FDSL 3.0
FIRMA DIGITAL
DE SAN LUIS

TÉRMINOS Y CONDICIONES CON TERCEROS USUARIOS

VERSION 3.0 – FECHA 20/02/2019

DE LA "POLÍTICA DE CERTIFICACIÓN PARA AUTENTICACIÓN DE SERVIDORES Y SERVICIOS"

OID 2.16.32.1.3.2.1.1.5.

INFRAESTRUCTURA DE FIRMA DIGITAL DE SAN LUIS

Versiones y modificaciones de este documento

V	R	Fecha	Elaborado por	Revisado por	Descripción
1	0	15/11/2010	FDSL	Director	Resolución N° 11150008-ULP-2010
2	0	03/10/2016	FDSL	Director	Resolución N° 10-MCyT-2016
2	1	12/01/2017	FDSL	Director	Resolución N° 07-ASLCTyS-2017
3	O	20/02/2019	FDSL	Director	Resolución N° 44-ACTySSL-2019

ÍNDICE

1.- DEFINICIONES 4
1.1.- DEFINICIONES DE CONCEPTOS 4
1.2.- ACRÓNIMOS 6
2.- RECONOCIMIENTO DE INFORMACIÓN SUFICIENTE 6
3.- POLÍTICA DE CERTIFICACIÓN 7
3.1.- TIPOS DE CERTIFICADOS 7
3.2.- APLICABILIDAD 7
3.2.1.- Usos Apropiados de los Certificados 7
3.2.2.- Usos Prohibidos de los Certificados 7
3.2.3.- Limitaciones en el Uso del Certificado 7
4.- OBLIGACIONES DEL TERCERO USUARIO (“relying party”) 8
5.- REVOCACIÓN DE LOS CERTIFICADOS DE NIVEL SUPERIOR 8
6.- LIMITACIONES DE RESPONSABILIDAD 8
6.1.- FUERZA MAYOR 9
6.2.- CASOS EN LOS CUALES EL CERTIFICADOR PUEDE LIMITAR SU RESPONSABILIDAD 9
7.- LEGISLACIÓN APLICABLE Y PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS 9
7.1.- LEGISLACIÓN APLICABLE 9
7.2.- PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS 9
8.- CONTACTOS 9

TÉRMINOS Y CONDICIONES CON TERCEROS USUARIOS DE CERTIFICADOS DE CLAVE PÚBLICA DE FIRMA DIGITAL DE SAN LUIS

TODO TERCERO USUARIO DE CERTIFICADOS DIGITALES DEBERÁ LEER EL PRESENTE DOCUMENTO DENOMINADO "TÉRMINOS Y CONDICIONES PARA TERCEROS USUARIOS DE CERTIFICADOS DE CLAVE PÚBLICA DE FIRMA DIGITAL DE SAN LUIS" ANTES DE VALIDAR UN CERTIFICADO DIGITAL EMITIDO BAJO LA "POLÍTICA DE CERTIFICACIÓN PARA AUTENTICACIÓN DE SERVIDORES Y SERVICIOS", Y/O ACCEDER A UNA BASE DE DATOS DE REVOCACIONES DE CERTIFICADOS E INFORMACIÓN COMPLEMENTARIA (REPOSITORIO) DE FIRMA DIGITAL DE SAN LUIS.

Por el presente, los terceros usuarios que verificarán los certificados digitales toman conocimiento y aceptan que Firma Digital de San Luis (en adelante, FDSL) no tiene vínculo contractual alguno con ellos, sino que se limitarán a utilizar los servicios brindados por FDSL en el marco de la Política de Certificación relacionada con el presente documento y de acuerdo con la normativa vigente.

