POLÍTICA CERTIFICADO FIRMA ELECTRÓNICA AVANZADA

e-certchile

CAMARA DE COMERCIO DE SANTIAGO

ÍNDICE

1. Introducción.

Este documento presenta la Política de Certificación (CP) para los certificados de firma electrónica avanzada, la que ha sido generada siguiendo las especificaciones del documento RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" propuesto por Network Working Group para este tipo de documentos.

En ella se describe la forma en que el suscriptor de un certificado de firma electrónica avanzada podrá utilizarlo para autenticarse y/o suscribir electrónicamente un documento. Asimismo, el ciclo de vida del certificado y se describe la aplicación utilizada para generar dicha firma y el tipo de dispositivo o servicio que utilizará para custodiarla y activarla (eToken). Asimismo, la forma en que deberán ser almacenados los datos generados por la misma. Finalmente, señala la forma en que cualquier usuario que recibe una autenticación o documento firmado electrónicamente debe determinar si confiar o no en ésta.

El modelo de confianza que ha implementado e-certchile para promover el comercio y gobierno electrónico seguro se sustenta en la regulación establecida por la Ley 19.799, el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y las normas técnicas dictadas conforme a éstas.

2. Titular del certificado.

Es la persona natural mayor de 18 años que es suscriptora de un certificado de firma electrónica avanzada.

El certificado permite al suscriptor demostrar fehacientemente su nombre completo, RUT y correo electrónico, posibilitando, asimismo, su uso para suscribir documentos electrónicos o recibir documentación cifrada para él con su clave público.

El régimen de responsabilidades de éste se encuentran detalladamente establecidas en las Prácticas de Certificación e-certchile (CPS e-certchile), siendo especialmente importante relevar que el certificado es personal e intransferible, que todo acto generado por el mismo

será considerado como propio aunque el mismo haya sido realizado por otra persona a la cual le ha entregado el acceso a los datos de creación de firma y que si bajo cualquier circunstancia considera que los datos de creación de firma han sido vulnerados debe solicitar sin delación la revocación del certificado.

3. Obligaciones.

3.1. e-certchile.

Se obliga a:

a. Ofrecer y mantener instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos establecidos en la Ley 19.799, el Decreto supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y las normas técnicas conforme a éste.

b. Cumplir y respetar los procedimientos establecidos en las Práctica de Certificación e-certchile (CPS e-certchile) y en esta Práctica de Certificados (CP) para la emisión de certificados.

c. Cumplir con todas las otras obligaciones establecidas en la Ley 19.799, el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo y las normas técnicas dictadas conforme a éste.

d. Comprobar fehacientemente la identidad del solicitante, a través de la comparecencia personal y directa de éste ante e-certchile.

e. Aprobar o rechazar las solicitudes de certificados, directamente o a través de las autoridades de registro, de conformidad con la Práctica de Certificación e-certchile (CPS e-certchile).

f. Emitir los certificados en conformidad al procedimiento establecido en la Prácticas de Certificación e-certchile (CPS e-certchile).

g. Comunicar al suscriptor de la emisión de su certificado.

h. Proveer al suscriptor del dispositivo de custodia de los datos de creación de firma (e-Token).

i. Configurar y mantener un Registro de Acceso Público de Certificados, con expresa indicación del estado de éstos (vigente, suspendido o revocado).

j. Revocar y/o suspender los certificados, notificando de ello al suscriptor.

k. Realizar razonables esfuerzos para comunicar a los suscriptores cualquier hecho conocido por e-certchile que pudiera afectar la validez del certificado.

l. Delegar la función de autoridad de registro en entidades de su confianza, asumiendo la responsabilidad por su cometido en el desarrollo de dicha función.

m. Publicar y difundir esta Política.

n. Mantener www.e-certchile.cl con información para el público sobre los servicios de e-certchile.

