POLÍTICA PRÁCTICAS DE CERTIFICACIÓN

Contenido

1 Identificación del Documento

Identificación del documento	Prácticas de Certificación
Documento(s) relacionado(s)	POL PKI 01 Política de Certificación 18PO 02 Guía de Acreditación
Responsable de aprobación (anual)	Directorio - Comité de Riesgo
Dueño funcional	Gerente de Riesgo
Período de revisión	Anual
Actualización	Anual

2 Control de Versiones

Versión	Descripción del cambio	Solicitado por:	Realizado por:	Aprobado por:	Fecha Aprobación	Vigente a partir de:
1.0	Revisión anual y cambio de formato	CEO	Gte Riesgo	Comité de Riesgo y Directorio	Jul18	Jul18
1.0	Revisión anual	CEO	Gte Riesgo	Comité de Riesgo y Directorio	Jul19	Jul19

3 Introducción

El modelo TOC para firma electrónica provee a toda la comunidad los servicios de firma electrónica, simple o avanzada, bajo los estándares que exige cada tipo y con constantes auditorias respecto a su adecuado uso.

TOC considera todos los aspectos legales, tecnológicos, comerciales y operacionales de un Modelo de Confianza entre la PSC de TOC y la comunidad de clientes. Todo lo anterior cumpliendo con los requisitos de la ley de firma electrónica, su reglamento y guías de acreditación.

Para la interacción de TOC con la comunidad de clientes, se ha definido un rol específico: el Oficial de la Autoridad de Registro (Oficial RA), cuyas principales responsabilidades son las de procesar todas las solicitudes de registro, aprobando o rechazando las solicitudes que genera la Autoridad de Registro (RA), enviándolas a TOC para la emisión del certificado.

El presente documento describe el proceso de contingencia, que se ha definido por cada solicitud realizada por la comunidad de clientes y está orientado a los oficiales RA.

4 Objetivo del documento

En el presente documento se detallan las Prácticas de Certificado (CP) del modelo de Firma Electrónica de TOC.

5 Glosario

- **Llaves (Claves) Públicas y Privadas:** Corresponde a dos secuencias de información relacionadas entre sí, que utilizan técnicas de encriptación, usando pares de llaves (o claves). Una se utiliza para encriptar y la otra para desencriptar. Al menos una de ellas debe ser privada.
- **Firma Electrónica:** De acuerdo a la ley de Firma Electrónica regida en Chile, es cualquier sonido, símbolo o proceso electrónico, que permite al receptor del documento electrónico, pueda identificar formalmente al autor. Es un vínculo único e irrepetible representado en una secuencia de caracteres. Este vínculo es el resultado entre el algoritmo hash al contenido del documento y la llave (o clave) privada del firmante. De esta forma se genera una asociación directa entre quien firmó el documento y el documento en sí y que se pueda detectar cualquier cambio posterior.
- **Firma Electrónica Avanzada:** Según la ley de Firma Electrónica que rige en Chile, es aquella que está certificada por un prestador acreditado. Ha sido creada bajo elementos que el autor mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo, permitiendo la detección de cualquier modificación posterior, verificando la identidad del autor.
- **Hashing:** Son una secuencia de caracteres que representan un documento. Estas secuencias son 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.
- **Certificado:** Es todo registro que evidencie el vínculo entre un firmante y los datos de creación de Firma Electrónica.
- **Firma electrónica:** Es un vínculo único e irrepetible representado en una secuencia de caracteres. Este vínculo es el resultado entre el algoritmo hash al contenido del documento y la llave privada del firmante. De esta forma se genera una asociación directa entre quien firmó el documento y el documento en sí y que se pueda detectar cualquier cambio posterior.
- **Suscriptor de un Certificado:** Corresponde a la persona o empresa a la cual se emitió el certificado. Este suscriptor posee una llave pública y otra privada que son utilizadas en cada firma que realice. Según la ley el suscriptor es la persona que tiene en su absoluto control el certificado de firma electrónica.
- **Certificador:** Es la persona o empresa que puede verificar la identidad de los solicitantes.
- **Autoridad de registro (AR o RA, por su sigla en inglés, Registry Authority):** Es la empresa o institución que controla la generación de certificados llevando un registro electrónico de los mismos, para los miembros de una entidad. Previa identificación, la Autoridad de Registro se encarga de realizar la petición del certificado y de guardar los datos pertinentes. Este registro se realiza encargándose de la detección, comercialización y administración de las solicitudes de todos los tipos de certificados que comercializa TOC.
- **Usuarios:** El usuario del certificado es la persona que decide usar los certificados emitidos por TOC y hace uso de ellos
- **CRL:** Es un directorio público donde se informa el estado de los certificados, específicamente los certificados revocados.
- **CPS:** Correspnde a las Prácticas de Certificación
- **DAS:** Son los dispositivos de almacenamiento Seguro y corresponden en el caso de TOC a los eToken que se utilizarán para almacenar las claves privadas y el certificado en forma segura.

