Firma.digital

P001 – POLÍTICA DE CERTIFICACIÓN

Junio 2019

Contenido

Introducción

Un Prestador de Servicios de Certificación (CA), por definición, es una institución o persona, ya sea pública o privada que presta servicios de firma electrónica y pueda emitir certificados, que expresamente actúa como tercera parte de confianza entre las personas o instituciones que participan en un acto de identificación, autentificación, firma y gestión documental, utilizando certificados digitales para firma electrónica.

Firma.digital posee dos instrumentos para gestionar su autoridad de registro, los cuales son la "CP" o las Políticas de Certificación y la "CPS" o Declaración de Prácticas de Certificación, definidos a continuación.

Política de Certificación (CP) es el conjunto de reglas de alto nivel, que definen los alcances de uso y aplicación de un certificado en un ecosistema de plataformas electrónicas, con requisitos de seguridad y utilización comunes, es decir, en general una CP o Política de Certificación define la funcionalidad según tipos de certificado para determinadas aplicaciones que exigen requisitos de seguridad y formas de usos.

La Declaración de Prácticas de Certificación (CPS) es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Firmante/Suscriptor o Tercero que confía y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados.

Alcance

Este documento detalla las condiciones de prestación de servicios de **Firma.digital**, para la validación del suscriptor y gestión del ciclo de vida de un certificado digital.

Aplicabilidad y ecosistema de suscriptores

Suscriptores

Firma.digital emitirá sus certificados digitales de firma electrónica simple bajo el estándar X.509 y serán emitidos de forma remota, por lo tanto, su presencia física no es necesaria.

Aplicabilidad

Los certificados emitidos por **Firma.digital** no han sido diseñados, ni se autoriza su uso para cualquier efecto, que al ser usado éste se deriva en muerte, lesiones a personas o al medio ambiente o infrinja la ley.

Los certificados emitidos por **Firma.digital** podrán ser usados en las siguientes necesidades de seguridad:

Identificación y Autentificación

Proporciona suficientes garantías, desde el proceso de validación y emisión, para la identidad y autentificación del suscriptor del certificado digital.

Firma Electrónica

Los certificados digitales, permiten las firmas electrónicas sobre documentos o transacciones, y generan la evidencia criptográfica necesaria para vincular el acto de firma al suscriptor.

Integridad

La información, transacciones o documentos firmados con un certificado digital emitido por **Firma.digital** permiten, a través de rutinas criptográficas estándares, validar que el elemento firmado no cambia su contenido desde el momento de la firma.

Privacidad

La información firmada con un certificado digital emitido por **Firma.digital** permite, a través de rutinas criptográficas estándares, cifrar elementos que solo pueden ser visualizados por el suscriptor.

Tipos y usos de certificados

Firma.digital posee la infraestructura para la emisión de certificados de Firma Electrónica Simple y Tributaria. La estructura de estos certificados cumple y es compatible con el estándar ISO/IEC 9594-8, donde la estructura y contenido de cada certificado cumple con el Reglamento de la Ley 19.799. Para el caso de Firma Electrónica Tributaria, cumple con los requisitos solicitados por el SII.

La estructura contiene al menos los siguientes datos:

- RUTdel suscriptor.
- Correo electrónico del subscriptor.
- Nombre completo del subscriptor.
- Tipo y usos de certificado.
- Datos del emisor **Firma.digital.**

Para el caso de los certificados de firma simple para usos tributarios, contendrá en forma explícita, que el certificado emitido es para operar en el ámbito tributario. Esta indicación queda inserta en el campo "CERTIFICATE POLICIES" de las extensiones del certificado en formato X.509 v3, y su texto debe ser: "Certificado para uso Tributario".

Datos de contacto

Para consultas respecto del contenido del presente documento, pueden ser realizadas vía correo o de forma presencial:

- Nombre: “Prácticas Firma.digital”
- Dirección de contacto: Santa Magdalena 10 of 26, Providencia, Santiago.
- Correo electrónico: practicas@firma.digital

Requerimientos generales y operacionales

Obligaciones

Obligaciones de CA Raíz

Los certificados digitales, se organizan en una jerarquía de confianza, denominada cadena de certificación, comenzando desde la CA raíz o Root CA, esto permite ser utilizado para firmar los certificados de la entidades certificadoras subordinadas o Sub CA necesarias, en estos términos **Firma.digital** se define como entidad raíz y una entidad intermedia, porque ha emitido un certificado par ser utilizado por el mismo para su cadena de certificación.

