en adelante **web del certificador**, se utiliza para la solicitud y revocación con presencia física de certificados de clave pública considerados de Firma Digital por la Ley 25506.

3. Fase Inicial: Solicitud de certificado

Para que un suscriptor potencial pueda utilizar su certificado de firma digital token, primero debe realizarse un registro inicial y validación de datos biométricos de carácter presencial ante un Oficial de Registro (OR) en una Autoridad de Registro (AR).

3.1. Requisitos Previos (Oficial de registro)

Capacitación: Haber realizado y aprobado el curso de capacitación para el rol correspondiente dictado o autorizado por la Dirección de Firma Digital dependiente de la Dirección Nacional de Firma Digital e Infraestructura Tecnológica de la Subsecretaría de Innovación dependiente de la Secretaría de Innovación, Ciencia y Tecnología de la Nación.

Enrolamiento: Haber finalizado la tramitación de la solicitud de designación mediante expediente, con la designación de rol firmada, según los requisitos indicados por la Dirección mencionada anteriormente. El enrolamiento consiste en asignar los permisos necesarios al agente para que pueda ejercer su rol como Oficial de Registro dentro de la web del certificador.

Puesto de trabajo en Autoridad de Registro: Debe tener un lugar de trabajo asignado en la Autoridad de Registro que le corresponda con los elementos necesarios para poder ejercer su rol correctamente (Computadora configurada según especificaciones, acceso a internet, driver del token del OR instalado, cámara web y lector de huellas).

3.2. Requisitos Previos (Solicitante)

Documento Nacional de Identidad (DNI): Debe estar vigente. Puede ser físico o digital desde la aplicación de miArgentina.

Completar la nota de envío de datos de solicitud: Debe completar y confirmar vía correo electrónico el formulario de solicitud de certificado con sus datos personales tal cual lo indica el DNI (nombre, apellido, tipo de documento, número de documento, país emisor, CUIT/CUIL), declarar correo personal, y seleccionar el provincia y localidad según lugar de residencia.

Seleccionar Autoridad de Registro: El solicitante deberá seleccionar también en el formulario la Autoridad de Registro donde realizará la solicitud de su certificado.

Aceptar acuerdo con suscriptores: Leer y aceptar el Acuerdo de Suscriptores, declarando haber tomado conocimiento de su contenido. Finalmente, enviar los datos de la solicitud del certificado correspondientes al formulario completado.

Confirmación de correo electrónico: El enlace de verificación de la dirección de correo tiene una vigencia de 24 horas. Transcurrido ese plazo, si el solicitante no confirma el correo, la solicitud se rechaza automáticamente y deberá iniciarse una nueva carga.

Una vez verificado tendrá una vigencia de 20 días hábiles. Superado dicho plazo sin completarse el trámite, la nota se rechazará automáticamente y el solicitante deberá volver a cargar sus datos.

IMPORTANTE: Un mismo solicitante no puede tener más de una solicitud pendiente de manera simultánea.

Dispositivo criptográfico token: El mismo debe cumplir con el estándar FIPS 140-2 nivel 2 o superior o FIPS 140-3 nivel 2 o superior, que soporte claves RSA de 2048 bits. Deberá tener certificación NIST (National Institute of Standards and Technology) en estado ACTIVO o, para suscriptores que no sean Oficial de Registro, en estado HISTÓRICO hasta 3 años del pase a dicha clasificación de acuerdo a lo establecido en la Política Única de Certificación de la AUTORIDAD CERTIFICANTE de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (AC ONTI).

Presencia física: Es requisito que la persona que va a gestionar su certificado de firma digital se presente de manera presencial ante la Autoridad de Registro declarado en la nota de envío de datos.

4. Tratamiento de solicitud de certificado por parte del Oficial de Registro

Al presentarse un solicitante en la Autoridad de Registro, el Oficial de Registro (OR) llevará a cabo las siguientes acciones:

Verificación de requisitos del solicitante: Se verifica que el solicitante cumpla con los requisitos para iniciar el trámite, es decir, verificando su presencia física, DNI, que tenga una solicitud cargada para esa Autoridad de Registro y derivando la verificación del dispositivo criptográfico token con el Responsable de Soporte Técnico.