6 Modelo de Confianza

El Modelo de Confianza adoptado por TOC se basa en implementar una infraestructura de confianza basada en PKI (Public Key Infraestcruture). Esta PKI utiliza tecnología y nomenclatura de llave (o clave) pública y privada.

Como infraestructura de confianza, esta provee el soporte de seguridad para las aplicaciones y documentos electrónicos de una organización, en forma uniforme. La infraestructura esta compuesta por una serie de elementos, entre los cuales se encuentra, las entidades registradoras (Clientes), certificadora (TOC) y todas las funciones y prácticas a su alrededor.

El Modelo de Confianza de TOC se basa principalmente en el tercero confiable (Trusted Third Party). Esto hace que un tercer elemento, ya sea, persona, empresa o aplicación, pueda confiar en otra sin necesidad que la conozca. Esto puede ocurrir básicamente por la identificación que realiza TOC.

Los niveles de confianza otorgados en los certificados emitidos por TOC, son un nivel superior en cada suscriptor, esto porque se realiza un acto presencial en cada emisión de certificado. Esta identificación positiva, queda disponible para todos los clientes que quieran validarla.

7 Aplicabilidad

Comunidad de Usuarios

TOC emitirá sus certificados digitales en el estándar ITU-T Recommendation X.509, y serán emitidos a toda persona física o representantes legales de empresas públicas o privadas. Para ello TOC requerirá asegurar la identidad del interesado o suscriptor requiriendo identificarlo completamente ante la Autoridad de Registro, con presencia física.

Aplicabilidad

Los certificados emitidos por la Autoridad Certificadora TOC no han sido diseñados, ni tampoco 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 de la República.

Los certificados emitidos por TOC, podrán ser usados en las siguientes necesidades de seguridad:

Necesidad	Detalle
Autenticación	Debe dar suficientes garantías respecto a la Identidad del Titular solicitante del certificado. Para esto debe requerir la presencia física del futuro suscriptor ante la Autoridad de Registro TOC. Junto a la presencia del futuro suscriptor, debe requerir la Solicitud del Certificado que acredite su identidad.
No Repudiación	Las firmas electrónicas producidas con certificados emitidos por la Entidad de Registro TOC tienen la evidencia necesaria para enfrentar que una persona deniegue la autoría de la firma digital, o el contenido de éste, que se haya firmado digitalmente con el certificado emitido a la persona.
Integridad	La información firmada con un certificado digital emitido por la **Autoridad de Registro TOC** permite validar que el elemento firmado no cambia su contenido entre el origen y el destino.
Privacidad	Los certificados emitidos por la **Autoridad de Registro TOC**, permiten cifrar elementos que solo pueden ser visualizados por el titular de los datos de creación de Firma Electrónica.

8 Aplicabilidad Global

Para el desarrollo de negocios de los suscriptores de TOC, en cuanto a firma electrónica simple o avanzada, resulta estratégico disponibilizar un modelo de confianza de visión global con el claro objetivo que los suscriptores puedan utilizar los servicios de TOC en forma transversal en cualquier industria, y siempre basándose en el Modelo de Confianza, es decir, el tercero que confia.

