Ministerio de Ciencia, Tecnología e Innovación Productiva
Consejo Nacional de Investigaciones Científicas y Técnicas

Política de Firma Digital de CONICET

Versión 1.0

1. Introducción

1.1. Alcance

Este documento establece las normas utilizadas para determinar bajo qué condiciones los métodos de creación y verificación de una firma digital son válidos cuando son usados dentro del contexto de los Servicios de Firma Digital de CONICET con equivalencia de firma hológrafa.

Además, el presente documento establece los roles, los derechos y las obligaciones de todos los actores involucrados en transacciones con los Servicios de Firma Digital de CONICET.

Finalmente, el presente documento establece los estándares técnicos y las operaciones utilizadas para crear las firmas digitales a través de los Servicios de Firma Digital de CONICET.

1.2. Organización del documento

La organización de este documento esta basada en el encuadre de Política de Firma definido por el Instituto Europeo de Normalización de las Telecomunicaciones (ETSI) en la norma ETSI TR 102 041 V1.1.1.

1.3. Publicación

Este documento puede obtenerse libremente en la Sede Central de CONICET o por Internet en https://si.conicet.gov.ar/firmadigital/pfd-v1.0.pdf. La administración de esta Política de Firma recae sobre la Gerencia de Organización y Sistemas de CONICET.

2. Servicios de Firma Digital de CONICET

2.1. Actores

Signatario: Es la persona que crea una firma digital; es decir los agentes del organismo que hayan obtenido su dispositivo seguro de creación de firma (token criptográfico), hayan gestionado su certificado digital y mediante los Servicios de Firma Digital de CONICET firmen digitalmente.

Verificador: Es la persona que verifica una firma digital. La verificación se realiza mediante los Servicios de Firma Digital de CONICET o caso contrario respetando el proceso de verificación descrito en la presente Política de Firma. El verificador puede ser una de las partes involucradas como así también un tercero interesado en la validez de la firma digital de un documento.

Servicios de Firma Digital de CONICET: Los Servicios de Firma Digital de CONICET asisten al signatario para crear una firma digital de acuerdo con la presente Política de Firma, a fin de asegurar que la firma generada tenga un valor legal equivalente a la firma hológrafa como lo establece la ley N° 25.506, su Decreto Reglamentario N° 2628/02 y los Decretos N° 1028/03, 409/05, 724/06, la Decisión Administrativa N° 06/2007 y sus normas complementarias (en adelante marco normativo de firma digital). Los Servicios de Firma Digital de CONICET asisten al verificador para evaluar si una firma digital fue realizada conforme con la presente Política de Firma.

2.2. Descripción de los Servicios de Firma Digital de CONICET

Los Servicios de Firma Digital de CONICET son servicios que asisten a los usuarios para crear y verificar firmas digitales. Dichas firmas cumplen con los requerimientos establecidos en el marco normativo vigente de modo tal que desde el punto de vista legal posean la misma validez y eficacia jurídica que la firma hológrafa.

Dado que los requerimientos del mencionado marco normativo son complejos para el público general, CONICET ha creado estos servicios quitando la mencionada complejidad al signatario y al verificador. De esta manera ambos pueden estar seguros de cumplir con el formato de la firma y el método de verificación para la ley.

Adicionalmente estos servicios ofrecen una serie de medidas complementarias para asegurar el no repudio de las firmas digitales a largo plazo. Sin perjuicio de lo dicho, la validez de la firma digital está condicionada a lo establecido en la Política de Certificación asociada al certificado digital utilizado y a la totalidad de las disposiciones del marco normativo de firma digital.

2.3. Estándares utilizados

Los Servicios de Firma Digital de CONICET utilizan el formato estándar de Firma Digital Avanzada en XML (XAdES), posibilitando que se pongan en práctica todas las medidas para garantizar el no repudio a largo plazo. Para más información consultar el estándar ETSI[8].