En el caso que otras entidades de certificación se quieran subordinar (Sub CA) a la jerarquía de certificación de **Firma.digital**, éste último firmará los certificados emitidos.

Obligaciones de la CA

Firma.digital cumple con las obligaciones necesarias para prestar servicio de certificación electrónica, a través de:

- Identificar y autenticar correctamente al suscriptor o usuario de firma electrónica usando correctamente los procedimientos de CA para estos efectos.
- Controles de Seguridad Física.
- Emitir certificados a quienes lo soliciten.
- Administrar un sistema tipo infraestructura de llaves públicas (PKI) para hacer operativa la certificación digital.
- Emitir y mantener una lista de certificados revocados.
- Cumplimiento a todas las obligaciones legales necesarias para el ejercicio de esta actividad.
- Emisión de Certificados:
    - **Firma.digital** emitirá certificados que sean solicitados previa validación y aprobación de los antecedentes necesarios de una persona natural.
- Administración de llaves:
    - **Firma.digital** puede emitir, de forma automática o gestionada, la llave pública y privada que se le entrega al titular, o manual dentro de un dispositivo seguro de almacenamiento

(totalmente opcional en certificasos de firma simple FES o tributarias), garantizando en ambos casos la confidencialidad dela llave privada.

Obligaciones con los suscriptores

- Garantizar que la información suscrita en el certificado es exacta y fiel reflejo de la información entregada por el suscriptor en el acto de emisión del certificado, utilizando si es necesario todas las herramientas de verificación a su alcance.
- Hacer uso de la tecnología adecuada, tanto en Hardware como Software, para la emisión de los certificados.
- Informar preventivamente la proximidad de la caducidad de los certificados.
- Revocar los certificados que no cumplan con las prácticas adecuadas de firma electrónica, o a petición del suscriptor.
- Disponibilizar lista de certificados revocados, la cual debe ser constantemente actualizada.
- Poseer procedimientos y políticas adecuadas para el resguardo de la llave privada del suscriptor.

Obligaciones del suscriptor

• Conservar y dar uso adecuado al certificado digital simple, según lo descrito en contrato de suscripción.

• Dar correcta custodia al certificado, resguardar su clave privada y no dar mal uso al mismo.

• Proteger el uso de su certificado mediante password en un PC o en plataformas transaccionales provistas por terceros que cumplan con estándares de confianza mínimos al suscriptor.

• Informar a **Firma.digital** inmediatamente por cualquier situación que afecte directamente la validez del certificado, o si su clave privada se ve comprometida.

Obligaciones generales de Firma.digital como CA

• Si **Firma.digital** decide dar término a sus funciones de firma electrónica, dará a conocer su decisión a todos sus suscriptores activos, y en lo posible, transferir todos sus certificados a otro prestador de firma electrónica compatible. Los suscriptores pueden negarse a dicha transferencia, en cuyo caso el certificado quedará en estado revocado.

• **Firma.digital** cumplirá todas las leyes que rigen este tipo de actividades, como la ley del consumidor Nº 19.496 y de protección de la vida privada Nº 19.628.

• **Firma.digital** podría informar preventivamente a entidades públicas de cualquier evento que afecte directamente la continuidad operacional.

• **Firma.digital** se compromete a mantener constantemente el registro electrónico de los antecedentes de los suscriptores.

• **Firma.digital** se compromete a almacenar de forma segura y electrónica la informacion que evidencie la validación y emisión de sus certificados de algún suscriptor por un periodo no menor a a la vigencia del certificado emitido.

Obligaciones del solicitante

• Entregar toda la información de identificación personal o de su empresa que se le solicite, a través de cualquier medio, tecnología o evidencia que se necesite para su correcta identificación y validación.

• El solicitante deberá cancelar la tarifa establecida y publicada en la página web **https://firma.digital** por el certificado que solicite.

Lista de revocación y estructura de información

En la página web de **Firma.digital** están los repositorios donde se informan los certificados emitidos y revocados para Firma Electrónica Simple y Tributaria.

Certificados para firma electrónica Simple:

Lista de certificados de revocación se encontrarán en: **https://firma.digital/public/fes.crl**

Confianza de terceros en la firmas

Las personas que reciben algún elemento con firma electrónica realizada con un certificado emitido por **Firma.digital** tendrán derecho a confiar en ello:

- La operación que se utilizó para firmar tiene todos los resguardos de seguridad y uso de las llaves privadas y públicas del suscriptor.
- Que el certificado que utilizó en la firma del elemento, no tenga estado caducado en el momento de la firma.

