ACUERDO CON SUSCRIPTORES

El presente acuerdo entre la DIRECCIÓN NACIONAL DE TRAMITACIÓN E IDENTIFICACIÓN A DISTANCIA de la SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS DE LA NACIÓN (en adelante, DNTEID), en su calidad de administrador de la Autoridad Certificante de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (en adelante AC ONTI) y sus suscriptores, determina los derechos y obligaciones de la partes respecto a la solicitud, aceptación y uso de los certificados emitidos en el marco de la Política Única de Certificación.

1. SOLICITUD DE CERTIFICADO Y DESCRIPCIÓN DE LOS CERTIFICADOS

a) Solicitud de Certificado.

Podrán ser suscriptores de los certificados emitidos por la AC ONTI las personas humanas, que requieran un certificado digital para firmar digitalmente cualquier documento o transacción, pudiendo ser utilizados para cualquier uso o aplicación, como así también para autenticación o cifrado. La AC ONTI emite también un certificado para ser usado en relación con el servicio On Line Certificate Status Protocol (en adelante, OCSP) de consulta sobre el estado de un certificado. Asimismo, la AC ONTI emite certificados de aplicación, y presta el servicio de sello de tiempo, según lo dispuesto en el artículo 9° de la Resolución MM N° 399-E/2016 del 5 de octubre de 2016 del entonces MINISTERIO DE MODERNIZACIÓN.

b) Descripción y Aplicabilidad de los Certificados emitidos por la AC ONTI.

Las claves correspondientes a los certificados digitales que se emitan bajo la presente Política Única de Certificación podrán ser utilizadas en forma interoperable en los procesos de firma digital de cualquier documento o transacción y para la autenticación o el cifrado. Las claves criptográficas de los suscriptores de certificados de personas humanas son generadas por hardware (nivel de seguridad alto) y almacenada por ellos. En este último caso los dispositivos criptográficos utilizados deben ser FIPS 140-2 Nivel 2 o superior. En el caso de las AR, cada Oficial de Registro genera y almacena su par de claves utilizando un dispositivo criptográfico FIPS 140-2 Nivel 2 o superior. Las claves criptográficas utilizadas por los proveedores de otros servicios relacionados con la firma digital serán generadas y almacenadas por módulos criptográficos de software o utilizando dispositivos criptográficos FIPS 140-2 Nivel 2 o superior (hardware).

2. SOLICITUD DE CERTIFICADO Y SU PROCESAMIENTO.

Las solicitudes sólo podrán ser iniciadas por el solicitante, en el caso de certificados de personas humanas, o bien por el representante legal o apoderado con poder suficiente a dichos efectos, o por el Responsable del Servicio o de aplicación, autorizado a tal fin, en el caso de certificados de aplicación.

Dicho solicitante debe presentar la documentación prevista en los apartados 3.2.2.- Autenticación de la identidad de Personas Jurídicas o Entidades Públicas y 3.2.3.-Autenticación de la identidad de Personas Humanas de la Política Única de Certificación.

En el caso de solicitudes de certificados de aplicación, el carácter de suscriptor debe ser probado por el representante legal o apoderado o, el responsable de la aplicación autorizado a tal fin.

Al ingresar en el sitio web del certificador, el solicitante debe seleccionar el enlace a la aplicación de solicitud de emisión de certificados para completar los datos solicitados. En ningún caso las claves criptográficas serán generadas ni almacenadas por la AC ONTI. En el caso que se utilicen dispositivos criptográficos, estos deberán ser homologados FIPS 140-2 Nivel 2.

Los suscriptores, incluyendo las AR y los proveedores de otros servicios de firma digital generan sus claves mediante el algoritmo RSA con un tamaño de clave 2048 bits.

El Certificador comprueba que el solicitante es el titular del par de claves mediante la verificación de la solicitud del certificado digital en formato PKCS#10, la cual no incluye la clave privada. Las claves siempre son generadas por el solicitante. En ningún caso el certificador licenciado ni sus autoridades de registro podrán tomar conocimiento o acceder bajo ninguna circunstancia a las claves privadas de los solicitantes o titulares de los certificados, conforme el artículo 21, inciso b) de la Ley N° 25.506.

Los procedimientos utilizados para el procesamiento de las solicitudes de certificados se encuentran descriptos en el apartado 4.2. del Manual de Procedimientos asociado a la Política Única de Certificación.

Cumplido el procesamiento de la solicitud, y en caso de corresponder, el proceso de emisión del certificado se encuentra descripto en el apartado 4.3 del Manual de Procedimientos asociado a la Política Única de Certificación.
El par de claves del suscriptor de un certificado digital debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y absoluto control. El suscriptor es considerado titular del par de claves; como tal, está obligado a generarlas en un sistema confiable y a no revelar su clave privada a terceros bajo ninguna circunstancia.

3. OBLIGACIONES

a) De los Suscriptores de Certificados.

Los suscriptores de los certificados digitales asumen las siguientes obligaciones:
a) Mantener el control exclusivo de los datos de creación de su firma digital, no compartirlos, e impedir su divulgación;
b) Utilizar un dispositivo de creación de firma digital que cumpla con las características definidas en la Política Única de Certificación;
c) Solicitar la revocación de su certificado a la AC ONTI ante cualquier circunstancia que pudiere comprometer la privacidad de sus datos de creación de firma;
d) Informar sin demora a la AC ONTI el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación;
e) Solicitar la revocación de su Certificado en caso de producirse cualquier modificación de los datos contenidos en el mismo.
f) Proveer toda la información que le sea requerida a los fines de la emisión del certificado de modo completo y preciso;
g) Utilizar los certificados de acuerdo con los términos y condiciones establecidos en la Política Única de Certificación que respalde su emisión;
h) Verificar la exactitud de los datos contenidos en su certificado al momento de su entrega;

b) Del Certificador.