La firma digital aplicada de acuerdo con la presente Política de Firma debe estar al menos en el formato definido por el perfil XAdES-T. Este perfil contiene un sello digital de tiempo que puede probar en qué momento fue realizada la firma. Otros perfiles XAdES superiores que encapsulen XAdES-T, tales como XAdES-X-L y XAdES-A también son aceptados.

En virtud de garantizar la validez a largo plazo de los documentos firmados digitalmente y en función de las recomendaciones internacionales en cuanto a seguridad de la información el organismo seleccionará convenientemente el perfil a aplicar en el formato XAdES de la firma digital.

Por otra parte, todas las firmas creadas bajo esta Política de Firma deben incluir dentro del formato XAdES referencias a la presente Política de Firma en forma de OID, hash y URL.

2.4. Creación de la firma digital

El signatario puede crear una firma de acuerdo con la presente Política de Firma utilizando los Servicios de Firma Digital. Es posible que en algún momento los Servicios de Firma Digital implementen Políticas de Firma distintas a la presente, no obstante lo cual las firmas realizadas con políticas anteriores mantendrán su validez. Las implementaciones basadas en los Servicios de Firma Digital tendrán en común lo siguiente:

- El usuario puede seleccionar un documento para ser firmado.
- Los Servicios de Firma Digital verificarán, no necesariamente en este orden:
    - Si la firma es válida para el documento firmado especificado.
    - Si el certificado fue emitido por una Autoridad Certificante reconocida por esta Política de Firma y se encuentra bajo una Política de Certificados aceptada. (Ver la sección 3.3.3.1.1.)
    - La validez del certificado: el certificado no se encuentra revocado o suspendido, el certificado esta dentro del período de vigencia (fechas desde y hasta válidas), validación de la cadena de certificados completa (incluyendo la validación de todos los certificados de la cadena).

  Cuando una de estas verificaciones falle, el proceso de firma será abortado.
- Los Servicios de Firma Digital crearán un formato de firma XAdES con perfil XAdES-T o superior.

2.5. Verificación de la firma

El verificador puede utilizar cualquier método para verificar la firma creada de acuerdo a esta política. Sin embargo, se deben cumplir las siguientes condiciones. El servicio de verificación de firma digital implementado cumple todos estos criterios, y esta abierto para el uso de cualquier verificador.

- Asegurar que la firma digital es válida para el documento firmado especificado.
- Validez del certificado al momento de la firma: certificado no revocado o suspendido, certificado no expirado y vigente, validación de la cadena de certificados completa (incluyendo la validación de todos los certificados de la cadena). Esto puede comprender la construcción de un perfil XAdES-X-L desde un perfil XAdES-T o la construcción de un perfil XAdES-A desde un perfil XAdES-X-L.
- Certificado emitido bajo una Política de Certificados aceptada (ver requisitos del certificado en la sección 3.3.3.1.1.)
- La verificación de todos los sellos digitales de tiempo para los perfiles XAdES-T, XAdES-X-L o XAdES-A (en caso que se hayan agregado sellos digitales de tiempo adicionales para garantizar el no repudio a largo plazo), incluyendo la verificación que los periodos de validez de los sellos digitales de tiempo se superponen (en cualquier punto del tiempo al menos uno de los sellos digitales de tiempo debería ser válido para asegurar, en caso de compromiso de los algoritmos, que nunca el valor del no repudio pudo haber sido comprometido).

3. Información de la Política de Firma

3.1. Información general de la Política de Firma

Cumpliendo con los requerimientos del ETSI, la presente Política de Firma incluye los siguientes datos:

3.1.1. Identificador de Política de Firma:

- Nombre de la Política de Firma: Política de Firma Digital de CONICET
- Versión de la Política de Firma: 1.0
- OID de la Política de Firma: 2.16.32.1.2.1.1.1.1.1.0 (los dos últimos dígitos definen la versión principal y secundaria respectivamente de la Política de Firma)
- URL de la Política de Firma: https://si.conicet.gov.ar/firmadigital/pfd-v1.0.pdf.

