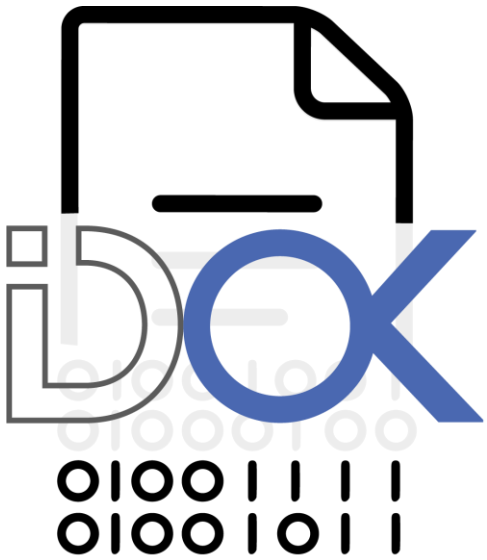

PO02 – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Resumen

Documento conteniendo la Declaración de Prácticas de Certificación de Firma Electrónica Avanzada

1. Introducción

IDOK posee dos instrumentos para gestionar su Autoridad de Registro los cuales son la Declaración de Prácticas de Certificación y la Políticas de Certificación, los cuales se definen a continuación para ayudar en su interpretación.

Política de Certificación (CP) es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos 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, etc.

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.

2. Alcance

El Alcance de la Declaración de Prácticas de Certificación (CPS) detalla las condiciones de los servicios de certificación que presta IDOK para la emisión de sus certificados de Firma Electrónica Avanzada.

3. Referencias y glosario

La presente declaración de Políticas de Certificación se ha generado siguiendo las especificaciones del documento RFC 3647 “Internet X.509 Public Key Infraestrure Certificate Policy and Certification Practices Framework”, y con las siguientes referencias:

- 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.
- NCh2829.Of.2003 Tecnología de la Información – Requisitos de Seguridad para Módulos Criptográficos.
- 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

- **Hashing**: Son una 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.
- **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.
- **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 IDOK.
- **Usuarios:** El usuario del certificado es la persona que decide usar los certificados emitidos por IDOK y hace uso de ellos.
- **CRL**: Listado de certificados revocados.
- **CPS**: Declaración de Prácticas de Certificación.
- **DAS**: Dispositivos de Almacenamiento Seguro.
- **PSC**: Prestador de Servicios de Certificación.
- **OCSP**: Online Certificate Status Protocol, Protocolo de consulta de estado de certificados en línea.

4. Antecedentes

El Modelo de confianza adoptado por IDOK se basa principalmente en implementar una infraestructura de confianza basada en PKI (Public Key Infraestructure), utilizando tecnología de llave pública y privada.
El modelo de confianza se basa principalmente en el tercero que confía (Trusted Third Party), este tercer elemento es la PSC.

5. Aplicabilidad y Comunidad de Usuarios

5.1. Comunidad de Usuarios

IDOK emitirá sus certificados digitales de firma electrónica avanzada en el estándar X.509 y serán emitidos a toda persona física. Para ello se requerirá asegurar la identidad del interesado o suscriptor frente a la autoridad de registro mediante su presencia física.

5.2. Aplicabilidad

Los certificados emitidos por IDOK 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 de la república.
Los certificados emitidos por IDOK podrán ser uso en las siguientes necesidades de seguridad:

5.2.1. Autentificación

Proporciona suficientes garantías respecto a la identidad del suscriptor del certificado, al requerirse la presencia del suscriptor junto con su Cédula Nacional de Identidad y al exigir el almacenamiento de la llave privada en un dispositivo acreditado según norma FIPS-140 nivel 2.

5.2.2. NO REPUDIO

Las firmas electrónicas producidas con certificados emitidos por la de Entidad de Registro IDOK tiene la evidencia necesaria frente a que una persona deniegue la autoría de la firma digital o el contenido firmado digitalmente con el certificado emitido a dicha persona

5.2.3. INTEGRIDAD

La información firmada con un certificado digital emitido por la de Entidad de Registro IDOK permite validar que el elemento firmado no cambia su contenido desde el momento de la firma.

5.2.4. PRIVACIDAD

La información firmada con un certificado digital emitido por la de Entidad de Registro IDOK permiten cifrar elementos que solo pueden ser visualizados por el titular de los datos de creación de firma electrónica.

6. Aplicabilidad Global

IDOK utiliza en la cúspide de su jerarquía un certificado raíz (IDOK ROOT) creado íntegramente en IDOK. Todos los certificados Intermedios quedan firmados por este certificado raíz, en particular el de Firma Electrónica Avanzada, de esta forma se disponibiliza un entorno de confianza global para todos los servicios basados en la PSC.
Este certificado raíz estará disponible tanto en la página web de acceso público psc.idok.cl como en la TSL.

