Firma.digital

P002 – DECLARACIÓN DE PRÁCTICAS 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.

Estos conceptos de Políticas de Certificación y Declaración de Prácticas de Certificación son distintos, pero aun así es muy importante su interrelación.

Una Declaración de Prácticas de Certificación detallada no forma una base aceptable para la interoperabilidad de Autoridades de Certificación. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes. En definitiva, una Política define "qué" requerimientos de seguridad son necesarios para la emisión de los certificados. La Declaración de Prácticas de Certificación nos dice "cómo" se cumplen los requerimientos de seguridad impuestos por la Política.

Alcance

Detallar las condiciones de prestación de servicios de **Firma.digital**, para la emisión de sus certificados de Firma Electrónica Simple (FES).

Antecedentes

El modelo de Confianza adoptado por **Firma.digital** se basa principalmente, en implementar una infraestructura de confianza basada en PKI (Public Key Infraestcruture). Esta PKI utiliza tecnología estándar y segura basado en certificados compuestos de un par entre llave pública y llave privada.

El modelo de Confianza de **Firma.digital** se basa en el tercero que confía (Trusted Third Party). Esto hace que un tercer elemento, ya sea, persona, empresa o aplicación pueda confiar en otra sin necesidad que la conozca.

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 durante el 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.

Aplicabilidad Global

Para el desarrollo de negocios de los suscriptores de **Firma.digital**, en cuanto a firma electrónica simple, resulta muy estratégico disponibilizar un modelo de confianza de visión global con el claro objetivo que los suscriptores puedan utilizar los servicios de **Firma.digital** en forma transversal en cualquier industria, y siempre basándose en el modelo de confianza, es decir, el tercero que confía.

Firma.digital utiliza una raíz creada por **Firma.digital**, generando una cadena de certificación, lo que hace confiar inmediatamente que cada certificado emitido por **Firma.digital** queda operativo bajo esa raíz, otorgando un reconocimiento inmediato de todas las organizaciones que reconozcan los certificados de clase 1 o clase 2 según sea necesario.

Rol frente a los suscriptores

El principal rol de **Firma.digital** frente a los suscriptores y terceros que confían, es de realizar todas las tareas, desarrollos y procedimientos orientados a mantener el modelo de confianza definido, correspondiente a las siguientes funciones:

- Administrar la CPS: corresponde a todas las tareas para mantener las prácticas de certificación de **Firma.digital**.
- Definición de requisitos y condiciones de aceptación de las Autoridades de Registro, con el fin de mantener el modelo de confianza de **Firma.digital**.
- Operación de la Autoridad de Registros de la CA.

Compatibilidad, neutralidad tecnológica e interoperabilidad

Son las especificaciones, requisitos y tareas, específicamente en lo tecnológico, para que la aplicación o proceso propietario del suscriptor y quien confía (modelo de confianza) pueda interactuar sin problemas con los servicios de firma de **Firma.digital**. Para esto **Firma.digital** utiliza en todos sus componentes software neutral tecnológicamente, y altamente apegado a estándares internacionales.

Para la opción de integración en soluciones propietarias del cliente o proyectos de mayor envergadura en el uso de firma electrónica, se deberá evaluar en conjunto con el suscriptor y el equipo de trabajo en cada caso.

Procedimientos

A continuación se describe el ciclo de vida en su totalidad, de la emisión de certificados de Firma Electrónica Simple.

Solicitudes

Para cada emisión de certificado de firma electrónica, la primera instancia es la solicitud por parte del futuro suscriptor, la cual se realiza vía Web.

Comprobación de Solicitud

Una vez recibida las solicitudes de emisión de certificados, **Firma.digital** debe validar la confianza de identidad de suscriptor en cada solicitud, utilizando todos los mecanismos, tecnologías o servicios tanto públicos como privados que tenga a su alcance.

Si el suscriptor posee un proceso de verificación, autentificación y/o enrolamiento previo exitoso, ya sea de Firma.digital o de otra CA o PSC acreditada en el país, entonces se emitirá el certificado solicitado, de lo contrario pasará a un proceso de evaluación y validación de scoring, en donde se solicitarán datos adicionales, para corroborar la identidad y asignar una clasificación de riesgo.