Confianza en los certificados

Las personas que utilicen o reciban un elemento firmado por un certificado emitido por **Firma.digital** tendrán derecho de confiar en dicho certificado.

Protección de información

Toda la información entregada por los clientes a Firma.digital es sólo de carácter interno y se compromete a no utilizar esta información en otros aspectos que sean exclusivamente relacionados con sus actividades de certificación. La entrega de esta información a terceros está estrictamente regida de la siguiente forma:

Información que se puede entregar

Para certificados de firma simple, la información contenida en los certificados será:

• RUTdel suscriptor.
• Correo electrónico del subscriptor.
• Nombre completo del subscriptor.
• Tipo y usos de certificado.
• Dato RUT del emisor **Firma.digital.**

Casos particulares de entrega de información de titulares de certificados

Firma.digital entregará información de titulares sólo en los casos que permite la ley que rige la firma electrónica, y esto es, por el titular del certificado o en algún tribunal en virtud de algún procedimiento judicial.

Declaración operacional

Registro inicial

Se verificará la identidad y/o autentificará al usuario que solicite el certificado exigiendo datos y antecedentes como el documento nacional de identidad, un certificado digital válidamente emitido y vigente, u otros medios admitidos en derecho. Adicionalmente se podrá hacer exigible otro mecanismo de autenticación entre los cuales pueden estar: un certificado digital previamente emitido vigente de **Firma.digital** o incluso de otra CA acreditada en Chile; una transacción electrónica válida originada por el suscriptor, y donde haya utiizado un factor de autentificación válido; una prueba de vida o biométrica, o en general cualquier medio, tecnología o evidencia que se necesite para su correcta identificación. Una vez generado el Registro, se autorizará para la emisión del certificado.

Reemisión de certificados

Los certificados emitidos por **Firma.digital** tendrán solo dos estados, Vigentes y Revocados, la reemisión de llaves no está soportada con el claro objetivo de mantener altos estándares de seguridad en el caso de los certificados emitidos por **Firma.digital**.

Lo mismo ocurre para el caso de los certificados revocados, no reemitirá llaves con un certificado en este último estado.

Revocación

Las solicitudes de revocación de los certificados emitidos por **Firma.digital** se realizarán por vía electrónica en la página web, o por correo electrónico directo a revocacion@firma.digital

Posibles causas de revocación

- Solicitud del suscriptor.
- Pérdida del certificado o alteración del elemento donde almacena el certificado.

- Fallecimiento del suscriptor o de algún representado, termino de la representación de la persona jurídica.
- Por alguna eventualidad que comprometa la llave privada del suscriptor, ya sea por robo, alteración, divulgación o cualquier otro tipo de causal circunstancial.
- Por incumplimiento de suscripción, por parte de la CA o el suscriptor.
- Por resolución judicial o administrativa.
- Por cualquier otro motivo, que exponga claramente o ponga en riesgo la llave privada del suscriptor, o no se cumpla de alguna forma el contrato de suscripción.

Formas de revocación

La revocación se genera mediante solicitud previa, por cualquiera de los canales que posee la CPS para estos efectos o por la concurrencia del suscriptor del certificado, o en su defecto, la persona jurídica a la cual fue emitido el certificado.

Canales de atención para la revocación

• Vía correo electrónico a revocacion@firma.digital

• Vía formulario en sitio Web

Sólo el suscriptor debe realizar esta tarea, si es el caso de que la solicitud sea realizada por otra persona, esto se deberá realizar por carta certificada a **Firma.digital**. Utilizando el formulario respectivo registrado en el sitio web, previa firma e impresión de huella dactilar en la misma.

Publicación de la revocación

El acto de revocación será comunicado al suscriptor, así como el origen de la decisión de la misma, vía correo electrónico. Cualquier forma de acción o solicitud de revocación será publicada en la lista de certificados revocados (CRL), disponible en https://crl.firma.digital/clase2firmadigital-G1.crl

Al ser publicado el certificado caducado, eso inmediatamente generará cambios en la CA con la imposibilidad de reutilizar el certificado. En el caso de término de actividades de firma electrónica de la CA, este acto de certificados revocados quedará efectivo inmediatamente después que esto ocurra.

Caducidad

Luego de finalizado el período de vigencia del certificado, éste caducará de forma automática. Se informará al suscriptor del certificado de forma anticipada y vía email a la fecha de caducidad para que pueda decidir preventivamente su total caducidad o renovación. La caducidad del certificado produce su invalidez de forma automática, caducando también los servicios de certificación.