Cualquier modificación realizada sobre este documento conllevará un cambio de versión y del identificador de objeto (OID).

3.1.2. Fecha de emisión

1 de septiembre de 2008.

3.1.3. Nombre del emisor de la Política de Firma:

Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET).

- Detalles de contacto: Av. Rivadavia 1917
  CP C1033AAJ
  Ciudad Autónoma de Buenos Aires
  República Argentina
  +54 11 5983 1420
  http://www.conicet.gov.ar
- OID del emisor de la Política de Firma: 2.16.32.1.2.1.1

3.2. Período de validez de la Política de Firma

La presente Política de Firma es válida desde la fecha de emisión hasta que sea reemplazada por una próxima versión.

3.3. Reglas generales

3.3.1. Reglas para el signatario

3.3.1.1. Ausencia de contenido dinámico basado en el tiempo

Los documentos generados por los sistemas de CONICET son carentes de cualquier tipo de contenido dinámico que pueda modificar el resultado visualizado del documento a través del tiempo. El signatario es responsable de no incluir en los documentos sujetos al uso del Servicio de Firma Digital ningún contenido dinámico.

3.3.1.2. Atributos firmados

El signatario debe proveer mediante los Servicios de Firma Digital de CONICET el siguiente conjunto de atributos firmados:

- Momento de la firma
- Certificado del signatario (incluyendo la cadena de certificados completa)
- Política de Firma (Política de Firma vigente en forma de OID, hash y URL)

3.3.1.3. Atributos no firmados

El signatario debería proveer mediante los Servicios de Firma Digital de CONICET el siguiente conjunto de atributos no firmados. Si no fueron agregados por el signatario, pueden ser agregados por el verificador.

- Sellos digitales de tiempo: Debe incluirse el atributo SignatureTimeStamps (sello digital de tiempo sobre la firma misma), debería incluirse el atributo SigAndRef TimeStamps (sello digital de tiempo sobre la combinación de la firma y las referencias a la información de validación), y puede incluirse el atributo ArchiveTimeStamps (sellos digitales de tiempo agregados a través del tiempo para mantener el valor del no repudio a largo plazo).
- Firma jerárquica: Es posible pero no obligatoria.
- Valores de los certificados: Debe incluirse el atributo CompleteCertificate Refs y debería incluirse el atributo CertificateValues.
- Referencias al estado de los certificados: debe incluirse el atributo CompleteRevocationData Refs y debería incluirse el atributo RevocationValues.

3.3.2. Reglas para el verificador

3.3.2.1. Atributos firmados

- Momento de firma: Solamente será utilizado como un indicador; solo un sello digital de tiempo puede dar información concluyente sobre una referencia temporal. El sello digital de tiempo más viejo dentro del formato XAdES será utilizado para determinar el momento de la firma.
- Certificado del signatario: Verificación completa del certificado del signatario al momento de la firma (momento de la firma durante el ciclo de vida del certificado, certificado no revocado o suspendido, verificación completa de la cadena de certificados).

  Nota: Si bien el perfil XAdES-X-L contiene datos de verificación del certificado, estos datos de verificación del certificado pueden haber sido reunidos sin tener en cuenta el período de resguardo (ver período de resguardo en la sección 3.3.3.2. de sellados digitales de tiempo). Realizar una nueva verificación del estado del certificado solo puede brindar el estado correcto concluyentemente si esta nueva verificación es realizada después del período de resguardo pero antes de la expiración del certificado. Frecuentemente los servicios de información sobre el estado de los certificados no conservan referencia sobre la revocación o suspensión de certificados expirados. Consecuentemente la manera en que se realiza la verificación depende del estado del certificado al momento de la verificación.
  - Cuando se realiza una verificación antes de la expiración del certificado de la firma: El verificador debería realizar una nueva verificación del estado del certificado. En caso que esta nueva verificación indique que el certificado ha sido revocado o suspendido, el verificador no debería confiar en la firma en caso que la fecha y hora de revocación o suspensión sea anterior o igual a la fecha y hora de firma, aún si los datos de estado del certificado incluidos en el perfil XAdES-X-L afirman que el certificado había sido válido en ese momento. Solo cuando el verificador no pueda obtener una nueva información de estado, la información de estado del certificado contenida en el perfil XAdES-X-L puede ser utilizada como única información sobre el estado del certificado, suponiendo una aceptación del riesgo resultante.
  - Cuando se realiza una verificación después de la expiración del certificado de la firma: La información sobre el estado del certificado contenida en el perfil XAdES-X-L debe ser utilizada como la única información sobre el estado del certificado, suponiendo una aceptación del riesgo resultante.
- Política de Firma: El verificador debería validar que la presente sea efectivamente la Política de Firma que se identifico en el perfil XAdES (por comparación de hash).

