2019

e-certchile

CAMARA DE COMERCIO DE SANTIAGO

CERTIFICADOS DE FIRMA ELECTRÓNICA SIMPLE E-CERTCHILE

PRÁCTICAS DE CERTIFICACIÓN ESPECÍFICAS

VERSION: 1.6

COMENTARIOS Y SUGERENCIAS

Invitamos a la comunidad de usuarios de internet a realizar comentarios y sugerencias de cara a futuras revisiones de este documento. Pueden ponerse en contacto a través de la siguiente dirección: oficialdeseguridad@e-certchile.cl o a empresa nacional de certificación electrónica S.A.: Oficial de seguridad de la información, Monjitas 392, piso 17 Santiago de Chile.

PRÁCTICAS DE CERTIFICACIÓN PARA FIRMA ELECTRÓNICA SIMPLE DE E-CERTCHILE

1 CONTENIDO

1. IDENTIFICACIÓN DE LAS PRÁCTICAS DE CERTIFICACIÓN 5

1.1 PRESENTACIÓN 5

1.2 IDENTIFICACIÓN 5

2. COMUNIDAD DE USUARIOS Y APLICABILIDAD 5

2.1. COMUNIDAD DE USUARIOS 5

2.2. DEFINICIONES Y ACRÓNIMOS 5

2.3. APLICABILIDAD 7

2.3.1. AUTENTICACIÓN 7

2.3.2. FIRMA Y NO REPUDIO 7

2.3.3. INTEGRIDAD 7

2.3.4. ENCRIPTACIÓN 7

2.4. USOS AUTORIZADOS 7

3. RECOMENDACIONES TÉCNICAS 8

4. PROCEDIMIENTO 8

4.1. SOLICITUD DE CERTIFICADO 8

4.1.1. REGISTRO INCIAL 8

4.1.2. AUTENTICACIÓN DE LA IDENTIDAD DEL SUSCRIPTOR 9

4.2. ACEPTACIÓN Y RECHAZO DE LA SOLICITUD 10

4.2.1. 4.2.1 ACEPTACIÓN DE LA SOLICITUD 10

4.2.2. 4.2.2 RECHAZO DE LA SOLICITUD 10

4.3. EMISIÓN DE CERTIFICADOS 10

4.4. PROPIEDAD Y OBLIGACIONES 10

4.5. ACEPTACIÓN DEL CERTIFICADO POR PARTE DEL SUSCRIPTOR 11

4.6. PUBLICACIÓN DEL CERTIFICADO 11

4.7. CONTENIDO CERTIFICADO 12

5. JERARQUÍA DE NORMAS 12

1. IDENTIFICACIÓN DE LAS PRÁCTICAS DE CERTIFICACIÓN

1.1 PRESENTACIÓN

El presente documento constituye la Práctica de Certificación específica correspondiente a los Certificados del tipo Firma Electrónica Simple a la cual se hará referencia mediante el acrónimo de su denominación en inglés CP.

La presente CP, junto con el Estatuto de Prácticas de Certificación (CPS) de E-certchile, recogen las políticas que la Empresa Nacional de Certificación Electrónica, actuando como Autoridad de Certificación y Prestador de Servicios de Certificación bajo la marca de E-CERTCHILE, empleará en la entrega del Certificado Firma Electrónica Simple.

1.2 IDENTIFICACIÓN

Esta CP puede localizarse en la siguiente dirección de Internet: http://www.e-certchile.cl/politicas-y-practicas

2. COMUNIDAD DE USUARIOS Y APLICABILIDAD

2.1. COMUNIDAD DE USUARIOS

Los Certificados Firma Electrónica Simple (Certificado) permiten que las personas se identifiquen digitalmente en Internet. Identificando al usuario de forma única y permitiendo su utilización en todas aquellas aplicaciones que precisen autenticación mediante certificados digitales X.509 v3. Adicionalmente, este certificado permitirá firmar, cifrar y garantizar el origen de las transacciones.

El solicitante de este tipo de Certificados podrá ser cualquier persona natural que cumpla con los requisitos establecidos en las presentes Prácticas de Certificación Específica (CP).

