2019

e-certchile

CAMARA DE COMERCIO DE SANTIAGO

Certificados de Firma Electrónica Avanzada

POLÍTICA DE CERTIFICACIÓN

VERSION: 2.4

Política de certificación para los certificados personales de firma electrónica avanzada de e-certchile

IDENTIFICACIÓN DE LA POLITICA DE CERTIFICACIÓN

ÍNDICE

1 IDENTIFICACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

1.1 PRESENTACIÓN

El presente documento constituye la Política de Certificación correspondiente a los Certificados de FIRMA ELECTRÓNICA AVANZADA, a la cual se hará referencia mediante el acrónimo de su denominación en inglés CP.

1.2 IDENTIFICACIÓN

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

2 COMUNIDAD DE USUARIO Y APLICABILIDAD

2.1 COMUNIDAD DE USUARIOS

Los Certificados de FIRMA ELECTRÓNICA AVANZADA permiten que las personas puedan firmar digitalmente transacciones y documentación electrónicas. Identifica al usuario de forma única y podrá utilizarse en aquellas aplicaciones que precisen firma digital mediante certificados digitales X.509 v3 emitidos bajo la Política FIRMA ELECTRÓNICA AVANZADA. Este certificado permitirá sólo firmar de acuerdo a lo establecido en la ley 19.799 y su reglamento.

2.2 APLICABILIDAD

2.2.1 Firma y No Repudio

El receptor de un mensaje firmado con el Certificado puede usar la clave pública del emisor para verificar que este 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. El mensaje firmado puede corresponder a una transacción y documento electrónico con validez legal según las normativas vigentes que dicen relación con la firma digital, como la ley 19.799.

2.2.2 Integridad

El uso de este sistema de claves asimétricas permite comprobar al receptor de un mensaje que el mismo no ha sido alterado entre el envío y la recepción.

2.3 DETALLES DE CONTACTO.

Atención.: Solicitud Clientes

E-CERTCHILE
Monjitas 392 Piso
17

Santiago de Chile

E-mail: sclientes@e-certchile.cl

Teléfono: (+56 2) 2360 7175

Mesa ayuda certificación: (+56 2) 2818 5760

- Casa Matriz Monjitas 392, piso 17. Santiago: Lunes a Jueves: 09:00 - 17:30 hrs. Viernes: 09:00 - 14:30 hrs.
- Sucursal Enrique Mac-Iver 410, Santiago: Lunes a Jueves: 09:00 – 17:30 hrs. Viernes 09:00 – 14:30 hrs.
- Sucursal Av. Nueva Providencia 2260, Local 81, Providencia: Lunes a Jueves: 09:00 – 17:30 hrs. Viernes 09:00 – 14:30 hrs.

2.4 USOS NO AUTORIZADOS

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

Estos certificados son válidos para asumir las responsabilidades económicas y compromisos en nombre propio permitidos por la Ley 19.799 de Firma Digital y en general serán válidos para los usos descritos en este documento.

No se permite un uso del Certificado contrario a:

- La normativa chilena y a los convenios internacionales ratificados por el Estado Chileno.
- Lo establecido en la CPS, en la Política de Certificación y en los contratos que se firmen entre la EC (Entidad de Certificación) / ER (Entidad de Registro) y el Suscriptor.

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

3 RECOMENDACIONES TÉCNICAS

Se recomienda el uso de navegadores de última generación compatibles con los protocolos, S/MIME y http con SSL (v2 y v3).

No se garantiza el correcto funcionamiento del Certificado en combinación con aplicaciones que no hayan sido previamente validadas por E-CERTCHILE.