La AC ONTI asume las obligaciones establecidas en la Política Única de Certificación, el Manual de Procedimientos, la Política de Privacidad y la restante documentación publicada, en un todo de acuerdo con la Ley N° 25.506 y la restante normativa vigente.

4. POLÍTICA DE PRIVACIDAD

La AC ONTI cumplirá con lo establecido en su documento de Política de Privacidad, publicado en su sitio web, protegiendo así los datos, tanto de los suscriptores como los propios. Mediante el presente acuerdo, el suscriptor manifiesta conocer y aceptar los términos de dicha Política.

5. LIMITACIONES O EXIMICIÓN DE RESPONSABILIDAD.

La AC ONTI no asumirá responsabilidad alguna en aquellos supuestos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados, en los supuestos de daños y perjuicios que resultaren del uso no autorizado de un certificado digital y en los supuestos donde las inexactitudes contenidas en el certificado resultaran de la información que hubiera presentado el suscriptor.

a) Fuerza mayor

Las partes del presente acuerdo no serán consideradas como responsables o incumplidoras, por cualquier finalización, interrupción o demora en el cumplimiento de sus obligaciones, que resultara como consecuencia de un terremoto, inundación, incendio, vendaval, desastre natural, guerra, conflicto armado, acción terrorista, siempre y cuando la parte que invoca esta sección haya puesto esta circunstancia en conocimiento de la otra parte dentro de los CINCO (5) días de conocido el fenómeno, y que haya tomado oportunamente las medidas necesarias para mitigar los efectos ocasionados por el hecho de fuerza mayor alegado.

b) Casos en los cuales el certificador puede limitar o eximirse de su responsabilidad.

La AC ONTI no asume responsabilidad en los casos no establecidos expresamente en la legislación aplicable, en aquellos casos de utilización no autorizada de un certificado cuya descripción se encuentra establecida en la Política Única de Certificación y en

eventuales inexactitudes en los datos contenidos en el certificado que resulten de información facilitada por el suscriptor del certificado y que hubieran sido objeto de verificación de acuerdo con los procedimientos establecidos en la Política Única de Certificación y en el Manual de Procedimientos.

6. LEY Y JURISDICCIÓN APLICABLE Y PROCEDIMIENTO DE RESOLUCIÓN DE CONFLICTOS.

La Política Única de Certificación y su correspondiente Manual de Procedimientos se encuentran en un todo subordinados a las prescripciones de la Ley N° 25.506, su Decreto Reglamentario N° 2628/02 y modificatorios, la Resolución MM N° 399-E/2016 del entonces MINISTERIO DE MODERNIZACIÓN y demás normas complementarias dictadas por la Autoridad de Aplicación.
Cualquier controversia y/o conflicto resultante de la aplicación de la Política Única de Certificación, deberá ser resuelta en sede administrativa de acuerdo a las previsiones de la Ley Nacional de Procedimientos Administrativos N° 19.549 y su Decreto Reglamentario N° 1759/72 T.O. 2017.
Los titulares de certificados y los terceros usuarios podrán interponer ante el Ente Licenciante recurso administrativo por conflictos referidos a la prestación del servicio por parte del Certificador. Una vez agotada la vía administrativa, podrá interponerse acción judicial, siendo competente la Justicia en lo Contencioso Administrativo Federal.
El reclamo efectuado por un tercero usuario o por el titular de un certificado digital expedido por la AC ONTI, sólo será procedente previa acreditación de haberse efectuado reclamo previo ante esta última con resultado negativo. Acreditada dicha circunstancia, el Ente Licenciante procederá a recibir, evaluar y resolver las denuncias mediante la instrucción del correspondiente trámite administrativo.

7. CESIÓN DE DERECHOS

Ninguna de las obligaciones del suscriptor de un certificado digital bajo el presente acuerdo podrá ser cedida o transferida.

8. DECLARACIÓN JURADA

El suscriptor declara que la información contenida en el certificado digital es fidedigna, en los términos de los Artículos 109 y 110 del Reglamento de Procedimientos Administrativos Decreto 1759/72 T.O. 2017 aprobado por el Decreto N° 894/2017.
El suscriptor declara haber leído y aceptado en todos sus términos la Política Única de Certificación.

9. CONTACTOS

Los suscriptores de los certificados de la AC ONTI, a los efectos de toda consulta, sugerencia y tramitación, deberán dirigirse a:
AC ONTI
Correo electrónico: consultapki@modernizacion.gob.ar

10. VIGENCIA

El solicitante de un certificado digital, una vez cumplidos los requisitos definidos por el Certificador, deberá aceptar los términos y condiciones del presente Acuerdo, como prueba de conocer y aceptar sus términos y los de la Política Única de Certificación de la AC ONTI vigente.
La vigencia del presente acuerdo comenzará a partir de la emisión del certificado digital relacionado con éste y continuará vigente en la medida en que sea válido el certificado emitido para la Autoridad Certificante del suscriptor y que éste no haya violado sus disposiciones. En caso de que el suscriptor hubiese violado alguna de sus disposiciones, persistirán a su cargo las obligaciones pendientes hasta su entera satisfacción.

11. MODIFICACIÓN A ESTE ACUERDO

El Certificador se reserva el derecho exclusivo de modificar el presente acuerdo, previa revisión y aprobación de la SECRETARÍA DE MODERNIZACIÓN ADMINISTRATIVA. Cualquier cambio en sus especificaciones dará lugar a la firma de un nuevo acuerdo con cancelación del presente.