IMPORTANTE: En caso de que el ST determine que el dispositivo no es válido, no se podrá continuar con el trámite y el solicitante deberá adquirir un nuevo dispositivo criptográfico que cumpla con los requisitos establecidos por el certificador.

Aceptación o Rechazo de solicitud de envío de datos: El OR deberá acceder a la Web de Firma Digital desde el navegador Google Chrome o desde un navegador

basado en Chromium, como Microsoft Edge, teniendo conectado al equipo su dispositivo criptográfico (token).

Una vez dentro del sitio web del certificador, deberá ingresar a la opción “Buscar solicitudes y certificados” del menú de Oficial de Registro, buscar la Nota de Envío de Datos previamente cargada por el solicitante y verificar que toda la información cargada sea correcta, incluyendo nombre y apellido, DNI, CUIL y demás datos requeridos.

IMPORTANTE: En caso de detectar inconsistencias o errores en la información, el OR deberá proceder al rechazo de la solicitud.

Validación biométrica: El OR se identifica ante el sitio de biométrico firmando digitalmente con su token. Se deberá seleccionar sexo del solicitante, se tomará una fotografía digital del rostro, declarar si existe imposibilidad física y se registrarán las huellas dactilares para ser validadas contra el servicio de datos del Registro Nacional de las Personas (RENAPER).

Solicitar certificado: Finalizada la validación de datos biométricos, el solicitante debe tildar el cuadro de verificación que ha verificado que los datos de la nota de envío de datos son correctos y que desea continuar con el trámite de solicitud de su certificado y hace clic en el botón “Solicitar certificado”.

4.1. Generación del par de claves

Selección de proveedor de servicio criptográfico: Luego de la verificación del dispositivo criptográfico (token) por parte del ST, el OR deberá conectar el token del suscriptor a su computadora. Es requisito que la computadora del OR tenga instalado el driver correspondiente al token del solicitante para que el dispositivo pueda ser correctamente reconocido. Una vez detectado, el OR deberá realizar la selección del proveedor criptográfico.

Aceptación de Acuerdo con Suscriptores: El solicitante debe declarar haber leído y aceptado el acuerdo con suscriptores.

Generar claves y solicitar certificado: El solicitante deberá seleccionar la opción “Generar claves y solicitar certificado” para que el sistema genere el par de claves criptográficas correspondiente. Para autorizar la generación, el solicitante deberá ingresar el PIN del token previamente configurado.

4.2. Aprobación de certificado

Validación de identidad y validación de clave pública: La forma técnicamente correcta de validar la clave pública es mediante la verificación del hash de la solicitud. El sitio web del certificador muestra el hash de la solicitud, el cual identifica de manera unívoca la solicitud y, en consecuencia, la clave pública contenida en la misma, que fue enviada a la Autoridad Certificante (AC).

El OR debe conectar su token y proceder a firmar digitalmente la aprobación de la solicitud de certificado del solicitante.

IMPORTANTE: El OR solo debe aprobar la solicitud siempre que el trámite no haya sido interrumpido desde el momento en que el solicitante realizó la solicitud hasta la instancia de aprobación por parte del mismo.

5. Emisión del Certificado de la AC ONTI

Una vez que el certificado se encuentre emitido se actualizará el sitio y el OR con el token suscriptor conectado deberá instalar el certificado haciendo clic en "Instalar certificado" y aguarde la confirmación. Una vez instalado podrá dar en "Finalizar".

Cuando se emite el certificado, el sistema envía un correo electrónico a la dirección previamente declarada por el titular, informando la emisión del certificado, el número de serie correspondiente y el PIN de revocación, el cual se recomienda conservar a fin de dar de revocar su certificado de firma si lo necesita.

6. Revocación del Certificado

La revocación es la anulación definitiva del certificado antes de su vencimiento. Debe hacerse en caso de robo de identidad, pérdida de factores de seguridad o compromiso de las claves o simplemente si el suscriptor desea darse de baja. La AC ONTI ofrece tres métodos de revocación de un certificado de firma digital.