4 PROCEDIMIENTO

4.1 SOLICITUD DE CERTIFICADO

4.1.1 Registro Inicial

El solicitante deberá llenar y enviar el formulario de solicitud del Certificado que estará a su disposición en la dirección de Internet: **http://www.e-certchile.cl** El envío de los datos solicitados en este formulario supondrá su consentimiento para ser registrado como solicitante de un Certificado E-CERTCHILE de FIRMA ELECTRÓNICA AVANZADA. La solicitud de este certificado no implicará en ningún caso su obtención si no se llegan a cumplir por parte del solicitante las cláusulas y condiciones establecidos en la CPS, en la Política de Certificación para los Certificados de FIRMA ELECTRÓNICA AVANZADA y en el Contrato el Suscriptor con la EC.

- Asimismo, con el envío del formulario, el solicitante se compromete a comparecer personalmente ante la ER y proporcionar a ésta toda la información que necesite, bien para registrar al solicitante como suscriptor, o con la finalidad de incluirla en el Certificado, de acuerdo con los requisitos establecidos en esta CP.

4.1.2 Autenticación de la Identidad del Suscriptor

Para acreditar las circunstancias que garantizará el Certificado, se requerirá la presentación ante la ER del suscriptor, además del original y copia para su revisión ocular, de los siguientes documentos:

- RUT del Suscriptor.
- Solicitud de FEA impresa (correo electrónico enviado como aprobación de solicitud).

- Para el caso de los Notarios, Conservadores y Archiveros Judiciales titulares, suplentes e interinos, debe presentar certificación de la condición de tales emitidas por el Secretario de la Corte de Apelaciones respectiva, o quien lo reemplace que será validado por la ER.

4.2 COMPROBACIÓN DE LAS SOLICITUDES DE CERTIFICADOS

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

En concreto, la ER confirmará:

a) En caso de dudas se realizará validación telefónica de la solicitud (al número de teléfono especificado en el formulario de ingreso de solicitud), para corroborar la veracidad de ésta. Producto de esta confirmación se cambiará el estado de la solicitud a "Solicitud Aceptada".

Casos de excepción:

- De no haber respuesta telefónica, se enviará un correo electrónico para tal fin.
- De no obtener respuesta confirmatoria, transcurridos 15 días desde la fecha de recepción de la solicitud, ésta será eliminada y se informará acerca de la eliminación a la dirección de correo electrónico entregada por el solicitante.

b) Verificación de Cédula de Identidad y domicilio mediante un servicio externo utilizando la plataforma de Equifax.

Casos de Excepción:

- En caso de no coincidir alguno de los datos se contactará al cliente para rectificar la información.
- En caso de tener problemas nuevamente con la confirmación de los datos se contactará al cliente, se le explicara el problema y se procederá a eliminar la solicitud.

4.3 ACEPTACIÓN DE LA SOLICITUD

Una vez superado el proceso de comprobación de solicitud de forma satisfactoria, siempre y cuando no existan circunstancias que de alguna manera afecten a la seguridad del servicio de certificación, la ER procederá a la aprobación de la solicitud. Se indicará al solicitante, vía email, la documentación a presentar y la fecha máxima de recepción de dicha documentación para realizar el cotejo de la identidad y de los atributos del certificado. Junto con presentar la documentación, el solicitante se

compromete a cancelar el importe correspondiente al tipo de Certificado que está requiriendo.

el solicitante deberá presentarse en Monjitas 392 piso 17, Edificio de la Cámara de Comercio de Santiago, entre las 09:00 hrs. y las 17:30 horas sólo en días hábiles.

4.4 RECHAZO DE LA SOLICITUD

Si la ER decidiese rechazar la solicitud del Certificado, comunicará por escrito al solicitante dicha decisión. En caso de que los defectos encontrados sean subsanables, se le otorgará al solicitante del Certificado un plazo de quince días para llevar acabo la corrección, de no haber rectificación a lo objetado por la ER, se procederá a confirmar el rechazo por escrito.

4.5 EMISIÓN DE CERTIFICADOS

Una vez aceptada por la ER la Solicitud del Certificado, se llevará a cabo el registro del solicitante.