Renovación

El procedimiento de renovación, se ejecuta cuando el certificado está próximo a caducar y el suscriptor decide su renovación con la misma CA. Para dicho caso, **Firma.digital** emitirá un nuevo certificado y se generarán nuevas llaves, requiriendo verificar previamente la vigencia de la validación del suscriptor, cuya vigencia es a lo más de 3 años, o bien generar una nueva verificación de identidad. Los certificados emitidos por **Firma.digital** tienen una vigencia que no podrá exceder de tres años contados desde la fecha de emisión; y para su renovación se debe cumplir:

- Que exista actividad de certificación previa en esta CA por parte del suscriptor y emitido por Firma.digital.
- Que el suscriptor solicite en los tiempos adecuados y preventivos para la renovación, y esta solicitud sea enviada a Firma.digital en los procedimientos declarados para esos efectos.
- Que la CA verifique que no exista una revocación previa del certificado original.
- Que el suscriptor pueda hacer todas las actividades necesarias para solicitar la emisión de un certificado.

Solicitud de renovación

Para renovación de certificados digitales, se utilizará el mismo proceso de solicitud de certificado, desde la página web. Si se cumplen los requisitos para la emisión.

Procedimiento de renovación

Una vez recibida la solicitud y verificado que cumple con los requisitos. Se procesará la solicitud de la misma forma como se procesan los demás certificados.

- La CA emitirá el certificado solicitado
- La emisión del certificado emitirá un correo electrónico al solicitante.
- En el correo se informará que el certificado está disponible y que puede ser descargado desde el sitio Web.

Cabe destacar que para la verificación del suscriptor se realizará lo siguiente:

• Se verificará la vigencia de la verificación de identidad almacenada, que confirma la identidad del suscriptor, requiriendo un nuevo procedimiento de enrolamiento si se considera vencida.

Término de actividades de la CA

En el caso del cese de actividades de la CA se declaran las siguientes medidas:

- Comunicación preventiva del cese de actividades:
  - Notificación vía Web.
  - Publicación de anuncio de cese en al menos dos diarios de divulgación nacional.
  - Toda información se realizará con al menos 60 días antes de la fecha indicada de cese definitivo.

Auditorías

Firma.digital podría contar con procesos de auditoría internos y de terceros cada vez que permitan asegurar, mantener y mejorar contínuamente los altos niveles de seguridad en sus procesos.

Administración y modificaciones

Firma.digital podrá hacer cambios en sus procedimientos, manteniendo siempre los estándares exigidos a una entidad emisora de certificados de firma electrónica. Estos cambios podrían ser justificados desde un punto de vista Técnico, Comercial y/o Jurídico, las veces que estime conveniente.

Publicación de modificaciones

Todo cambio en la CP o CPS que involucre directamente la operación de los certificados, podría ser informado vía Web a sus suscriptores y solicitantes en un período no superior a 15 días, desde la aplicación de los cambios.

Luego del comunicado, y si no se recibe ninguna declaración por escritor de suscriptores o solicitantes, en contra de lo comunicado, las modificaciones se declararán como aceptadas por la comunidad de suscriptores.

Referencias y glosario

Cómo referencia se consideraron las principales normas técnicas registradas por la Entidad de Acreditación, aunque si bien es cierto aplican sólo para certificados de firma electrónica avanzada (FEA), son usados como marco de trabajo referencial en certificados digitales para firma simple (FES), vinculados desde https://www.entidadacreditadora.gob.cl/normas-tecnicas/

- ETSI TS 102 042 V1.1.1 (2002-04). Technical Specification. Policy requirements for certification authorities issuing public key certificates.
- NCh2805.Of2003 Tecnología de la Información – Requisitos de las políticas de las autoridades certificadoras que emiten certificados de claves públicas.
- ETSI TS 102 042 V1.2.2 (2005-06) .RTS/ESI-000043.Keywords e-commerce, electronic signature, public key, security.
- ETSI TS 102 042 V2.1.1 (2009-05). Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 102 042 V2.1.2 (2010-04) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- NCh27002.Of2009 Tecnología de la información – Código de práctica para la gestión de seguridad de la información.
- ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001).
- NCh.2820/1.Of2003 Tecnología de la información – Técnica de seguridad – Criterio de evaluación de la seguridad de TI – Parte 1: Introducción y modelo general.
- NCh2832.Of2003 Tecnología de la información – Protocolos operacionales de infraestructura de clave pública LDAPv2 para Internet X.509.
- RFC 2559 BOEYEN, S. et al., "Internet X.509 Public Key Infrastructure. Operational Protocols LDAPv2", Abril 1999.
- RFC 3377 LDAPv3: Technical Specification, September 2002, Lightweight Directory Access Protocol (v3): Technical.