6.1. Revocación con PIN de Revocación

Al emitirse el certificado, se envía un código especial por correo. Puede usarlo para revocar el certificado por uno mismo desde el sitio web del certificador.

Proceso para revocación de certificado con PIN de revocación: El suscriptor debe acceder al correo que previamente le llegó cuando se emitió su certificado. Copiar su PIN de revocación e ingresar al enlace provisto del sitio web del

certificador para avanzar con el proceso de revocación. Esta opción de revocación también está disponible en el siguiente enlace: https://www.argentina.gob.ar/revocar-certificado-con-pin-de-revocacion

Ingresar PIN de Revocación: Deberá pegar su PIN de revocación y escribir su número de DNI.

Seleccionar el motivo de la revocación: El usuario deberá seleccionar el motivo de la revocación y, de manera opcional, ingresar un comentario adicional.

Completar Captcha: Deberá escribir el captcha que le muestro el sitio y finalmente seleccionar la opción “Revocar”.

Confirmación de solicitud de revocación: El sistema mostrará un mensaje de confirmación indicando: “Atención: esta operación no se puede deshacer. ¿Está seguro de que desea revocar el certificado?”. Al confirmar la acción, el sistema procederá a revocar el certificado.

Una vez completado el proceso, el solicitante recibirá un correo electrónico notificando la revocación de su certificado.

6.2. Revocación con clave privada

El suscriptor debe ingresar a la página oficial de la Autoridad Certificante en la sección “Revocación con Clave Privada” desde el siguiente enlace:

https://www.argentina.gob.ar/jefatura/innovacion-publica/innovacion-administrativa/firma-digital/autoridad-certificante-de-la-5

Para revocar un certificado utilizando la clave privada, el titular deberá conectar el dispositivo criptográfico (token) a su equipo. En caso de contar con más de un certificado emitido en el token, deberá seleccionar en la pantalla emergente el certificado que desea revocar, manteniendo el dispositivo conectado durante todo el proceso.

Requerimientos tecnológicos: El procedimiento requiere contar con alguno de los siguientes sistemas operativos: Windows Vista, Windows 7, Windows 8, 8.1, Windows 10 o Windows 11. Asimismo, debe encontrarse instalada la cadena de certificación, el Soporte Criptográfico Argentina (el sistema solicitará su instalación al ingresar al sitio) y el driver del dispositivo criptográfico token.

Lectura del dispositivo criptográfico token: El sistema leerá el certificado desde el token y solicitará el ingreso del PIN del dispositivo.

Seleccionar el motivo de la revocación: Se visualizarán los datos del certificado. El usuario deberá seleccionar el motivo de la revocación y, de manera opcional, ingresar un comentario adicional. Finalmente seleccionar la opción “Revocar”.

Confirmación de solicitud de revocación: El sistema mostrará un mensaje de confirmación indicando: “Atención: esta operación no se puede deshacer. ¿Está seguro de que desea revocar el certificado?”. Al confirmar la acción, el sistema procederá a revocar el certificado.

Una vez completado el proceso, el solicitante recibirá un correo electrónico notificando la revocación de su certificado.

6.3 Revocación con Presencia física

Si no se tiene acceso al PIN de Revocación, o extravío su dispositivo criptográfico token debe acudir a una Autoridad de Registro para que un OR realice la revocación tras validar su identidad.

Proceso de revocación presencial: El OR debe acceder al sitio web del certificador y desde la solapa "Oficial de Registro" seleccionar la opción "Revocación con presencia física", allí puede buscar el certificado por Apellido y DNI.

Validación biométrica: El OR se identifica ante el sitio de biométrico firmando digitalmente con su token. Se deberá seleccionar sexo del solicitante, se tomará una fotografía digital del rostro, declarar si existe imposibilidad física y se registrarán las huellas dactilares para ser validadas contra el servicio de datos del Registro Nacional de las Personas (RENAPER).