1.- DEFINICIONES

1.1.- DEFINICIONES DE CONCEPTOS

Definiciones de los conceptos relevantes utilizados en la Política de Certificación para Autenticación de Servidores y Servicios:

- Autoridad de Aplicación: AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS.
- Ente Licenciante: es el órgano administrativo encargado de otorgar las licenciantes a los Certificadores Licenciado Provinciales y de supervisar su actividad. El INSTITUTO FIRMA DIGITAL DE SAN LUIS y la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS, constituyen el Ente Licenciante del régimen provincial de firma digital en San Luis (art. 24º y 26° del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018). Cuando el INSTITUTO FIRMA DIGITAL DE SAN LUIS actúa como Certificador Licenciado Provincial, la AGENCIA DE CIENCIA, TECNOLOGÍA Y SOCIEDAD SAN LUIS cumple el rol de Ente Licenciante Provincial (art. 18º de Resolución Nº 17-ASLCTyS-2017).
- Certificador Licenciado Provincial: Es el ente público, ente privado u organismo de derecho público no estatal que emite certificados de clave pública, entendiendo por tal al que asocia una clave pública con un suscriptor, durante el período de vigencia del certificado, haciendo plena prueba dentro de la Administración del Sector Público Provincial, los Poderes del Estado Provincial y el sector privado de la veracidad de su contenido y cuenta con una licencia provincial para ello (artículo 31 del Decreto Nº 0428-MP-2008).
- Autoridad de Registro: Es la entidad en quien el Certificador Licenciado Provincial delega las funciones relativas a la verificación de la identidad y demás datos correspondientes al aspirante a suscriptor del servicio, de registro de presentaciones y trámites que le son formuladas, así como la responsabilidad de las comunicaciones con el Ente Licenciante Provincial y/o el Certificador Licenciado Provincial en el proceso técnico de registración (artículo 39 del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018). La Autoridad de Registro puede actuar en una instalación fija o en modalidad móvil, siempre que medie autorización del Certificador Licenciado para hacerlo (artículo 40 del Decreto Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018).
- Autoridad Certificadora: Es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- Suscriptor o Titular de Certificado Digital: Persona o entidad a cuyo nombre se emite un certificado y que posee una clave privada que se corresponde con la clave pública contenida en el mismo (art. 36 del Decreto Nº 0428-MP-2008).

- Tercero Usuario: Persona humana o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente. Son Terceros Usuarios de los certificados emitidos bajo la presente Política de Certificación, toda persona humana o jurídica que realiza una conexión segura a un servidor que utilice el certificado de autenticación de servidores emitido por FDSL para establecer el canal de comunicación. Las personas humanas o jurídicas que utilicen el servicio de sellado de tiempo TSA – FDSL. Las personas humanas o jurídicas que utilicen el Servicio de Consulta en Línea del Estado del Certificado OCSP – FDSL para verificar la validez de un certificado digital.
- Infraestructura de Firma Digital San Luis: Se entiende por tal al conjunto integrado por las leyes, decretos y normativa legal complementaria que regulen la firma digital en la jurisdicción de la Provincia de San Luis, las obligaciones y deberes de todas aquellas instituciones, organismos y personas que formen parte del circuito de la firma digital tales como la Autoridad de Aplicación Provincial, el Ente Licenciante Provincial, los Certificadores Licenciados Provinciales, las Autoridades de Registro, así como también, a los estándares tecnológicos, los procedimientos de seguridad, el hardware, el software, las redes, los bancos de datos y la infraestructura física de alojamiento, que permitan la utilización de la firma digital en condiciones de seguridad e integridad (artículo 10º del Decreto Nº 0428-MP-2008).
- Firma Digital: Se entiende por Firma Digital al resultado de una transformación de un documento digital empleando una criptografía asimétrica y un digesto seguro, de forma tal que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza lo siguiente: 1) si la transformación se llevó a cabo utilizando la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio; 2) si el documento digital ha sido modificado desde que se efectuó la transformación, de manera tal de garantizar con esta comprobación la integridad del documento. Todo lo cual conlleva a garantizar las características de "no repudio" y la "integridad" del documento que son requisitos de la firma digital (artículo 7º del Decreto Nº 0428-MP-2008).
- Criptografía Asimétrica: Se entiende por Criptografía Asimétrica al algoritmo que utiliza, por un lado, una clave privada que es utilizada para firmar digitalmente y por otro su correspondiente clave pública para verificar esa firma digital. Debe ser técnicamente confiable (artículo 8º del Decreto Nº 0428-MP-2008).
- Digesto Seguro: es una función matemática que transforma un documento digital en una secuencia de bits de longitud fija, llamada como tal, de forma que se obtiene la misma secuencia de bits de longitud fija cada vez que se calcula esta función respecto del mismo documento digital (artículo 9º del Decreto Nº 0428-MP-2008).
- Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13 de la Ley N° 25.506).
- Certificado Digital de Fecha y Hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.
- Lista de Certificados Revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado Provincial, la cual ha sido firmada digitalmente y publicada por el mismo. En inglés: *"Certificate Revocation List"* (CRL).
- Servicio OCSP (PROTOCOLO de Estado de Certificado en Línea): Servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el certificado de servicio OCSP del Certificador Licenciado Provincial que brinda el servicio. En inglés: *"Online Certificate Status Protocol"* (OCSP)
- Manual de Procedimientos: Conjunto de prácticas utilizadas por el Certificador Licenciado Provincial en la emisión y administración de los certificados. En inglés: *"Certification Practice Statement"* (CPS).