Prerrequisitos

- Entrega de la documentación requerida y que ésta sea correcta
- Cédula de Identidad (Fotocopiada por ambos lados).
- Solicitud de FEA impresa (correo electrónico enviado como aprobación de solicitud).
- Para el caso de los Notarios, Conservadores y Archiveros Judiciales titulares, Suplentes e interinos, debe presentar certificación de la condición de tales emitidas por el Secretario de la Corte de Apelaciones respectiva, o quien lo reemplace que será validado por la ER.

4.5.1 Casos de Excepción:

En el caso que el suscriptor no cumpla con algún requerimiento, se solicitará que provea dicho requisito en el momento (ya sea por mano o le sea enviado por correo electrónico), de no poder cumplir con esto se solicitará al suscriptor que vuelva posteriormente con toda la documentación requerida para continuar con el proceso. Se definirá un plazo de 15 días, como máximo, para cumplir con lo requerido.

4.5.2 Entrega:

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

a) El operador ER, deberá registrar y validar con el sistema biométrico, acordado y disponible, que asegura que los datos de creación de firma se mantienen bajo el exclusivo control del titular del certificado (en caso de falla de la validación Biométrica se realiza validación Manual). El operador ER, tomará fotografía digital al suscriptor la que se adjuntará al formulario de enrolamiento a completarse por el suscriptor.
b) El Operador ER entregará al suscriptor el formulario de enrolamiento en 2 copias, en ambas deberá estampar su huella dactilar y su firma, quedando una copia en poder del cliente y otra en poder de E-certchile. Este formulario será almacenado físicamente en una bóveda bancaria, el respaldo digital del mismo será guardado en un directorio de acceso restringido y respaldado semanalmente.
c) El operador ER, deberá entregar al suscriptor el contrato de aceptación del servicio de certificación.
d) El Operador ER, generará y entregará las claves para descargar el certificado dentro de un sobre sellado.
e) Por último, se debe registrar en el sistema de inventario interno, la salida del dispositivo portable seguro, registrando el número de serie de cada elemento y la información del suscriptor.

Caso de excepción:

Si se efectúa exitosamente el registro del suscriptor, pero por algún motivo, no es posible emitir el certificado de forma inmediata, se entregará los dispositivos necesario para que personalmente obtenga su certificado, desde sus instalaciones, en un plazo no superior a 15 días de efectuado el registro.

El Suscriptor se obliga a:

a) Descargar y almacenar el certificado en los dispositivos autorizados por la EC y que han sido validados por esta, de acuerdo a lo establecido en la Ley 19.799 de Firma Digital. La descarga y almacenamiento del certificado será realizada por el suscriptor (asesorado por el operador ER), en un dispositivo portable seguro (e-token), en las dependencias de E-certchile o en las oficinas del suscriptor. Una vez bajado el certificado, se debe proceder a verificar la correcta instalación de éste en el e-token, asimismo se debe indicar al suscriptor el cambio del PIN del dispositivo, este dispositivo permite firmar internamente el documento sin dejar jamás disponible la clave privada del titular.
b) El dispositivo portable seguro cuenta con un mecanismo que lo inhabilita en caso de reiterados intentos fallidos de acceso.

c) El solicitante declarará formalmente que el uso de la clave privada correspondiente a su certificado y el conocimiento del PIN de acceso al dispositivo portable seguro (tarjeta inteligente o e-token), serán su responsabilidad.
d) Conservar y utilizar correctamente el Certificado que se le entrega en concepto de depósito.
e) No revelar la clave privada de seguridad del dispositivo en donde se encuentra almacenado el Certificado.
f) Custodiar el Certificado, de forma diligente, tomando las precauciones razonables para evitar su perdida, revelación, modificación o uso no autorizado y garantizar su seguridad así como la del procedimiento para el cual se emiten, especialmente cuidando de no divulgar las claves privadas en cualquier otro documento que el Suscriptor conserve o transporte, especialmente si existe la posibilidad de extravío, hurto o sustracción indebida.
g) 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 en conformidad con el procedimiento que se establece en la CPS.
h) Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado "REVOCACIÓN DE CERTIFICADOS" de la CPS.
i) 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.
j) Destruir o borrar 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.