Aprobar la solicitud de revocación: El OR debe conectar su token a la computadora y proceder con la aprobación de la solicitud de revocación del suscriptor ingresando el PIN del token. El sistema mostrará un mensaje de confirmación indicando: “Atención: esta operación no se puede deshacer. ¿Está seguro de que desea revocar el certificado?”. Al confirmar la acción, el sistema procederá a revocar el certificado.

IMPORTANTE: El suscriptor puede solicitar la revocación de su certificado ante cualquier Autoridad de Registro sin importar dónde lo solicitó previamente.

Una vez completado el proceso, el solicitante recibirá un correo electrónico notificando la revocación de su certificado.

IMPORTANTE: El OR sólo interviene en la revocación presencial, pero es necesario que conozca las demás opciones para informar al suscriptor correctamente.

7. Olvido de PIN del dispositivo criptográfico token:

No existe un método de recuperación del PIN, únicamente es posible la generación de uno nuevo.

En caso de olvido del PIN, el suscriptor deberá presentarse de manera presencial, exhibiendo su DNI y el dispositivo criptográfico (token) siempre y cuando cumpla con los requisitos previamente mencionados, a fin de iniciar nuevamente el trámite desde el comienzo.

8. Solicitud de asistencia

Ante cualquier inconveniente con el sitio web del certificador el OR o ST deben generar un ticket con la AC para ser tratado desde:

https://incidencias.innovacion.gob.ar/servicedesk/customer/portal/16

Ingreso a la mesa de ayuda de firma digital: Para crear una incidencia en el Centro de Soporte de Firma Digital el OR/ST debe ingresar al centro de soporte desde el portal correspondiente e Iniciar sesión con usuario y contraseña. Si es la primera vez, debe registrarse con un correo electrónico válido.

Cargar una incidencia: Una vez dentro, seleccionar el perfil que corresponda: Oficial de Registro o Soporte Técnico y cargar el asunto, la misma debe contener una descripción breve y clara del problema (E: Rechazo de solicitud).

Seleccionar la Autoridad Certificante: Autoridad Certificante ONTI - Firma TOKEN.

Completar el formulario: Seleccionar el nombre de la AR y especificar si es una sede y especificar el tipo de error.

Completar datos del OR: Se debe completar los datos de nombre y apellido, teléfono de contacto y CUIL del OR que levanta la incidencia.

Completar datos del ciudadano afectado: Se debe completar los datos de nombre y apellido y CUIL del ciudadano afectado.

Completar descripción: detallar el inconveniente, incluyendo contexto, mensajes de error y pasos realizados.

Adjuntar archivos: Esto puede ser una capturas de pantalla si es necesario (sin recortar ni modificar las imágenes).

Enviar la incidencia: Se debe finalizar creando para enviar la incidencia. El sistema generará un número de ticket, que permitirá realizar el seguimiento del caso desde la sección “Mis solicitudes” y ante cualquier intercambio de información el OR.

9. Solicitud de Rechazo de nota de envío de datos

En aquellos casos donde el solicitante se dirige a una autoridad de registro distinta a donde cargó y confirmó la nota de envío de datos, el OR debe proceder a realizar un ticket vía mesa de ayuda solicitando a la AC que procedan con el rechazo de la solicitud previamente cargada a fin de que el solicitante pueda cargar nuevamente el formulario declarando la Autoridad de Registro correcta. (ver 8. Solicitud de asistencia)

10. Validación de tokens para OR por Responsable de ST

Una de las funciones del Responsable de Soporte Técnico de Firma Digital es validar los dispositivos criptográficos (token) que utilizarán los Oficiales de Registro. Es decir que deberá identificar y validar dispositivos criptográficos que cumplan con el estándar FIPS 140-2 Nivel 2 o superior o FIPS 140-3 Nivel 2 o superior y que soporten claves RSA de 2048 bits.

Además, los dispositivos deberán contar con **certificación del NIST** (National Institute of Standards and Technology) en estado **“Activo”**, conforme a lo establecido en la Política Única de Certificación de la AC ONTI, requisito obligatorio para los Oficiales de Registro.