3.3.2.2. Atributos no firmados

El signatario debería proveer mediante los Servicios de Firma Digital de CONICET el siguiente conjunto de atributos no firmados. Si no fueron agregados por el signatario, pueden ser agregados por el verificador.

- Sellos digitales de tiempo: Pueden haber sido aplicados varios sellos digitales de tiempo. Sumado a la verificación de la validez de los sellos digitales de tiempo en si mismos y la validez de los certificados de sellado digital de tiempo, el verificador debería asegurarse que los sellos digitales de tiempo hayan sido agregados de forma tal que los periodos de validez del sello digital de tiempo se superpongan (en cualquier punto del tiempo al menos uno de los sellos digitales de tiempo debería ser válido para asegurar, en caso de compromiso de los algoritmos, que nunca el valor del no repudio pudo haber sido comprometido), todo esto entre el periodo comprendido desde el momento de la firma y el momento de la verificación.
- Contrafirma (posible pero no obligatoria): Las mismas validaciones que a la primera firma.
- Valores de los certificados: Los utilizados en las verificaciones precedentes.
- Referencias al estado de los certificados: Las utilizadas en las verificaciones precedentes.

3.3.3. Condiciones de confianza

3.3.3.1. Certificado del signatario

3.3.3.1.1. Requerimientos del certificado

Los puntos de confianza que deben usarse para iniciar el procesamiento de la cadena de certificados de firma (los certificados autofirmados para las CAs) están limitados a:

- Certificados de la Autoridad Certificante Raíz de la República Argentina.
- Certificados de la Autoridad Certificante de la Oficina Nacional de Tecnologías de la Información.

Longitud de la cadena de certificados

No se imponen limitaciones sobre la longitud de la cadena de certificados.

Políticas de certificación aceptadas

Solo se aceptaran las Políticas de Certificación que apliquen a los certificados almacenados en el dispositivo seguro de creación de firma.

Restricciones de nombres

No existe ninguna restricción sobre los nombres.

Indicación explícita de las Políticas de Certificación

- AC Raíz de la República Argentina
  - http://acraiz.gov.ar/cps.pdf (2.16.32.1.1.0)
- AC ONTI
  - http://ca.pki.gov.ar/policy.html
- AC AFIP
  - http://acn.afip.gov.ar/cps/

3.3.3.1.2. Requerimientos de revocación

La información sobre el estado de revocación del certificado del signatario debería ser validada de la siguiente manera:

- Certificados de la AC Raíz: Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.
- Certificados de la AC ONTI: Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.
- Certificados de la AC AFIP: Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.

La información sobre el estado de revocación de los certificados de las AC, correspondientes a la cadena de certificados del signatario, debería ser validada de la siguiente manera:

- Certificados de la AC Raíz: Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.
- Certificados de la AC ONTI: Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.
- Certificados de la AC AFIP: Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.

3.3.3.2. Sellado digital de tiempo

Reglas sobre la clave pública de las autoridades de sellado digital de tiempo

El certificado de la clave pública de las autoridades de sellado digital de tiempo debería incluir el valor sellado digital de tiempo en el atributo ExtendedKeyUsage (OID: 1.3.6.1.5.5.7.3.8).