3.2. Autoridad de Registro.

Se obliga a:

a. Comprobar la identidad del solicitante de un certificado de conformidad al procedimiento establecido en la Práctica de Certificación e-certchile (CPS e-certchile) y en la forma señalada en esta Prácticas de Certificado (CP).

b. Registrar y custodiar por 6 años los antecedentes, requeridos a los solicitantes, que sirvieron de base para la emisión de los certificados.

c. Aprobar o rechazar las solicitudes de emisión de certificados.

d. Recibir las solicitudes de revocación o suspensión de certificados e informarlas a e-certchile.

e. Obtener la aceptación en forma inequívoca de los términos y condiciones del servicio por parte del solicitante.

f. Permitir operar solamente certificados que hayan sido aceptados por el solicitante.

g. Prestar cualquier otro servicio que e-certchile le solicite.

Todas las actuaciones indicadas en las letras anteriores, las realiza la Autoridad de Registro por cuenta y riesgo de e-certchile.

3.3. Suscriptor.

Antes de la emisión del certificado se obliga a:

a. Ser persona natural mayor de 18 años.

b. Solicitar la emisión del certificado aceptando los términos y condiciones descritos en las "CPS e-certchile" y esta Política de Certificados (CP).

c. Comparecer personal y directamente ante e-certchile o sus autoridades de registro a solicitar el certificado, presentando su cédula de identidad y una representación impresa de la misma.

d. Proveer a e-certchile y/o la autoridad de registro toda la información que de acuerdo con esta Política de Certificados (CP) es requerida para verificar su identidad.

e. Crear y descargar el certificado en un dispositivo de almacenamiento al que se tenga acceso y control.

f. Pagar las tarifas convenidas por concepto de los servicios de certificación, aun cuando no se acepten o no se ocupen los certificados emitidos.

Una vez emitido el certificado se obliga a:

a. Aceptar el certificado. Se entiende que un certificado es aceptado por el suscriptor cuando:

i) Haya sido emitido por e-certchile, aun cuando el certificado no haya entrado en vigor por contener una fecha de inicio de operación posterior a su fecha de emisión.

ii) No se haya formulado un reclamo por error o inexactitud en la emisión al momento de su recepción.

iii) Se haya utilizado la clave de confirmación comunicada por e-certchile para retirar el certificado, se haya instalado éste en el dispositivo de generación y almacenamiento de firma o haya sido utilizado por el suscriptor.

b. Comunicar a e-certchile cualquier error o inexactitud en el certificado que reciba. Si no lo hace al momento de su recepción todas las declaraciones se tendrán por verdaderas.

c. Usar los datos de creación de firma asociados al certificado para fines legales y autorizados, de conformidad con lo previsto en la Ley 19.799, la Prácticas de Certificación e-certchile (CPS e-certchile) y en esta Práctica de Certificado (CP).

d. Utilizar correctamente el certificado.

e. Ser un usuario final y no usar el certificado para actuar como certificadora de firma electrónica.

f. Comunicar inmediatamente a e-certchile y/o a una autoridad de registro el compromiso, pérdida, hurto, robo, acceso no autorizado o extravío, falsificación de sus datos de creación de firma o certificado o cualquier circunstancia que pudiera ser causal de suspensión o revocación de un Certificado.

g. Custodiar los datos de creación de firma, tomando precauciones razonables para evitar su pérdida, modificación y uso no autorizado.

h. No revelar los mecanismos de protección de los dispositivos en que se almacenen los datos de creación de firma (eToken).

i. Solicitar la suspensión o revocación del certificado cuando se presente alguna de las causales indicadas para este efecto.

j. No usar los datos de creación de firma una vez que el certificado haya expirado o haya sido solicitada la suspensión o revocación.

k. Destruir los datos de creación de firma en caso que e-certchile así se lo solicite y haya sido revocado previamente el certificado.

3.4. Usuarios.

Se obliga a:

a. Verificar la validez del certificado mediante una consulta al registro de acceso público de certificados.

b. Verificar la firma del suscriptor.

c. Comprobar cualquier limitación funcional que incorpore el certificado.

d. Validar el uso de certificado para propósitos autorizados de conformidad con la legislación vigente.