- Plan de Cese de Actividades: Conjunto de actividades a desarrollar por el Certificador Licenciado Provincial en caso de finalizar la prestación de sus servicios.
- Plan de Continuidad de las Operaciones: Conjunto de procedimientos a seguir por el Certificador Licenciado Provincial ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones. También denominado Plan de Contingencia.
- Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección de los recursos del Certificador Licenciado Provincial.
- Política de Privacidad: Conjunto de declaraciones que el Certificador Licenciado Provincial se compromete a cumplir de manera de resguardar los datos de los solicitantes y suscriptores de certificados digitales por él emitidos.

1.2.- ACRÓNIMOS

AC	- Autoridad Certificante
ACR-SL	- Autoridad Certificante Raíz San Luis
AR	- Autoridad de Registro
ARD	- Autoridad de Registro Delegada
ACTySSL	- Agencia de Ciencia, Tecnología y Sociedad San Luis
CIPE	- Cédula de Identidad Provincial Electrónica
CLP	- Certificador Licenciado Provincial
CP	- Política de Certificación
CRL	- Lista de Certificados Revocados
CUIL	- Clave Única de Identificación Laboral
CUIT	- Clave Única de Identificación Tributaria
FD	- Firma Digital
FDSL	- Instituto Firma Digita de San Luis
FIPS	- Norma Federal de Procesamiento de la Información
MCyT	- Ministerio de Ciencia y Tecnología de San Luis
MPC	- Manual de Procedimientos de Certificación
OCSP	- Protocolo de estado de certificado en línea -Online Certificate Status Protocol
OID	- Identificador de Objeto (“Object Identifier”).
PKI	- Infraestructura de Clave Pública
RFC	- Request for Comments.

2.- RECONOCIMIENTO DE INFORMACIÓN SUFICIENTE

El tercero usuario cuenta con información suficiente disponible en el repositorio público que se encuentra en el sitio http://www.firmadigital.sanluis.gov.ar, que contiene el conjunto de documentos normativos que permiten la operatoria de la infraestructura mencionada, en particular la “Política de Certificación para Autenticación de Servidores y Servicios” y está disponible veinticuatro (24) horas los siete (7) días de la semana.
Para la verificación de la vigencia del certificado digital se podrá consultar dicho sitio de internet y utilizar los medios disponibles tales como la consulta en línea del estado de los certificados (OCSP) o la CRL.
Se considera que el Tercero Usuario que intenta validar un Certificado Digital emitido por FDSL, conoce el contenido del total de dicha documentación y reglamentaciones.
En tal sentido, el Tercero Usuario es el único responsable de la decisión de confiar o no en la información del certificado.

3.- POLÍTICA DE CERTIFICACIÓN

Estos Términos y Condiciones con Terceros Usuarios complementan lo dispuesto en la Política de Certificación para Autenticación de Servidores y Servicios.

3.1.- TIPOS DE CERTIFICADOS

En el marco de la Política de Certificación asociada a estos Términos y Condiciones sólo se emitirán certificados para autenticación de servidores, certificados para brindar el servicio de sellado de tiempo y certificados para autenticar la respuesta de la consulta del estado de los certificados que se realiza en línea con el protocolo OCSP.