Glosario:

- Representación Digital: Es un documento representado en forma binaria, sin hacer referencia a su medio de almacenamiento o soporte, susceptible de ser firmado electrónicamente.

- Documento Digital: Es toda representación digital que de testimonio de un hecho, una imagen o una idea.

- Firma Electrónica: El sustituto digital de la firma ológrafa que permite al receptor de un documento digital, verificar con certeza la identidad proclamada por el emisor del mismo, mantener la integridad del contenido del documento digital transmitido e impedir al signatario desconocer la autoría del documento digital o repudiarlo en forma posterior.

- Certificado Digital: Es un documento digital firmado y emitido electrónicamente por un Prestador de Servicios de Certificación, que asocia una clave pública con su titular durante el período de vigencia del certificado y que, debidamente almacenado y publicado en un repositorio o registro público electrónico, se utiliza como referencia para acreditar la identidad digital del contribuyente, que es titular de dicha clave, junto a sus datos de identificación, utilizando sistemas que garanticen la seguridad técnica y criptográfica de los procesos de certificación.

- Signatario: Es la persona que actúa en nombre propio o en el de otra persona natural o jurídica a la que representa, y que, habiendo obtenido previamente un certificado digital de un Prestador de Servicios de Certificación debidamente acreditado ante el Servicio, tiene la capacidad de firmar un documento digital.

- Clave Privada: Es aquella que se utiliza para firmar electrónicamente, utilizando un criptosistema asimétrico seguro.

- Clave Pública: Clave que es publicada y que al ser incorporada en un certificado digital válidamente emitido y almacenada en un repositorio, es utilizada para verificar las firmas electrónicas, basadas en su correspondiente o correlativa clave privada.

- Criptosistema Asimétrico Seguro: Es un método criptográfico que utiliza un par de claves compuesto por una clave privada utilizada para firmar electrónicamente y su correspondiente clave pública, utilizada para verificar esa firma electrónica, de forma tal que, con las longitudes de claves utilizadas, sea computacionalmente no factible tanto obtener o inferir la clave privada a partir de la correspondiente clave pública como desencriptar aquello que ha sido encriptado con una clave privada sin la utilización de la correspondiente clave pública.

- Prestadores de Servicios de Certificación: Son las entidades que, en resguardo de la fe pública en materia tributaria, otorgan los certificados digitales, para lo cual generan, reconocen y revocan claves en forma expedita y segura.

- Entidad de Certificación Acreditada: Prestador de Servicios de Certificación previamente autorizado por el Servicio de Impuestos Internos, para operar como emisor de certificados digitales para uso tributario.

- Certificados Digitales Para Uso Tributario: Certificados que han sido emitidos por una Entidad de Certificación Acreditada y que cumplen con los requisitos establecidos por el Servicio de Impuestos Internos para que el contribuyente los utilice para respaldar y asegurar técnica y jurídicamente los trámites realizados electrónicamente o intercambiar información con el Servicio de Impuestos Internos. Estos pueden ser de dos tipos: primero, certificados para personas naturales y segundo, certificados para representantes legales o mandatarios de personas jurídicas o naturales.

- Certificado Digital para Pago Tributario: Es un tipo de certificado digital para uso tributario, que tiene la característica de ser aceptado por algún banco o institución financiera autorizada para efectuar cargos en cuentas bancarias de los contribuyentes.

- Tarjeta Inteligente: Cualquier tarjeta portátil que pueda almacenar en forma segura y persistente certificados digitales y que, de acuerdo a estándares técnicos ampliamente aceptados, permite que ellos sean intercambiados.

- Usuario Certificado: Es un contribuyente o su representante legal o mandatario, que posee un certificado digital para uso tributario vigente, el cual puede estar almacenado en forma segura en el mismo computador, en una tarjeta inteligente o en otros medios tecnológicos que el Servicio de Impuestos Internos acepte como válidos.

- Sistema de Acreditación: Conjunto de exigencias, prácticas y procedimientos que el Servicio de Impuestos Internos define para acreditar a los Prestadores de Servicios de Certificación.

- Hashing: Secuencia de caracteres que representan un documento. Esta secuencia es de tamaño fijo y reducido. La principal característica es que es una representación única del

documento original y que si existe una alteración mínima el resultado es absolutamente distinto y deja de representar al documento original.