2.2. DEFINICIONES Y ACRÓNIMOS

A continuación se procede a entregar una definición formal de los principales conceptos de este documento:

Definiciones

- Autoridad de Registro: Es la entidad que realiza la comprobación de la identidad de los solicitantes para la emisión de certificados.

- Certificado: Certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica.
- Datos de creación de firma: Son los datos únicos del solicitante con los que la PSC crea la firma electrónica (clave privada) y que se encuentran inequívocamente unidos a la clave pública contenida en el certificado de firma electrónica.
- Clave Pública: Parte del certificado electrónico utilizado para verificar la Firma Electrónica por un usuario distinto al suscriptor del mismo certificado.
- Declaración de Prácticas de Certificación: Descripción procedimental y sistémico mediante las cuales la PSC entrega sus certificados.
- Firma electrónica Simple: Es el certificado entregado por la PSC que permite al receptor de un documento electrónico identificar al menos formalmente a su autor.
- Listas de Revocación de Certificados: Registro de acceso público que contiene el detalle los certificados de firma electrónica simple que no tienen vigencia por haber sido revocados.
- OCSP (Online Certificate Status Protocol): Lista disponibilizada por la PSC para comprobar la vigencia de un certificado al momento de su utilización.
- Prestador de Servicios de Certificación (PSC): E-certchile.
- Política de Certificación: Es el conjunto de reglas que indican la aplicabilidad de un certificado, estableciendo las condiciones de uso y los procedimientos para la emisión de los mismos.
- Solicitante: Persona natural que solicita la emisión de un certificado de firma electrónica cumpliendo las exigencias establecidas por la PSC en su CP.
- Suscriptor: Es la persona cuya identidad personal ha quedado vinculada a los datos de un certificado, a través de una clave pública certificada por la PSC.
- X.509: Estándar desarrollado por la UIT, que define el formato electrónico básico para certificados electrónicos.
- Vigencia del certificado: Extensión de tiempo en el cual el certificado está en vigor y observancia.

Acrónimos

- AC: Autoridad Certificadora.
- CP: Prácticas de Certificación.
- CPS: Estatuto de Prácticas de Certificación.
- CRL: Certificate Revocation List.
- ER: Entidad de Registro.
- FIPS: Federal Information Processing Standard.
- LDAP: Protocolo Ligero de Acceso a Directorios, Repositorio de Certificados.
- OCSP: On-line Certificate Status Protocol.
- PKI: Public Key Infrastructure.
- UIT: Unión Internacional de las Telecomunicaciones
- X.509: Estándar desarrollado por la UIT, que define el formato electrónico básico para certificados electrónicos.

2.3. APLICABILIDAD

2.3.1. AUTENTICACIÓN

El suscriptor del Certificado puede autenticar, frente a otra parte, su identidad a través de una red remota de comunicaciones la posesión de la clave privada asociada con la clave pública que se incluye en el Certificado.

2.3.2. FIRMA Y NO REPUDIO

El receptor de un mensaje firmado con el Certificado puede usar la clave pública del emisor para verificar que éste último ha usado su clave privada para firmar el mensaje. El servicio de no repudio permite confirmar frente a un tercero la identidad del emisor del mensaje y la no alteración del mismo.

2.3.3. INTEGRIDAD

El uso de este sistema de claves asimétricas permite comprobar al receptor de un mensaje, que el mismo no ha sido alterado con posterioridad a su suscripción.

2.3.4. ENCRIPTACIÓN

Uso del certificado de firma electrónica para originar un procedimiento que, utilizando sus algoritmos, permite transformar un mensaje sin atender a su estructura lingüística o significado, para hacerlo incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave que permita descifrarlo.

E-CERTCHILE no se hace responsable en ningún caso de la pérdida total o parcial de la información encriptada mediante este tipo de certificado.

2.4. USOS AUTORIZADOS

Se deja constancia de que los certificados no son medios de pago, sino que su finalidad es identificar a una determinada persona en un sistema de redes abiertas o cerradas. No obstante, los certificados regidos por esta PRÁCTICA DE CERTIFICACIÓN pueden ser utilizados en operaciones que importen órdenes de pago o transferencias de dinero.

Estos Certificados no son válidos para asumir responsabilidades económicas ni compromisos en nombre propio y en general no serán válidos para usos diferentes de los descritos en este documento.

