Declaración de prácticas de Certificado

Indice

Control de Cambios

Versón	Fecha	Revisión	Observaciones
1.0	11/11/2015	1.0	Primer Documento

Observaciones	Fechas
Elaborado por: Comité de Seguridad de la Información Consultora de Seguridad de la Información	26/10/2015
Revisado por: Comité de Seguridad de la Información	
Autorizado por: Gerente General TOC S.A.	
Fecha Publicación	
Representante Legal	
Oficial de Seguridad	
Gerente Operaciones/TI	

Introducción

El modelo de TOC para firma electrónica, es de proveer a toda la comunidad servicios de firma electrónica, tanto simple como avanzada, teniendo los estándares que exige cada tipo, con constantes auditorias respecto al uso. Junto con lo anterior TOC proveerá a toda la comunidad de clientes de TOC el apoyo tecnológico suficiente para el apoyo electrónico de potenciación de sus negocios.

Esta certificadora ha considerado todos los aspectos necesarios, esto es, legales, tecnológicos, comerciales y operaciones de un modelo de Confianza entre TOC y la comunidad de clientes. Todo lo anterior cumpliendo e incluyendo todos los requisitos de la ley de firma electrónica, su reglamento asociado a la firma electrónica y el cumplimiento a las guías de acreditación para que la firma electrónica, cumpla todos los requisitos para su legalidad como firma electrónica avanzada.

Para la interacción de TOC con la comunidad de clientes, se ha definido un rol específico para ello, 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 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, que se destina en esta labor.

Objetivo del documento

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

Glosario

Los siguientes son los términos mas utilizados en el presente documento

- ✓ **Claves Publicas y Privadas:** Corresponde a dos secuencias de informadas relacionadas entre sí, para ser utilizadas técnicas de encriptación, usando pares de llaves. Este par de llaves, una se utiliza para encriptar y la otra para desencriptar. 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.
- ✓ **Firma Electrónica Avanzada:** Según la ley de Firma Electrónica que rige en Chile, es aquella que está certificada por un prestador acreditado, que ha sido creado bajo elementos que el autor mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo, permitiendo al detección de cualquier modificación posterior, verificando la identidad del autor.
- ✓ **Hashing:** Son una secuencia de caracteres que representan un documento. Esta secuencia 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 firmo el documento y el documento en sí y que se pueda detectar cualquier cambio posterior.
- ✓ **Subscriptor de un Certificado:** Corresponde a la persona o empresa a la cual se emitió el certificado. Este subscriptor posee una llave pública y otra privada que son utilizadas en cada firma que realice. Según la ley el subscriptor 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:** Es la empresa o institución que llevara el registro electrónico de los Certificados emitidos por la Autoridad de registro. Este registro se realiza encargándose de la detección, comercialización y administración de las solicitudes de todos los tipos de certificados que comercializa TOC S.A.
- ✓ **Usuarios:** El usuario del certificado es la persona que decide usar los certificados emitidos por TOC S.A. y hace uso de ellos.
- ✓ **CRL:** Es un directorio publico donde se informa el estado de los certificados, específicamente los certificados revocados.
- ✓ **CPS:** Corresponde a la Declaración de 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.

Antecedentes

El modelo de Confianza adoptado por TOC se basa principalmente, en implementar una infraestructura de confianza basada en PKI (Public Key Infraestcruture). Esta PKI utiliza tecnología y nomenclatura de llave 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 que 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 TOC.

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

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 empresa pública o privada. Para ello TOC requerirá asegurar la identidad del interesado o suscriptor requiriendo identificar completamente ante la autoridad de registro, con presencia física.

Aplicabilidad

Los certificados emitidos por la Autoridad Certificadora TOC S.A. 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 S.A. podrán ser uso en las siguientes necesidades de seguridad:

Necesidad	Detalle
Autenticación	Debemos dar suficientes garantías respecto a la Identidad del Titular solicitante del certificado. Para esto debemos requerir la presencia física del futuro suscriptor ante la Autoridad de Registro. Junto con la presencia del futuro suscriptor, debemos requerir Solicitud del Certificado, que acrediten su identidad.
No Repudación	Las firmas electrónicas producidas con Certificados emitidos la Entidad de Registro TOC S.A. tiene la evidencia necesaria frente a 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 S.A. 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 S.A., permiten cifrar elementos que solo pueden ser visualizados por el Titular de los datos de Creación de Firma Electrónica