3.2.- APLICABILIDAD

Los certificados emitidos en el marco de la Política de Certificación para Autenticación de Servidores y Servicios, podrán ser utilizados para: autenticar la identidad de un servidor y establecer luego un canal de transmisión seguro entre el servidor y el usuario del servicio, garantizar la fecha y hora de las transacciones y el no repudio en procesos en los cuales intervenga cualquier organismo o entidad con los que FDSL haya formalizado un Convenio de Servicio de Sellado de Tiempo, autenticar la respuesta de la consulta del estado de los certificados que se realiza en línea con el protocolo OCSP.

3.2.1.- Usos Apropiados de los Certificados

En tal sentido, de manera enunciativa dichos certificados podrán ser utilizados a fin de:

- **CLASE I: Autenticación de Servidores**

Los certificados CLASE I emitidos en el marco de la presente Política de Certificación podrán ser utilizados exclusivamente a los fines de autenticar la identidad de un servidor y establecer luego un canal de transmisión seguro entre el servidor y el usuario del servicio.

- **CLASE II: Servicio de Sellado de Tiempo**

Los sellos de tiempo emitidos por la Autoridad de Sellado de Tiempo de FDSL, TSA - FDSL, pueden emplearse para garantizar la fecha y hora de las transacciones y el no repudio en procesos en los cuales intervenga cualquier organismo o entidad con los que FDSL haya formalizado un Convenio de Servicio de Sellado de Tiempo.

- **CLASE III: Servicio de Consulta en Línea del Estado del Certificado**

Los certificados para el Servicio de Consulta en Línea del Estado del Certificado de FDSL, OCSP – FDSL podrán ser usados exclusivamente a los fines de autenticar la respuesta de la consulta del estado de los certificados que se realiza en línea con el protocolo OCSP.

3.2.2.- Usos Prohibidos de los Certificados

Todo uso que exceda el alcance señalado en el Punto 3.2 de estos Términos y Condiciones se encuentran prohibidos.

3.2.3.- Limitaciones en el Uso del Certificado

El uso de los certificados digitales emitidos deberá hacerse conforme a la Política de Certificación para Autenticación de Servidores y Servicios - bajo la cual fue emitido -, fuera de estos casos, no

existen restricciones en el uso del certificado, excepto aquellas indicadas en la legislación vigente en materia de firma digital de la Provincia.

4.- OBLIGACIONES DEL TERCERO USUARIO ("relying party")

Los Terceros Usuarios tienen las siguientes obligaciones:
a) Conocer los alcances de la Política de Certificación aplicable;
b) Rechazar la utilización del certificado para fines distintos a los previstos en la Política de Certificación que lo respalda y de usarlo conforme a los Términos y Condiciones con Terceros Usuarios;
c) Verificar la validez del certificado digital. Para ello, los Terceros podrán realizar cualquiera de las siguientes acciones:
• Utilizando la Lista de Certificados Revocados

- Verificar que el certificado digital correspondiente al documento firmado, no se encuentre incluido en la Lista de Certificados Revocados publicada en el siguiente sitio http://fd01.firmadigital.sanluis.gov.ar/fdsl/servidores.crl
  y alternativamente, en:
  http://fd02.firmadigital.sanluis.gov.ar/fdsl/servidores.crl
- Verificar la autenticidad de la Lista de Certificados Digitales, mediante la verificación de la firma digital de la AC-FDSL que la emite y de su período de validez.

Si no se pudiera obtener una CRL actualizada, se deberá optar entre rechazar el documento firmado digitalmente o aceptarlo, bajo exclusiva responsabilidad de quien consulta.

• Utilizando el servicio de consulta basado en el protocolo de comunicación OCSP.