Solicitud Aceptada

Una vez confirmados los datos de compra del suscriptor, se enviará un código de activación a la casilla de email del suscriptor, para que continúe con su proceso de emisión.

Solicitud Rechazada

En el caso que los suscriptores no cumplan la adecuada información o bajo scoring de seguridad, o su documentación no esté vigente, o que no concuerden todos los antecedentes, o que no cumplan los requisitos para ser Suscriptor, la solicitud será rechazada.

Emisión de Certificados

Una vez que todos los antecedentes del suscriptor sean aprobados por **Firma.digital**, se generará y ejecutará el procedimiento técnico para emitir certificado, siendo de carácter personal e intransferible a nombre del Suscriptor.

El Suscriptor se obliga a:

No revelar la clave privada del certificado

- Custodiar el certificado, previniendo su pérdida, uso inadecuado.
- Notificar cualquier detección de robo o falsificación, al igual que pérdida.
- Devolver el certificado en el caso que **Firma.digital** lo solicite.
- Destruir el certificado si no se utiliza

La duración de todos los certificados emitidos por **Firma.digital** no podrán exceder de tres años contados desde la fecha de emisión.

Condiciones de Uso de Certificados de Firma Electrónica

Los certificados de Firma Electrónica emitidos por **Firma.digital** podrán ser utilizados por toda su comunidad de clientes en los lugares y operaciones que el suscriptor estime conveniente y donde **Firma.digital** haya sido homologada o reconodida previamente para funcionar, cumpliendo con sus obligaciones como suscriptor.

Verificación de Certificados

Mediante el protocolo OCSP (Online Certificate Status Protocol) toda la comunidad de clientes de **Firma.digital** y terceros que confían pueden verificar el estado de los certificados de Firma Electrónica Simple.

La lista de certificados revocados (CRL), de igual forma se puede utilizar para estos fines, ya que en esta lista se encuentran los certificados revocados que alguna vez emitió **Firma.digital.**

La autoridad de Registro, directamente indicará los costos asociados del servicio de consulta del estado del certificado, si fuese el caso.

Revocación de Certificados

Los certificados revocados se encontrarán en la lista de revocación (CRL), publicadas en la página **https://crl.firma.digital/clase2firmadigital-G1.crl**

Las causales de revocación de los certificados son:

- 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.

Expiración de Certificados

Una vez que se cumple la fecha de expiración de los certificados emitidos por **Firma.digital**, quedan automáticamente deshabilitados para su uso. Sin perjuicio de lo anterior, **Firma.digital** notificará a los suscriptores cuyos certificados vayan a expirar para ofrecerles la alternativa de renovación del certificado. **Firma.digital** emitirá certificados con vigencia que no podrá exceder de tres años contados desde la fecha de emisión.

Contenido y Estructura de Certificados

A continuación, se detallan las características del contenido de los certificados:

- Versión. Deberá ser versión 3.
- Número de Serie. Identificador Único de los certificados emitido por Firma.digital.
- Algoritmo de Firma. Será SHA256 con RSA.

- Datos del Emisor de la Firma. DN en formato x.500, incluyendo al menos: Tipo de certificado, email de contacto, Nombre del emisor, Rut del emisor.
- Período de validez. Fecha de inicio y término de vigencia del certificado.
- Datos del Suscriptor. Nombre completo, email, RUT.
- Clave Pública.

Respecto a la clave privada, ésta no podrá ser de una longitud menor a 2048 bits.

Almacenamiento de Certificados

Almacenamiento

Una vez emitido el certificado digital, para el caso de Firma Electrónica Simple, será posible y admisible la instalación en disco duro o similar y no necesariamente criptográfico.

Obligaciones del suscriptor

• El suscriptor se obliga almacenar su certificado en los dispositivos compatibles.

• Utilizar el certificado emitido para los fines solicitados, informando de manera oportuna a Firma.digital en caso de presentarse un compromiso de seguridad del mismo.

• Solicitar la revocación del certificado en caso de cumplirse las condiciones establecidas.

• No revelar la clave privada ni claves para acceder a ella.

• Verificar y asegurar que la información contenida en el certificado es fidedigna e informar a **Firma.digital** de cualquier información incorrecta o inexacta.

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.