Restricciones de nombres

No existe ninguna restricción sobre los nombres.

Período de resguardo

Al momento de la creación de la firma con perfil XAdES-X-L por los Servicios de Firma Digital de CONICET, se realizará una verificación sobre la validez del certificado utilizado para la firma. Esto incluye la verificación que el certificado no haya estado revocado o suspendido durante el momento que fue utilizado para firmar. Tal verificación se realiza obteniendo la información de revocación del emisor del certificado (CRL ó OCSP). Algún tiempo pasa entre el momento en que se solicita la revocación de un certificado y el momento en que los servicios de revocación (CRL ó OCSP) publican este cambio de estado. Esto significa que existe un pequeño riesgo que el estado de revocación recabado durante la creación del perfil XAdES-X-L no sea correcto (un certificado es considerado válido, mientras que no lo es). Consecuentemente existe un riesgo que el perfil XAdES-X-L asevere que la firma es válida, mientras que en realidad la firma no es válida.

Una manera de eliminar este riesgo consiste en esperar determinado tiempo (período de resguardo o período de gracia) después de la firma antes de la creación del perfil XAdES-X-L. Si este período de gracia es mayor al tiempo que le toma al servicio de estado del certificado publicar la información de revocación, el riesgo es mitigado completamente. Sin embargo, en esta Política de Firma se elige no imponer tal período de gracia por las siguientes razones:

- Los certificados permitidos por esta Política de Firma están almacenados en un dispositivo seguro de creación de firma, lo cual limita considerablemente el riesgo de abuso sobre un certificado robado o extraviado.
- Las AC utilizadas actualizan la información de revocación diariamente.
- Incluir un período de gracia podría en la mayoría de los casos desorganizar el flujo normal de los eventos en los cuales la firma es parte, de forma tal que compensaría el efecto positivo de aplicar el período de gracia.
- Si el perfil XAdES-X-L no contiene información de verificación de un plazo superior al período de gracia, la Política de Firma actual requiere que el verificador verifique los datos de revocación en línea para evaluar si el certificado signatario no estaba revocado o suspendido al momento de la firma.

Tiempo máximo de aceptación

No aplica.

3.3.3.2.1. Requerimientos del certificado

El sellado digital de tiempo se limita a certificados emitidos por:

- TS CONICET
- TS AFIP

Longitud de la cadena de certificados

No se imponen limitaciones sobre la longitud de la cadena de certificados.

Restricciones de nombres

No existe ninguna restricción sobre los nombres.

Políticas de Certificación aceptadas

No hay ninguna indicación específica sobre las Políticas de Certificación aceptadas.

3.3.3.2.2. Requerimientos de revocación

La información sobre el estado de revocación del certificado de sellado digital de tiempo debería ser validada de la siguiente manera:

- Certificados de la TS AFIP: Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.
- Certificados de la TS CONICET: Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.

La información sobre el estado de revocación de los certificados de las AC involucradas en la cadena de certificados del certificado de sellado digital de tiempo, de existir alguna, deberían ser validadas de la siguiente manera:

- Debería utilizarse el servicio de OCSP. Cuando por cualquier razón no pueda utilizarse el servicio de OCSP, deberían utilizarse los CRL completos.

3.3.3.3. Atributos

Ninguna firma de atributos es parte de esta Política de Firma.

3.3.3.4. Restricciones sobre algoritmos

Se aplican a las firmas creadas bajo esta Política de Firma las siguientes restricciones sobre los posibles algoritmos para el signatario:

- Los algoritmos del signatario: Alguno de los siguientes algoritmos debería ser utilizado RSA/SHA1, RSA/SHA256 o RSA/SHA512.
- Longitud mínima de la clave: Las Políticas de Certificación aceptadas definen la longitud mínima de la clave.

Esta Política de Firma no define restricciones sobre los posibles algoritmos en autoridades de sellado digital de tiempo.