TOC utiliza una raíz creada íntegramente por TOC, y que está disponible en la Time Stamping List (TSL), lo que permite confiar ya que cada certificado emitido por TOC queda operativo bajo esa raíz, otorgándole un reconocimiento inmediato de todas las organizaciones que reconozcan los certificados de clase 2.

9 Rol de TOC frente a los suscriptores

El rol de TOC frente a los suscriptores y terceros que confían, es el de realizar todas las tareas y desarrollos para mantener el Modelo de Confianza, lo que corresponde a una serie de funciones que se encargan de:

- Administrar la Declaración de Prácticas de Certificación (CPS): Corresponde a todas las tareas para mantener las prácticas de certificación de TOC, igualmente se encarga de revisar las PSC que están postulando para ser acreditadas y que puedan estar en el Modelo de Confianza descrito.
- Definir de todos los requisitos y condiciones de aceptación de las Autoridades de Registro, incluyendo contratos, regulaciones, etc. con el claro objetivo de mantener el Modelo de Confianza de TOC.
- Operar la Autoridad de Registros (RA) de la Prestadora de Servicios de Certificación (PSC) como lo reconoce la ley de firma electrónica en Chile.
- Regular las normas y políticas de conicimiento público, resguardando la propiedad intelectual y velar por la No utilización de esto sin previo aviso o autorización por TOC.

10 Requisitos de Integración

Son las especificaciones, requisitos y tareas específicamente tecnológicas para que la aplicación o proceso propietario del suscriptor y quien confía, puedan interactuar sin problemas con los servicios de firma de TOC.

Las aplicaciones que interactúan naturalmente con los servicios de firma de TOC, son específicamente los browser (Explorer, Firefox y otros).

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

11 Procedimientos

Para la firma electrónica avanzada, se implementan procedimientos adecuados para el otorgamiento del producto.

11.1 Solicitud de un Certificado

Para cada emisión de certificado de firma electrónica, la primera instancia es la solicitud por parte del futuro Suscriptor, sea por presencial o vía Web.

Para el caso de firma electrónica avanzada se requiere:

- Identificación adecuada: es presencial y considera la firma de un contrato de suscriptor, la firma de formulario de entrega de firma electrónica avanzada y la fotocopia de la Cédula de Identidad.
- Si estuviese disponible, se puede incluir procedimientos adicionales de identificación positiva, como por ejemplo elementos de identificación Biométrica.

Comprobación de Solicitud

Una vez recibida la solicitud de emisión de certificados, TOC debe generar la confianza de identidad de cada solicitud.

Los Suscriptores de certificados TOC que posean un certificado válido, están protegidos contra el fraude de identidad cuando ellos lo utilicen. Los Terceros que confían en un certificado correctamente emitido, también están protegidos contra el fraude de identidad, siguiendo los procedimientos de verificación que TOC establece en las prácticas de certificación.

Solicitud Aceptada

Una vez confirmada la identidad, la aceptación de la solicitud se realiza ante la Autoridad de Registro y debe cumplir con los requisitos de suscriptor. Se indicará al solicitante vía correo electrónico, la documentación que debe presentar, comprometiéndose el solicitante a paguar el importe que corresponde al tipo de certificado que esta solicitando.

El solicitante deberá presentarse en Avenida Santa María 2670, oficina 403, Las Condes en horarios de 9:00 a 18:00, solo en días hábiles.

Solicitud Rechazada

En el caso que los solicitantes no cumplan la adecuada información, su documentación no esté vigente, que no concuerden todos los antecedentes, o que no cumplan los requisitos para ser suscriptor, la solicitud será rechazada.

11.2 Emisión de Certificados

Una vez que todos los antecedentes del solicitante sean aprobados por la Autoridad de Registro, se genera y ejecuta el procedimiento técnico para emitir certificado y es en carácter personal e intransferible a nombre del ahora, 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 TOC lo solicite.
- Destruir el certificado si no se utiliza.

La duración de todos los certificados emitidos por TOC será de 1 año

11.2 Casos de Excepción

En el caso que el Suscriptor no cumpla con algún requisito documental, se le solicitará que lo solucione a la brevedad, pidiendo que vuelva posteriormente con toda la documentación necesaria para el proceso de emisión de firma electrónica avanzada.