4. Responsabilidades.

4.1. e-certchile.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

4.2. Limitación de responsabilidad.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

4.3. Autoridad de Registro.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

4.4. Suscriptor.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

4.5. Usuario.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

5. Ciclo de vida del Certificado.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

6. Identificación y autenticación.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile), con todo se previene que los certificados de firma electrónica avanzada se emiten una vez que e-certchile o una de sus autoridades de registro han comprobado fehacientemente la identidad del solicitante.

Cuando el solicitante del certificado comparezca en forma personal y directa a las oficinas de e-certchile o de la autoridad de registro se comprueba la identidad a través de un pareo entre la información biométrica de la cédula de identidad del solicitante y la huella digital de éste, verificándose que la cédula de identidad no se encuentre bloqueada ante el Registro Civil y que la persona no figure en el Registro de Defunciones.

7. Usos del Certificado.

7.1. Composición del certificado.

e-certchile tiene en operación dos CA Root que cumple con los requisitos exigidos por la Ley 19.799 y el Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Turismo, así como, por las normas técnicas dictadas conforme a éste. Una CA Root opera para los certificados de firma electrónica avanzada SHA1 y la otra para aquellos que se emiten bajo SHA2.

Certificado tipo firma electrónica avanzada de e-certchile SHA1.

Nombre	Descripción	Tipo Dato	Valor
Versión	Versión del certificado que deberá ser versión 3.	Fijo	V3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los certificados de firma electrónica avanzada emitidos por e-certchile.	Variable	123abc00000000123abc
Algoritmo de firma	Algoritmo usado por e-certchile para firmar el certificado	Fijo	SHA1RSA
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = email del Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor	Variable	E = sclientes@e-certchile.cl CN = E-CERTCHILE CA FIRMA ELECTRONICA AVANZADA OU = Autoridad Certificadora O = E-CERTCHILE L = Santiago S = Region Metropolitana C = CL
Período de Validez	Fecha de inicio y termino en que es válido el certificado.	Variable	Dayname, Month day, year hh:m:ss PM/AM
Nombre del Titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500.	Variable	E = correo electrónico del suscriptor CN = nombres apellido1 apellido2 OU = unidad organizacional O = Nombre de la empresa L = Localidad S = Región C = País CL
Clave pública	Clave pública del titular del certificado	Variable	RSA (2048 Bits)

Nombre	Descripción	Tipo Dato	Valor
KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	Fijo	Digital Signature
BasicConstrains	Permite diferenciar entre un certificado de PSC y uno de suscriptor final.	Fijo	Subject Type=End Entity Path Length Constraint=None
ExtendedKeyUsage	Esta extensión define una serie de propósitos respecto al uso del certificado, adicionalmente a las definidas en KeyUsage. El certificado debe ser utilizado sólo para los propósitos definido por esta extensión.	Fijo	N/A.
AuthorityKeyIdentifier	Medio para identificar la llave pública de e-certchile El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier.	Fijo	KeyID=3710 CADF FD46 2285 C9E8 9EE6 1DD8 9CEF 00B6 AE50
CertificatePolicy	Ver Política de Certificados	Fijo	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.8658.5 1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.e-certchile.cl/html/CPS.htm 1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de

Nombre	Descripción	Tipo Dato	Valor
			usuario Certificador: Texto de aviso=Certificado emitido para Firma Electronica Avanzada. PSC acreditado por Resolucion Administrativa Exenta Nro. 317 del 14 de agosto del 2003 de la Subsecretaria de Economia.
IssuerAltName	Identificador alternativo del emisor, corresponde al RUT.	Fijo	RUT de EC emisora, OID: 1.3.6.1.4.1.8321.2
SubjectAltName	Permite definir términos que identifican al sujeto o titular del certificado, adicionalmente a lo establecido en el campo estándar Subject.	Variable	Rut del suscriptor, OID: 1.3.6.1.4.1.8321.1
CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la siguiente. estructura: DistribuitonPoint: Un URI para identificar el CRL.	Fijo	URL=http://crl.E-CERTCHILE.cl/ecertchilecaFEA.crl
Algoritmo de identificación		Fijo	SHA1
Huella digital		Variable	65643bfa17be169c983713e8a3cb302d3eb1b6db

Certificado tipo firma electrónica avanzada de e-certchile SHA2.