No se permite un uso del Certificado contrario a:

2.4.1 La normativa chilena y a los convenios internacionales ratificados por el Estado Chileno.

2.4.2 Lo establecido en la CP, en los Estatutos Prácticas de Certificación entregados por E-CERTCHILE.

Los certificados no podrán ser alterados y deberán utilizarse tal y como son suministrados por E-CERTCHILE.

3. RECOMENDACIONES TÉCNICAS

Para realizar la correcta descarga del certificado el computador del suscriptor debe contar con el siguiente software:

Sistema Operativo:

- Windows XP a Windows 10.

Navegador o Browser:

- Internet Explorer 8 a Internet Explorer 11,
- No es compatible con el navegador de Windows, Microsoft EDGE.

No se garantiza la descarga del Certificado en sistemas operativos o navegadores diferentes a los señalados.

4. PROCEDIMIENTO

Para realizar la correcta descarga del certificado el computador del suscriptor debe contar con el siguiente software:

4.1. SOLICITUD DE CERTIFICADO

4.1.1. REGISTRO INCIAL

El solicitante deberá completar el formulario de solicitud del Certificado que está a su disposición en la dirección de Internet: https://www.e-certchile.cl, junto con acompañar la vigencia del certificado, los datos del solicitante, adjuntar copia firmada de su cédula, además deberá aceptar las condiciones e ingresar los datos para la facturación.

Con el envío del formulario, el Solicitante proporciona a E-CERTCHILE toda la información y documentación que necesite, para registrarlo como Suscriptor e incluirla en el Certificado, de acuerdo con los requisitos establecidos en esta CP.

Si los datos recibidos por la Entidad de Registro no son válidos o suficientes, ésta enviará un e-mail de petición al Solicitante, informando la documentación a aportar y la fecha máxima de recepción de dicha documentación.

Si los datos son correctos el solicitante recibirá un correo, donde se indican los procedimientos que debe llevar a cabo.

Con la Aceptación de la solicitud que se despliega en pantalla el solicitante deberá realizar el pago correspondiente al tipo de Certificado, vía webpay, directamente en la ER, a través de transferencia electrónica o depósito bancario, en estos últimos casos, enviando el comprobante de pago a la ER de manera que, realizada la validación de pago y datos entregados, le informe al Solicitante por e-mail el ID y Password necesarios para generar y descargar el certificado en un computador vía web.

El envío de los datos solicitados en este formulario y el abono de las tasas de registro supondrá su consentimiento para ser registrado como suscriptor de un certificado de E-CERTCHILE. La solicitud de este certificado no implicará en ningún caso su obtención si no se llegan a cumplir por parte del solicitante los requisitos establecidos en la CPS y en las CP de Certificados Firma Electrónica Simple.

La solicitud de un certificado de firma electrónica para fines tributarios a que se refiere esta solicitud es un acto personalísimo y en tal sentido se reconoce que la usurpación de nombre es un delito que se sanciona penalmente por ejercicio ilegal de nombre y/o por estafa y otros engaños. Asimismo, declara que acepta las políticas de certificación de e-certchile.cl y de uso de estos certificados por el Servicio de Impuestos Internos. Revisar en nuestras políticas y prácticas.

4.1.2. AUTENTICACIÓN DE LA IDENTIDAD DEL SUSCRIPTOR

Para acreditar las circunstancias que garantizará el Certificado en la fase definitiva se requerirá la presentación de los siguientes documentos:

- Imagen digital de la cédula de identidad chilena vigente del suscriptor con la imagen de Firma manuscrita del mismo.
- En caso de asistir a las sucursales o entidades de registro, el solicitante debe llevar su cedula de identidad chilena vigente a través de la cual se procede con la identificación, mediante las últimas tecnologías disponibles para estos efectos.

4.2. ACEPTACIÓN Y RECHAZO DE LA SOLICITUD

Una vez recibida la solicitud y la documentación, la ER debe proceder a la aceptación de la misma, previo proceso de verificación de la información proporcionada.

En concreto, la ER confirmará:

a) La información entregada por el solicitante y que figurará en el Certificado.
b) Que se haya entregado la documentación requerida y que ésta se ajuste a lo solicitado.
c) La comprobación de la cédula a través de la serie, vigencia, bloqueo, y otras preguntas personales, se realiza mediante consulta a un bureau de información.
d) Cualquier otra información que se incluye en el Certificado, a no ser que en este se indique expresamente la ausencia de la verificación correspondiente.