5.- REVOCACIÓN DE LOS CERTIFICADOS DE NIVEL SUPERIOR

Para no verse expuesto a los riesgos que implica el compromiso de las claves privadas del nivel superior, el tercero usuario debe verificar el estado de validez del certificado de la Autoridad Certificante del Certificador Licenciante Provincial y de la Autoridad Certificante Raíz de la Infraestructura de Firma Digital de la Provincia de San Luis. En caso de producirse la revocación de los certificados de nivel superior, este estado se hará evidente para el Tercero Usuario en el momento en que se genere una consulta para verificar la validez del certificado de un suscriptor. La verificación de la validez del certificado de un suscriptor, se realiza a través del siguiente procedimiento:
a) Verificando la cadena de confianza del certificado del suscriptor, la cual se realiza en el siguiente orden:
• Contra el certificado con que se emitió el certificado del suscriptor: Certificado de la Autoridad Certificante de FDSL para la Política de Certificación para Autenticación de Servidores y Servicios.
• Contra el certificado con que se emitió el certificado de la Autoridad Certificante FDSL: Certificado de la Autoridad Certificante Raíz ACRaíz02 y Certificado de la Autoridad Certificante Raíz ACRaíz01.
b) Verificando la vigencia y el estado del certificado, a través de la consulta a la última CRL emitida por la Autoridad Certificante FDSL para la Política para Autenticación de Servidores y Servicios.

6.- LIMITACIONES DE RESPONSABILIDAD

FDSL será responsable, en caso de corresponder, ante terceros por el incumplimiento de las previsiones de la Ley Provincial Nº V-0591-2007, Decreto Reglamentario Nº 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018, y toda otra normativa aplicable, respecto a los procedimientos que respaldan la emisión de certificados, por los errores u omisiones en los certificados por él emitidos y por su falta de revocación en la forma y plazos previstos.

6.1.- FUERZA MAYOR

No cabe responsabilidad alguna para FDSL por hechos fortuitos o de fuerza mayor, que éste no pudiera prever, o habiendo sido previsto no pudo evitarlo, conforme el Art 1730 del Código Civil y Comercial de la Nación.

6.2.- CASOS EN LOS CUALES EL CERTIFICADOR PUEDE LIMITAR SU RESPONSABILIDAD

No cabe responsabilidad alguna para Firma Digital de San Luis, en caso de utilización no autorizada de un certificado digital, cuya descripción se encuentra establecida en su Política de Certificación, como tampoco responde por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y procedimientos establecidos, deba ser objeto de verificación; ni frente a la omisión de los responsables de revocar un certificado digital cuando éstos no lo hicieran.
En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un Certificador Licenciado Provincial, público o privado, comprometerá la responsabilidad pecuniaria del Estado de San Luis en su calidad de Ente Administrador de la Infraestructura de Firma Digital Provincial.

7.- LEGISLACIÓN APLICABLE Y PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS

7.1.- LEGISLACIÓN APLICABLE

La interpretación, obligatoriedad, diseño y validez de este Acuerdo y sus documentos asociados se encuentran sometidos a lo establecido por la Ley Provincial Nº V-0591-2007, el Decreto Reglamentario Nº 0428-MP-2008 modificada por Decreto N° 6011-MCyT-2018, la Resolución N° 341-ACTySSL-2018, Ley Nacional Nº 25.506, el Decreto Nº 2628/2002 y demás normas complementarias aplicables dictadas por autoridad competente.

7.2.- PROCEDIMIENTOS DE RESOLUCIÓN DE CONFLICTOS

La resolución de cualquier controversia y/o conflicto resultante de la aplicación de lo dispuesto en este Acuerdo y/o en cualquiera de sus documentos asociados, será resuelta en sede administrativa ante FDSL.
Agotada la vía administrativa ante FDSL, la controversia o conflicto será resuelto por la Autoridad de Aplicación conforme a su régimen recursivo.
Pueden recurrir a este procedimiento tanto los Suscriptores como los Terceros Usuarios de certificados de clave pública.

8.- CONTACTOS

Firma Digital de San Luis funciona en el ámbito de la Agencia de Ciencia, Tecnología y Sociedad San Luis.
Para consultas y sugerencias acerca de este documento se puede obtener información personalmente o por correo en:

Instituto Firma Digital de San Luis
Dirección: Edificio de Descentralización Administrativa "Terrazas del Portezuelo" - Torre III, 3º Piso - Autopista de las Serranías Puntanas Km. 783, Provincia de San Luis, República Argentina. Código Postal 5700.
Teléfono: (0266) 4452000, Internos: 6095 y 3574.
Correo Electrónico: firmadigital@sanluis.gov.ar
Sitio Web: http://www.firmadigital.sanluis.gov.ar