Nombre	Descripción	Tipo Dato	Valor
Versión	Versión del certificado que deberá ser versión 3.	Fijo	V3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los certificados de firma electrónica avanzada emitidos por e-certchile.	Variable	1200000a12a123a123a12a123a000100000a12
Algoritmo de firma	Algoritmo usado por e-certchile para firmar el certificado	Fijo	sha256RSA
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = email del Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor	Variable	E = sclientes@e-certchile.cl CN = E-CERTCHILE CA FEA 02 OU = Autoridad Certificadora O = E-CERTCHILE L = Santiago S = Region Metropolitana C = CL
Período de Validez	Fecha de inicio y termino en que es válido el certificado.	Variable	Nombre Dia, dia, mes, año hh:m:ss
Nombre del Titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500.	Variable	E = correo electrónico del suscriptor CN = nombres apellido1 apellido2 OU = unidad organizacional O = Nombre de la empresa L = Localidad S = Región C = País CL
Clave pública	Clave pública del titular del certificado	Variable	RSA (2048 Bits)

Nombre	Descripción	Tipo Dato	Valor
KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	Fijo	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (f0)
BasicConstrains	Permite diferenciar entre un certificado de PSC y uno de suscriptor final.	Fijo	PSC: Tipo de asunto=Entidad de certificación (CA) Restricción de longitud de ruta=Ninguno Suscriptor Final: N/A
ExtendedKeyUsage	Esta extensión define una serie de propósitos respecto al uso del certificado, adicionalmente a las definidas en KeyUsage. El certificado debe ser utilizado sólo para los propósitos definido por esta extensión.	Fijo	N/A.
AuthorityKeyIdentifier	Medio para identificar la llave pública de e-certchile El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier .	Fijo	Id. de clave=a1ec749252db286c502040f709612f355656c798
CertificatePolicy	Ver Política de Certificados	Fijo	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.8658.5 1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: http://www.e-certchile.cl/html/CPS.htm 1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado emitido para Firma

Nombre	Descripción	Tipo Dato	Valor
			Electronica Avanzada. PSC acreditado por Resolucion Administrativa Exenta Nro. 317 del 14 de agosto del 2003 de la Subsecretaria de Economia.
IssuerAltName	Identificador alternativo del emisor, corresponde al RUT.	Fijo	Rut de EC emisora, 1.3.6.1.4.1.8321.2=16 0a 39 36 39 32 38 31 38 30 2d 35
SubjectAltName	Permite definir términos que identifican al sujeto o titular del certificado, adicionalmente a lo establecido en el campo estándar Subject.	Variable	Rut del suscriptor, 1.3.6.1.4.1.8321.1=16 0a 31 35 36 31 39 36 33 37 2d 31
CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la siguiente. estructura: DistribuitonPoint: Un URI para identificar el CRL.	Fijo	URL=http://crl.ecertchile.cl/E-CERTCHILE CA FEA 02(1).crl (http://crl.ecertchile.cl/E-CERTCHILE%20CA%20FEA%2002(1).crl)
Acceso a la información de la entidad emisora	Protocolo de estasdo de certificado en línea	Fijo	URL= http://ocsps2.ecertchile.cl/ocsp
Algoritmo de identificación		Fijo	SHA2
Huella digital		Variable	581a52623bf1b4e74db6e97a7b6dd4977d04e182

8. Aplicación de Firma.

La aplicación que el suscriptor utilice para firmar electrónicamente un documento es de su responsabilidad, sin embargo, le sugerimos que tenga especial preocupación que aquella que elija garantice que los datos de creación de firma nunca queden expuestos a terceros usuarios o aplicaciones.