7. Rol frente a los suscriptores

El principal rol de IDOK es realizar todas las tareas, desarrollos y procedimientos orientados a mantener el modelo de confianza definido, correspondiente a las siguientes funciones:

- Administrar la CPS.
- Definición de requisitos y condiciones de aceptación de las Autoridades de Registro, manteniendo el modelo de confianza de IDOK.
- Operación de la Autoridad de Registro como PSC para Firma Electrónica Avanzada.

8. Requisitos de Integración.

Los servicios de certificación de IDOK interactúan de manera nativa con las aplicaciones de uso de firma electrónica, tanto para la acción de firma como la consulta de CRL y OCSP, con los navegadores de uso común.
Los dispositivos de almacenamiento seguro entregados por IDOK disponen del software necesario para interactuar con software de terceros para el uso de parte del suscriptor de los certificados. Este software estará disponible en la página web psc.idok.cl.
Para la opción de integración de soluciones propietarias, se dispone de los protocolos PKCS11 para la implementación en conjunto con el suscriptor, previa evaluación de alcances.

9. Procedimientos

A continuación, se describe el ciclo de vida completo de la emisión de certificados de Firma Electrónica Avanzada IDOK.

9.1. Solicitudes

Todas las solicitudes de emisión deben comenzar con una primera instancia por parte del solicitante, mediante los cuatro canales dispuestos para ello: de forma presencial, mediante correo electrónico a contacto@idok.cl, mediante el formulario web dispuesto en la página psc.idok.cl o mediante servicios de integración en aplicaciones o servicios propios o de terceros autorizados por la PSC.
Independiente del canal, la solicitud debe contener al menos tres datos:

- Rut del futuro suscriptor
- Email del futuro suscriptor
- Nombre Completo del futuro suscriptor

La PSC dará al solicitante las instrucciones para continuar con el procedimiento.

9.2. Firma Electrónica Avanzada

Para firma electrónica avanzada, se considera que la emisión de los certificados debe requerir la presencia física del suscriptor.
En virtud de lo anterior, se incluirá en el proceso de identificación la solicitud de un documento de identificación vigente (Cédula de Identidad, Pasaporte) el que será debidamente registrado.
Adicionalmente se puede solicitar otros mecanismos adicionales, los que pueden incluir evidencia visual de concurrencia, prueba de vida o biométrica, o en general cualquier medio, tecnología o evidencia que se necesite para su correcta identificación.

9.3. Comprobación de Solicitud

De manera interna, IDOK verificará que la evidencia generada en la solicitud de certificado de Firma Electrónica Avanzada sea veraz y exacta, utilizando todos los mecanismos, tecnologías o servicios tanto públicos como privados que tenga a su alcance.

9.4. Solicitud Aceptada

Una vez confirmada la identidad del suscriptor se indicará al suscriptor mediante correo electrónico la documentación que debe presentar, si aplicase, además de los comprobantes del pago del importe correspondiente publicado en la página web psc.idok.cl.
El solicitante deberá presentarse en las oficinas de atención de IDOK, Av. Dardignac 08, piso 4, Providencia, Santiago, en horario de 09:00 a 18:00 horas, en días hábiles, o donde le indique la PSC en el correo de aceptación, para iniciar el proceso de emisión del certificado mediante un oficial de registro capacitado y autorizado por la PSC.

9.5. Solicitud Rechazada

Si la información de suscripción, la documentación solicitada o los requisitos de admisibilidad no son correctos, no concuerden o sean inconsistentes entre sí, se rechazará la solicitud.

9.6. Emisión de Certificados

Una vez aceptada y aprobada la solicitud se generará el certificado de acuerdo con el procedimiento técnico para la emisión de los mismos, cumpliendo con la generación de la clave privada dentro de un dispositivo de almacenamiento seguro, los cuales estarán previamente configurados para proteger su contenido con un PIN de exclusivo conocimiento del suscriptor.

El suscriptor puede delegar la custodia de la clave privada de su certificado en la PSC, la que dispondrá de un DAS tipo HSM que cumpla con los mismos estándares FIPS 140-2 nivel 2 al menos, aplicando mecanismos y procedimientos seguros para la emisión y posterior uso de las claves, los que tendrán las siguientes características:

- Se aplicarán los procedimientos técnicos pertinentes al DAS utilizado para asegurar que la clave privada nunca estará expuesta, generándola en el DAS en modo no exportable y protegiéndola con un PIN de exclusivo dominio del suscriptor.
- Se aplicará un mecanismo de transporte encriptado del PIN del suscriptor mediante claves RSA emitidas dentro del DAS, para la comunicación entre el DAS y la aplicación o servicio de captura del PIN, tanto para su establecimiento como uso posterior.
- El DAS tipo HSM no deberá estar expuesto a la red pública.
- Las aplicaciones o servicios que con posterioridad requieran el uso de la clave privada deberán contar con una autorización del suscriptor mediante su PIN y proveerán a la PSC toda la documentación y evidencia necesaria para la certificación del cumplimiento del procedimiento de su captura y transporte.