3.3.3.5. Extensiones comunes

No han sido definidas extensiones comunes en esta Política de Firma.

3.4. Reglas según compromiso

No se aplican reglas según el tipo de compromiso.

3.5. Extensiones de la Política de Firma

No son pertinentes extensiones de la presente Política de Firma.

3.6. Área de aplicación

Esta Política de Firma se aplica en el contexto de las transacciones con los Servicios de Firma Digital de CONICET.

3.6.1. Usos permitidos

Las firmas digitales generadas en el ámbito de esta Política de Firma pueden utilizarse con cualquier tipo de documentos digitales del Consejo Nacional de Investigaciones Científicas y Técnicas, de acuerdo con las limitaciones de uso y restricciones derivadas de la Política de Certificación a la que está sometido el certificado digital utilizado en su creación, la presente Política de Firma y lo dispuesto por el ordenamiento jurídico vigente.

3.6.2. Usos prohibidos

Todos aquellos no contemplados en el apartado “Usos permitidos”.

3.7. Ciclo de vida

El ciclo de vida de una firma emitida por los Servicios de Firma Digital de CONCIET es a largo plazo. Se establece un período de validez mínimo de veinte años, siempre y cuando:

- Los algoritmos criptográficos utilizados en la emisión de los certificados y en la generación de la firma digital sigan siendo considerados internacionalmente como seguros.
- La longitud de la clave empleada en la emisión de los certificados y en la generación de la firma digital siga siendo considerada internacionalmente como segura.
- La firma digital incorpore un sello de tiempo emitido por una AC reconocida en la presente Política de Firma.

En caso de producirse un cambio de algoritmo o ampliación de la longitud de la clave, los Servicios de Firma Digital de CONICET cuentan con mecanismos de re-timbrado que permiten mantener la vigencia de las firmas hasta ese momento producidas.

3.8. Política de Firma explícita

La referencia a una Política de Firma dentro de un documento firmado es explícita, es decir esta incluida dentro de los atributos firmados por el signatario. El beneficio es permitir el procesamiento de firmas digitales aún mucho tiempo después que hayan sido creadas y fuera de su contexto original de uso (Ej.: delante de un juez).

La Política de Firma es identificable unívocamente por un identificador de objeto (OID) y verificable utilizando un hash de la Política de Firma. Por lo tanto cada vez que se genera una firma digital, incluye dentro del documento firmado el identificador de objeto de la Política de Firma, el valor de hash de la Política de Firma y una ubicación (URL) donde puede obtenerse una copia de la Política de Firma.

3.9. Publicación de la Política de Firma del Servicio de Firma Digital de CONICET

Antes de firmar, un signatario debe estar seguro sobre la Política de Firma que será aplicada. De la misma manera, cuando se verifica una firma digital, un verificador necesita conocer que Política de Firma se aplica.

CONICET emite sus propias Políticas de Firma y las pone a disponibilidad de los interesados colocándolas en un sitio web seguro, el cual puede ser accedido vía SSL. De esta manera un signatario o un verificador tienen la garantía que poseen la Política de Firma genuina.

3.10. Archivo de la Política de Firma del Servicio de Firma Digital de CONICET

En el caso que la versión actual de esta Política de Firma sea reemplazada, la versión siguiente de la Política de Firma identificará el repositorio donde la versión de la Política de Firma presente será archivada, y la manera en que el verificador puede accederla. Esto podría ser requerido para la verificación de una firma digital creada bajo la versión de la Política de Firma actual.

3.11. Conformidad con los estándares de la Política de Firma del Servicio de Firma Digital de CONICET

La presente Política de Firma mantiene conformidad con la ley N° 25.506, su Decreto Reglamentario N° 2628/02 y los Decretos N° 1028/03, 409/05, 724/06, la Decisión Administrativa N° 06/2007 y sus normas complementarias. Además cumple con lo establecido por los documentos ETSI TS 101 903 y ETSI TR 102 041.

4. Glosario

Atributos de la Firma: información adicional que se firma conjuntamente con el documento digital.