8.1. Efectos.

De conformidad con lo dispuesto en la Ley 19.799 los actos y contratos suscritos por medio de firma electrónica serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel.

Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.

Finalmente, es importante que el suscriptor y el usuario tengan presente que los instrumentos privados suscritos con firma electrónica avanzada tienen un valor probatorio privilegiado según lo dispuesto en el artículo 5º de la Ley 19.799 ya que hacen plena prueba al igual que los instrumentos públicos.

9. Usuario.

El usuario es aquella persona que voluntaria y libremente decide hacer uso y/o confiar en un certificado de firma electrónica avanzada emitido por e-certchile.

Por lo tanto, el usuario es responsable de validar el contenido del documento, la firma y el certificado asociado a dicha firma con anterioridad a tomar la decisión de confiar en él.

e-certchile a través de tecnologías y procedimientos que dispone, permite asegurar la identidad del suscriptor de un certificado para firma electrónica y las acciones que efectúe con él.

10. Verificación de Firma.

La verificación de la firma electrónica avanzada de un documento electrónico se realiza para determinar que:

a. La firma electrónica fue creada por los datos de creación de firma correspondiente a la clave pública contenida en el certificado del suscriptor que firma.
b. El mensaje no ha sido modificado con posterioridad a su suscripción.

10.1. Efecto de validar al suscriptor.

La firma electrónica avanzada genera efectos jurídicos para el que la incorpora a través de sus datos de creación de firma en un documento electrónico, siempre y cuando:

a. Haya sido creada durante el período de vigencia del certificado.
b. La firma electrónica avanzada pueda ser verificada por medio de la cadena de verificación.
c. El usuario no tiene conocimiento del incumplimiento de la Práctica de Certificación e-certchile (CPS e-certchile) por parte del suscriptor
d. El usuario ha cumplido con todos los requisitos de la Práctica de Certificación e-certchile (CPS e-certchile).

10.2. Responsabilidad por no validar una firma.

Un usuario que confía en una firma electrónica avanzada que no ha sido verificada en forma total, por cualquier razón, asume todos los riesgos y no puede hacer ninguna presunción de que la firma es válida bajo los términos de la Práctica de Certificación e-certchile (CPS e-certchile).

10.3. Confianza en la firma electrónica.

Un usuario sólo puede confiar en la firma electrónica avanzada con que se ha suscrito un documento electrónico en la medida que:

a. La firma electrónica haya sido creada durante el período de vigencia del certificado.

b. La confianza es razonable de acuerdo con las circunstancias.

La decisión de confiar o no en una determinada firma electrónica avanzada la toma en forma libre y exclusiva el usuario que realiza la verificación.

10.4. Almacenamiento de antecedentes.

Para efectos de disponer de los adecuados antecedentes para una verificación posterior de la firma electrónica, el usuario debe mantener los siguientes antecedentes:

- Documento que se firmó electrónicamente.
- Firma Electrónica.
- Certificado del suscriptor o en su defecto alguna identificación que permita buscar posteriormente el certificado en el registro de acceso público de e-certchile.

11. Instalaciones, gestión y controles operacionales.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

12. Controles técnicos de seguridad.

De acuerdo con lo especificado en la Práctica de Certificación e-certchile (CPS e-certchile).

NORMA(S) QUE APLICA(N)	
Norma	**Referencia Normativa**
ISO 9001:2015	5.2 Política | 8.2.2 Determinación de los requisitos relacionados con los productos y servicios **(SGI-PO-06)**
ISO 27001:2013	5.2 Política
Guía de Acreditación (Minecon) FEA	PO01 Política de Certificados de Firma Avanzada
Guía de Acreditación (Minecon) BIO	N/A
Guía de Acreditación (Minecon) TSA	N/A

CONTROL DE CAMBIOS		
N° DE VERSIÓN	**FECHA**	**DESCRIPCIÓN DE CAMBIOS**
0	2020/07	Creación del documento, se recomiendo la lectura completa del documento