El suscriptor con el acto de aceptación del certificado, recepción del token o delegación de custodia y firma del contrato de suscripción se obliga a:

- No revelar la clave privada del certificado, así como el PIN que la protege en el DAS.

- Custodiar el certificado, previniendo su pérdida y uso inadecuado o delegar dicha custodia en la PSC.
- Notificar a IDOK de cualquier compromiso de la clave privada, robo, falsificación o pérdida.
- Devolver el certificado en caso de que IDOK lo solicite.
- Destruir el certificado si no se utiliza.

La duración de los certificados de Firma Electrónica Avanzada será de 1 año.

10. Condiciones de Uso de Certificados de Firma Electrónica Avanzada

Los certificados de Firma Electrónica Avanzada emitidos por IDOK pueden ser utilizados por toda su comunidad de clientes en los lugares y operaciones que el suscriptor estime conveniente y cumpliendo con sus obligaciones como suscriptor.

11. Verificación de Certificados

Mediante el protocolo OCSP toda la comunidad de clientes de IDOK y terceros que confían pueden verificar el estado de los certificados de Firma Electrónica Avanzada emitidos. Las instrucciones de uso estarán publicadas en la página web psc.idok.cl. Los usuarios que no tengan acceso al servicio pueden consultar en un formulario provisto en la misma página web.
La lista de certificados revocados (CRL) se puede utilizar para consultar los certificados que haya revocado la PSC. EL repositorio de esta lista está en la página web psc.idok.cl y se puede consultar dentro de los atributos de los certificados emitidos por IDOK.
La autoridad de Registro directamente indicará costos asociados al servicio de consulta en línea de certificados OCSP, si aplicase.

12. Revocación de Certificados

Los certificados revocados se encuentran en la lista de revocación (CRL), publicadas en la página web psc.idok.cl.
Las causales de revocación de los certificados de Firma Electrónica Avanzada son:

- Solicitud del suscriptor.
- Pérdida del certificado o alteración física del dispositivo token que almacena el certificado.
- Fallecimiento del suscriptor.
- Por alguna eventualidad que comprometa la llave privada del suscriptor.
- Por incumplimiento de suscripción, por parte de la PSC 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 el contrato de suscripción.

13. Expiración de Certificados

Una vez que se cumple la fecha de expiración de los certificados de Firma Electrónica Avanzada emitido por IDOK, quedan automáticamente deshabilitados para su uso. Sin perjuicio de lo anterior, IDOK notificará a los suscriptores cuyos certificados vayan a expirar para ofrecerles la alternativa de renovación del certificado.
Los certificados de Firma Electrónica Avanzada emitidos por IDOK tienen una duración de 1 año.

14. Contenido y Estructura de Certificados

A continuación, se detallan las características del contenido de los certificados de Firma Electrónica Avanzada de IDOK:

- Versión. Deberá ser versión 3.
- Número de Serie. Identificador Único de los certificados emitido por IDOK.
- 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 como número de serie, localidad y país.
- Clave Pública.

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

15. Almacenamiento de Certificados

Dispositivo de Almacenamiento Seguro (e-token)

Los suscriptores que operen con certificados de Firma Electrónica Avanzada emitidos por IDOK, deberán hacerlo utilizando Dispositivos de Almacenamiento Seguro, para emitir la clave privada de forma segura, con procedimientos validados por la PSC. Los DAS deben cumplir con el estándar de seguridad FIPS 140 nivel 2, de tal modo que nunca exponga la clave privada del suscriptor, la que quedará protegida por un PIN; así como su inhabilitación en caso de reiterados intentos fallidos de uso.

HSM

En el caso que el suscriptor ceda la custodia de su clave privada a la PSC en DAS de tipo HSM, el procedimiento debe asegurar que el PIN de acceso a la clave privada sea de exclusivo dominio del titular, mediante mecanismos de transporte de claves encriptadas al momento de la emisión de la misma y en el uso posterior. En cuanto a la no exposición de la clave privada y la inhabilitación en caso de reiterados intentos fallidos de uso (pin incorrecto) aplican los mismos mecanismos y procedimientos.

16. Obligaciones del suscriptor

- El suscriptor se obliga almacenar su certificado en los dispositivos autorizados por la PSC.
- Utilizar el certificado emitido para los fines solicitados, informando de manera oportuna a IDOK 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 el PIN para acceder a ella.
- Verificar y asegurar que la información contenida en el certificado es fidedigna e informar a IDOK de cualquier información incorrecta o inexacta.