El objetivo esencial de esta validación es poder identificar al dispositivo criptográfico que tiene presente físicamente e identificarlo unívocamente (o lo más posible) con una certificación NIST que cumpla los requisitos mencionados y así asegurar que es válido para utilizarse.

Para realizar la verificación, se debe ingresar al sitio oficial del Cryptographic Module Validation Program (CMVP) del NIST y consultar el módulo correspondiente a evaluar:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

Previamente, el Responsable de ST debe realizar una verificación en la página oficial del fabricante con el fin de identificar el dispositivo y si posee la certificación del NIST.

Encontrará información útil para la validación en el driver del dispositivo (por ejemplo, nombre oficial del producto, versión de hardware, firmware, tipo de tarjeta, tipo y tamaño de clave admitido, entre otras dependiendo del dispositivo)

Con la información recabada y con una posible certificación NIST en estado "Activo" del modelo, deberá investigar sobre la manera en que pueda vincular la información del dispositivo y la certificación.

Dependiendo del tipo de tarjeta puede encontrar software que le será de ayuda, como por ejemplo el programa GlobalPlatformPro que se ve en los cursos para tokens de tipo JavaCard u otros similares para otros tipo de tokens.

Si puede vincular correctamente a través de varias características la certificación con la información que muestra el dispositivo, podrá asegurar que el token y la certificación se corresponden y por lo tanto es válido para ser utilizados por Oficiales de Registro.

IMPORTANTE: Los dispositivos criptográficos (tokens) con estado "Histórico" no son válidos para Oficiales de Registro, aun cuando su certificación tenga una antigüedad menor a 3 años.

11. Configuración de computadora por Responsable de ST

El ST es el encargado de garantizar que los puestos de trabajo de la AR cuenten con el equipamiento y la configuración necesarios para la correcta operatoria de los servicios de firma digital.

Computadora con acceso a internet: En términos generales, cualquier computadora que cuente con una cámara web estándar es apta para operar. En caso de que el equipo no disponga de cámara incorporada, deberá instalarse una cámara web externa.

Cámara para captura de fotografía: Para realizar la validación de foto con RENAPER. No se requieren especificaciones técnicas particulares. En el caso de operar con notebooks, podrá utilizarse la cámara integrada del equipo.

Adquisición de dispositivos criptográficos (tokens): Uno por cada Oficial de Registro. El ST debe configurar la computadora del OR descargando el driver del token a ser utilizado por el OR.

Lectores biométricos: Para realizar la validación de huellas con RENAPER. Uno por cada puesto de trabajo. Para verificar los modelos habilitados, se deberán utilizar exclusivamente aquellos que se encuentren homologados y validados para su uso de la AC ONTI. El listado de dispositivos habilitados deberá consultarse en su versión actualizada ante la AC ONTI. (ver 9. Solicitud de asistencia)

Instaladores e instructivos de configuración de lectores:

https://pki.jgm.gov.ar/docs/biometrico.zip

Extensión de navegador "Agile Extensión Argentina": Es requisito fundamental tener instalado la e Extensión Agile para poder operar en el sitio web del certificador:

https://chromewebstore.google.com/detail/kamiiblepfclodiekhefkhpialgmhlkn

Instalador Java JDK8: Se requiere contar con la versión de Java JDK 8 para el uso de la PFDR, la misma puede ser descargada a través del siguiente enlace: https://pki.jgm.gov.ar/docs/jdk8u321x64.exe

Instalador Certificados de la Autoridad Certificante: Estos deben ser descargados de la página oficial de la autoridad certificante. Puede acceder a la misma desde el siguiente enlace: https://www.argentina.gob.ar/servicio/valida-los-documentos-electronicos-firmados-digitalmente

Importante: Es responsabilidad de la organización donde se constituye la Autoridad de Registro asegurar la disponibilidad de todos los roles involucrados en el proceso, así como la correcta prestación de los servicios de la AR a los usuarios de sus sistemas informáticos, garantizando en todo momento la continuidad operativa.

Modificación	Versión	Fecha
Creación del documento	1.0	21/01/2026


JEFATURA DE GABINETE
REPÚBLICA ARGENTINA