Autoridad Certificante (CA): una autoridad confiable para crear y asignar certificados.

Autoridad de Sellado Digital de Tiempo (TSA): una autoridad confiable que provea servicios de sellado digital de tiempo.

Certificado Reconocido: un certificado que cumple con lo indicado en el apartado 3.3.3.1.1.

Clave Privada: aquella clave perteneciente al par de claves asimétricas que permanece en secreto y sólo debe ser utilizada por el propietario.

Clave Pública: aquella clave perteneciente al par de claves asimétricas que puede ser publicada.

Datos a Firmar (DTBS): los datos digitales completos a ser firmados, incluyendo tanto el documento digital como los atributos de la firma.

Datos de Creación de la Firma: datos únicos, como códigos o claves privadas, que son utilizadas por el signatario para crear la firma digital.

Datos de Validación de la Firma: datos adicionales, recolectados por el signatario y/o por un verificador, necesarios para verificar la firma digital cumpliendo los requerimientos de la Política de Firma.

Datos de Verificación de la Firma: los datos, tales como códigos o claves públicas, que se utilizan para verificar la firma digital.

Dispositivo de Creación de la Firma (SCD): un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de la firma digital.

Dispositivo de Verificación de la Firma: un programa informático configurado o un aparato informático configurado, que sirve para aplicar los datos de verificación de la firma.

Dispositivo Seguro de Creación de la Firma (SSCD): un dispositivo de creación de la firma que cumple con los siguientes requisitos:

- Los dispositivos seguros de creación de firma garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:
    - los datos utilizados para la generación de la firma sólo pueden producirse una vez en la práctica y se garantiza razonablemente su secreto;
    - existe la seguridad razonable de que los datos utilizados para la generación de la firma no pueden ser hallados por deducción y la firma está protegida contra la falsificación mediante la tecnología existente en la actualidad;
    - los datos utilizados para la generación de la firma pueden ser protegidos de forma fiable por el signatario legítimo contra su utilización por otros.
- Los dispositivos seguros de creación de la firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al signatario antes del proceso de firma.

Documento Digital: los datos a los cuales la firma digital se encuentra adjunta o lógicamente asociada.

Emisor de la Política de Firma: una organización que crea, mantiene y publica una Política de Firma.

Firma Digital Reconocida: una firma digital basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma.

Firma Jerárquica: cuando la estructura de firma digital es secuencial y en cadena, es decir, antes de firmar una determinada persona ha de firmar otra previamente.

Firma Paralela: cuando en la estructura de firma digital no existe ni orden ni jerarquía, lo que realmente importa es que un conjunto de “n” personas firmen un mismo documento.

Framework de Firma Digital: es el conjunto de la Política de Firma y los componentes de software implementados conforme a la política en cuestión para crear y verificar firmas digitales. Este framework provee servicios que pueden ser utilizados por diferentes sistemas informáticos.

Función de Hash: una función que proporciona una secuencia de bits pequeña y de longitud fija asociada a los bits de entrada cumpliendo las siguientes propiedades:

- Es computacionalmente irrealizable encontrar para una salida dada una entrada que pueda ser asociada a dicha salida.
- Es computacionalmente irrealizable encontrar para una entrada dada una segunda entrada que pueda ser asociada a la misma salida.

Identidad del Signatario: el nombre registrado del signatario.

Identificador de Objeto (OID): una secuencia de números que hacen referencia unívoca y permanentemente a un objeto.

Identificador de Política de Firma: un identificador de objeto que identifica sin ambigüedades a una Política de Firma.

Identificador del Certificado: un identificador único de un certificado consiste en el nombre de la CA y el número de serie del certificado asignado por la CA.

Lista de Revocación de Certificados (CRL): es una lista conteniendo los números de serie de los certificados revocados de una CA dada, conjuntamente con otra información de revocación.

Marca de Tiempo: una prueba de existencia de un dato en un punto particular en el tiempo, en forma de registro auditable, el cual incluye al menos un valor de tiempo confiable y un hash que represente dicho dato.