4.2.1. 4.2.1 ACEPTACIÓN DE LA SOLICITUD

De no haber circunstancias que de alguna manera afecten a la seguridad del servicio de certificación y siempre que la identidad del solicitante sea válida, la ER procederá a la aprobación de la solicitud.

4.2.2. 4.2.2 RECHAZO DE LA SOLICITUD

Si la ER decidiese rechazar la solicitud del Certificado, comunicará a través de correo electrónico la decisión, con indicación de los motivos que la provocaron. En caso de que los defectos encontrados sean subsanables, se le otorgará al solicitante del certificado un plazo de veinticuatro horas para llevar a cabo la subsanación, transcurrido el cual la ER procederá a confirmar o a revocar su decisión de manera definitiva.

4.3. EMISIÓN DE CERTIFICADOS

Una vez aceptada por la ER la solicitud del Certificado y recibido su pago, la EC emitirá el Certificado, enviando el ID y Password a través del correo electrónico informado en la solicitud. De este modo, el solicitante vía web podrá descargar el certificado adquirido.

4.4. PROPIEDAD Y OBLIGACIONES

El Certificado y su contenido son propiedad de la EC y se emitirá con carácter personal e intransferible a nombre del Suscriptor. El Suscriptor se obliga a:

a) Conservar y utilizar correctamente el Certificado que se le entrega en concepto de depósito.
b) Reportar cualquier dato erróneo en su certificado.
c) No revelar la clave privada del Certificado.

d) Custodiar el Certificado, de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado y garantizar su seguridad así como la del procedimiento para el cual se emiten, especialmente cuidando de no anotar las claves privadas en cualquier otro documento que el suscriptor conserve o transporte, especialmente si existe la posibilidad de que se pierda, se robe o se falsifique al mismo tiempo que aquel.
e) Notificar de inmediato la pérdida, robo o falsificación del Certificado que contiene, así como el conocimiento por otras personas, contra su voluntad, del código de activación o de las claves privadas solicitando la revocación del Certificado de conformidad con el procedimiento que se establece en la CPS.
f) Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado "REVOCACIÓN DE CERTIFICADOS" de la CPS.
g) Devolver el certificado cuando así lo exija la EC en virtud del derecho de propiedad que en todo caso conserva, cuando el Certificado caduque o sea revocado.
h) Destruir el Certificado que quede en desuso o que haya sido sustituido por otro a utilizar con los mismos fines.

La EC se reserva el derecho a negarse a emitir Certificados cuando concurra cualquier causa justificada, por lo que no podrá exigírsele responsabilidad alguna por este motivo.

La EC, se reserva el derecho de realizar validaciones post entrega del certificado a los suscriptores.

4.5. ACEPTACIÓN DEL CERTIFICADO POR PARTE DEL SUSCRIPTOR

La descarga y la aceptación de condiciones implicarán la aceptación del Certificado por parte del Suscriptor.

Aceptando el Certificado, el Suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que de ello se deriven frente a la ER, la EC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

4.6. PUBLICACIÓN DEL CERTIFICADO

Una vez aceptado el Certificado por parte del Suscriptor, la EC procederá a la publicación, en el *Repositorio de Certificados (LDAP),* de los datos del Certificado.

La publicación de los datos del Certificado en el LDAP significa para los terceros usuarios de buena fe, que confíen en el Certificado que ha sido aceptado.

4.7. CONTENIDO CERTIFICADO

Versión x509 v3:

- Versión
- Número de serie
- Algoritmo de firma
- Algoritmo hash de firma
- Emisor del Certificado
  - E = sclientes@e-certchile.cl
  - CN = E-CERTCHILE
  - OU = Autoridad Certificadora
  - O = Empresa Nacional de Certificación Electrónica
  - L = Santiago
  - S = Región Metropolitana
  - C = CL
- Válido desde
- Válido hasta
- Sujeto
- Clave Pública

5. JERARQUÍA DE NORMAS

En todo lo no expresamente previsto por las presentes Prácticas de Certificación (CP) será de aplicación lo señalado en la CPS de E-CERTCHILE.