Aplicabilidad Global

Para el desarrollo de negocios de los suscriptores de TOC, en cuanto a firma electrónica, tanto simple como avanzada, resulta muy 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 estará disponible en la TSL, lo que hace confiar inmediatamente y que cada certificado emitido por TOC queda operativo bajo esa raíz, lo que

otorga un reconocimiento inmediato de todas las organizaciones que reconozcan los certificados de clase 2

Rol de TOC frente a los suscriptores

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

- ✓ Administra la 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.
- ✓ Definición 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.
- ✓ Operación de la Autoridad de registros de la prestadora de Servicios de Certificación como lo reconoce la ley de firma electrónica en Chile.
- ✓ Regular las normas y políticas públicas, resguardando la propiedad intelectual y velar con la No utilización de esto sin previo aviso o autorización por TOC.

Requisitos de Integración

Son las especificaciones, requisitos y tareas específicamente en lo tecnológico para que la aplicación o proceso propietario del suscriptor y es quien confía (modelo de confianza) pueda 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 (IExplorer, Firefox y otros).

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

Procedimientos

Para la firma electrónica avanzada, se debe tener muy claro todos los procedimientos adecuados para el otorgamiento del producto. Se describirá el ciclo de vida del procedimiento:

Solicitudes

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

Firma Electrónica

Para el caso de avanzada, se debe tener muy claro todos los pasos necesarios y que se describen en las prácticas de certificación, que incluyen:

- ✓ Debe incluir un proceso de identificación adecuado para estos efectos, y que en términos prácticos, debe incluir, firma de contrato de suscriptor, firma de formulario de entrega de firma electrónica avanzada y fotocopia de Carnet de Identidad.
- ✓ Lo anterior se debe realizar en un acto presencial.
- ✓ Si estuviese disponible, se puede incluir procedimientos adicionales de identificación positiva, como por ejemplo elementos de identificación Biométrica.

Comprobación de Solicitud

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

Los suscriptores de certificados TOC que tengan un certificado válido, están protegidos contra el fraude de identidad cuando ellos lo utilicen utilizando los procedimientos de uso y almacenamiento que TOC tenga disponibles. Los Terceros que es quien confían en un certificado correctamente emitido, también están protegidos contra el fraude de identidad, siguiendo los procedimientos de verificación que TOC establecidos en las prácticas de certificación.

Solicitud Aceptada

Una vez confirmada fehacientemente la identidad, la aceptación de la solicitud es mediante la Entidad de Registro y cumplir con los requisitos del futuro Suscriptor. Se indicará al solicitante vía correo electrónico, la documentación que debe presentar, comprometiéndose que solicitante pague 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 suscriptores 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.

Emisión de Certificados

Una vez que todos los antecedentes del suscriptor 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 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 perdida.
- ✓ 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

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, descrita en las políticas de certificación de TOC.

Condiciones de uso de 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

Verificación de Certificados

Mediante el protocolo OCSP (Online Certificate Status Protocol) toda la comunidad de Suscriptores y de terceros que confían podrá verificar la vlidez y status del certificado emitido por TOC. La comunidad antes mencionada, que no pueda tener acceso en línea a este servicio podrá verificar la validez del certificado por el repositorio de certificados TOC.

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 TOC.

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 no validos se encontraran en la lista de certificados revocados (CRL), las que serán publicadas en el sitio www.toc.cl o pueden ser enviados a terceros que confían.

Existirán otros motivos, diferentes a los de certificado expirado, especialmente los asociados a la que la autoridad determine que es causal de revocación:

- ✓ 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

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 renovará, emitiendo un nuevo certificado de firma electrónica avanzada. La alternativa de renovación está disponible para no generar un registro completo nuevamente del mismo suscriptor.

TOC emitirá certificados con duración de 1 año para todos sus efectos.

Contenido y Estructura de los Certificados

A continuación se detallan las características del contenido 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 avanzada como también firma Simple

Tipos de almacenamiento de Certificados

Almacenamiento en Token

Los clientes que operen con la firma electrónica de TOC, deberán operar con Token ya que deben disponer estándares de seguridad FIPS 140 nivel 2, ara recibir y emitir las claves en forma segura. En caso de que un cliente quiera reutilizar un token, TOC debe validar los estándares de seguridad para estos efectos. Este dispositivo permite nunca exponer la clave privada del suscriptor y lo inhabilita en caso de reiterados intentos fallidos de uso, ingreso de claves.

La administración y soporte será responsabilidad de quien lo opere, en este caso es el Suscriptor.

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.

Obligaciones

El 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 dispositivo portable seguro.
- ✓ Conservar y utilizar correctamente el certificado entregado al Suscriptor.