Online Certificate Status Protocol (OCSP): fuente de confianza, en línea y en tiempo real que brinda información sobre el estado de un certificado.

Período de Validez del Certificado: el intervalo de tiempo durante el cual la CA garantiza que mantendrá información sobre el estado del certificado.

Política de Certificación: un conjunto de reglas que indica la aplicabilidad de un certificado a una comunidad particular con requisitos de seguridad comunes.

Política de Firma: conjunto de requisitos técnicos y procedimientos para la creación y verificación de una firma digital, bajo los cuales la firma puede ser determinada como válida.

Punto de distribución de CRL: una fuente de distribución para CRL's; una CRL distribuida a través de un punto de distribución de CRL puede contener entradas de revocación para sólo un subconjunto del total de certificados publicados por una CA o puede contener entradas de revocación de múltiples CAs.

Ruta de Certificación: una cadena de múltiples certificados, conteniendo un certificado del dueño de la clave pública firmado por una CA, y cero o más certificados adicionales de CAs firmados por otras CAs.

Sello Digital de Tiempo (Time Stamp): una prueba de la existencia de un dato en un punto particular en el tiempo, en forma de una estructura de datos firmada por una autoridad de sellado digital de tiempo, la cual incluya al menos un valor de tiempo confiable, un identificador único para cada nuevo timbre de tiempo generado, un identificador que refiera unívocamente a la política de sellado digital de tiempo con la cual el timbre de tiempo fue creado y un hash que represente dicho dato.

Servicios de Firma Digital de CONICET: cualquier producto o servicio que haga uso del Framework de Firma Digital para crear firmas digitales para el usuario del servicio.

Servicio de Sellado Digital de Tiempo: un servicio que provee una asociación confiable entre un dato y un punto particular en el tiempo, que permite establecer una prueba fidedigna indicando el tiempo en el cual el dato existió.

Signatario: la persona que crea una firma digital para firmar un documento.

Verificación de la Firma: un proceso realizado por un verificador ya sea al poco tiempo de la creación de la firma digital o posteriormente para determinar si una firma digital es válida según una Política de Firma referenciada implícita o explícitamente.

Verificación Inicial: un proceso realizado por un verificador que debe ser realizado al poco tiempo que la firma es generada para capturar la información que haga a dicha firma válida en una verificación a largo plazo.

Verificación Usual: un proceso ejecutado por un verificador que puede ser llevado a cabo años después que la firma digital fue producida; no necesita capturar más datos que aquellos capturados al momento de la verificación inicial.

Verificador: una persona que verifica una firma digital de un documento. Puede ser una de las partes involucradas como así también un tercero interesado en la validez de la firma digital.

5. Referencias

[1]: Ley N° 25.506: “Ley de Firma Digital”.

[2]: Decreto Reglamentario N° 2628/02.

[3]: Decretos N° 1028/03, 409/05, 724/06.

[4]: Decisión Administrativa N° 06/2007.

[5]: EC 1999/93: European Community (EC) DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND COUNCIL ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES.

[6]: ETSI ES 201 733 (V1.1.3): “Electronic Signature Formats”.

[7]: ETSI TR 102 041 (v1.1.1): “Signature Policies Report”.

[8]: ETSI TS 101 903 (v1.3.2): “XML Advanced Electronic Signatures (XAdES)”.

[9]: ETSI TR 102 045 (v1.1.1): “Signature Policy for Extended Business Model”.

[10]: ETSI TS 101 733 (V1.7.3): “CMS Advanced Electronic Signatures (CAdES)”.

[11]: ETSI TS 102 904 (V1.1.1): “Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)”.

[12]: RFC 5126: “CMS Advanced Electronic Signatures (CAdES)”.

[13]: RFC 3280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

[14]: RFC 2560: “X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP)”.

[15]: RFC 3161: “Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)”.

[16]: RFC 3647: “Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework”.