11.3 Condiciones de uso de un certificado

Los certificados de firma electrónica emitidos por TOC podrán ser usados por toda la comunidad de clientes de TOC, será decisión solo de los clientes en qué lugares u operaciones utilizará la firma electrónica avanzada.

11.4 Verificación de Certificados

Mediante el protocolo OCSP (Online Certificate Status Protocol) toda la comunidad de Suscriptores y de Terceros que confían podrá verificar la validez y status del certificado emitido por TOC.

La comunidad antes mencionada, que no tenega acceso en línea a este servicio podrá verificar la validez del certificado por el repositorio de certificados TOC.

La lista de certificados revocados (CRL) contiene todos los certificados revocados y expirados (o caducados), que alguna vez emitió TOC y se encuentra disponible para consultas en www.toc.cl.

La Autoridad de Registro indicará los costos asociados al servicio de consulta del estado del certificado.

12.2 Revocación de Certificados

Existen motivos diferentes a la expiración de un certificado, asociados a la que la Autoridad determine que es causal de revocación, estos son:

- Por solicitud del suscriptor.
- Por fallecimiento del titular o disolución de la sociedad a la cual el representa.
- Por resolución judicial.
- Por falta a las políticas de certificación de TOC.

12.3 Expiración de Certificados

Una vez que se cumpla la fecha de vigencia del certificado, cuya fecha está contenida en el mismo, se publicará este certificado en la lista de certificados revocados (CRL). TOC notificará al Suscriptor vía correo electrónico la pronta fecha de caducidad de su certificado para así y en el caso que sea necesario, se renovarlo, emitiendo un nuevo certificado de firma electrónica avanzada. La alternativa de renovación está disponible para no generar un registro completo nuevamente del mismo suscriptor.

13 Contenido y Estructura de los Certificados

A continuación se detallan las características del contenido y estructura del certificado

- Certificado X.509 v.3
- Para certificados de objetivos de Firma y Encriptación para Firma Electrónica
- Encriptación Simétrica de 128 bit con largos de claves de 1.024 bits para Firma Electrónica.
- Tipos de Certificados, tanto para Firma Electrónica Avanzada como Simple

14 Almacenamiento de Certificados

14.1 Almacenamiento en eToken

Los clientes que operen con la firma electrónica de TOC, utilizarán un eTtoken ya que deben disponer estándares de seguridad FIPS 140 nivel 2, para recibir y emitir las claves en forma segura. En caso de que un cliente quiera reutilizar un eToken, TOC debe validar los estándares de seguridad para estos efectos. Este dispositivo permite no exponer la clave privada del suscriptor y lo inhabilita en caso de reiterados intentos fallidos de ingreso de claves.

La administración y su porte serán responsabilidad de quien lo opere, en este caso es el Suscriptor.

14.2 Almacenamiento en Disco Duro

Para el caso de firma electrónica avanzada, el certificado y la clave privada se puede almacenar solo en token, por exigencias de estándares de seguridad no es posible almacenar en disco duro. Para el caso de Firma Electrónica Simple, será posible y admisible la instalación en disco duro.

15 Obligaciones Del Suscriptor

- Según lo establecido en la Ley 19.799 de firma digital, el suscriptor se obliga a almacenar en los dispositivos autorizados por la PSC, generalmente en un dispositivo portable seguro (etoken), en las oficinas de TOC o en las oficinas del Suscriptor.
- Cuando esté instalado el certificado, se debe verificar la correcta instalación en el eToken.
- De igual forma se debe indicar al suscriptor el cambio de PIN de acceso al dispositivo.
-
- El solicitante deberá tener resguardo y en exclusiva responsabilidad de la clave privada y PIN de acceso de uso del eToken.
- Conservar y utilizar correctamente el certificado que le es entregado.

Firma Electrónica

DNI 09337627
Alexander Pascual
De Feudis Kockova
NGJkZjZhOTc7STEwNjg3
2020/07/16 03:44:41 UTC
www.toc.pe