4.6 ACEPTACIÓN DEL CERTIFICADO POR PARTE DEL SUSCRIPTOR

La entrega del Certificado, la firma, estampado de huella dactilar en Formulario de Enrolamiento y la firma contrato de adhesión al sistema de Certificación implicará la aceptación del Certificado por parte del suscriptor.

La aceptación del Certificado deberá realizarse de forma expresa, por escrito y ante el encargado de la ER.

En caso de ser requerido el suscriptor deberá firmar original y copia del contrato, estableciendo su total aceptación al servicio de certificación que se le ha otorgado. La copia del contrato perteneciente al suscriptor será despachada por correo certificado a su domicilio.

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

4.7 PUBLICACIÓN DEL CERTIFICADO

Una vez aceptado el Certificado por parte del suscriptor, la EC procederá a la publicación, en el *Registro de Acceso Público.*

La publicación de los datos del Certificado en el *Registro de Acceso Público* significa que ha sido aceptado para los terceros usuarios de buena fe, que confíen en el Certificado Contenido del Certificado versión x509 v.

Perfil de Certificado de la Política de FIRMA ELECTRÓNICA AVANZADA

Certificate: Data:
Version: 3 (0x2)
Serial Number: 3f:b7:99:ec:00:00:00:00:01:3b
Signature Algorithm: Sha2WithRSAEncryption
Issuer:
emailAddress = sclientes@e-certchile.cl
commonName = E-CERTCHILE CA FIRMA ELECTRONICA AVANZADA
organizationalUnitName = Autoridad Certificadora
organizationName = E-CERTCHILE
localityName = Santiago
stateOrProvinceName = Region Metropolitana
countryName = CL
Validity
Not Before: Ene 26 15:04:58 2019 GMT
Not After : Ene 25 15:04:58 2022 GMT
Subject:
emailAddress = pperez@e-certchile.cl
commonName = Priscila Perez Vega
organizationalUnitName = Certificacion Electronica
organizationName = Nacional de Certificacion Electronica
localityName = Santiago
stateOrProvinceName = Metropolitana
countryName = CL
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)

Modulus (2048 bit):
00:ab:7c:1b:64:1f:c2:e4:f8:30:1e:42:43:f3:46:18:2f:18:41:76:c
2:07:ae:00:90:52:21:9f:b4:f3:92:cb:f7:e4:5d:92:ce:f2:ba:b5:ff:
4d:7:97:c4:f6:81:54:fc:d4:38:e6:14:b4:03:31:36:c2:a3:37:bc:80
:9d:4d:4c:d7:cc:60:e9:35:30:d4:6a:f9:d2:3e:4b:7c:85:6e:5f:d:c
d:32:89:2d:4e:76:1a:78:53:48:77:ca:19:0c:5e:97:a0:53:82:c8:8
0:0c:d0:63:8b:24:94:52:6f:8d:2a:f1:12:5d:b7:13:2d:af:27:4e:1
b:05:d2:d1:3d:3c:f1
Exponent: 65537(0x10001) X509v3
extensions: X509v3
Key Usage: Digital Signature, Non Repudiation, Key Encipherment Encipherment X509v3
Subject Key Identifier:
81:7A:9D:27:B9:12:0B:8D:05:51:E1:8A:5F:D4:A1:EE:7D:D8:AA:43
X509v3 Authority Key Identifier:
keyid:CC:49:F6:95:58:78:16:74:4B:87:4F:87:02:1E:1B:A5:7B:77:AC:03
X509v3 CRL Distribution Points:
URI:http://crl.e-certchile.cl/ecertchilecaFEA.crl}
X509v3 Subject Alternative Name:
othername: 1.3.6.1.4.1.8321.1=16 0a 31 35 36 31 39 36 33 37 2d 31
X509v3 Issuer Alternative Name:
Othername: 1.3.6.1.4.1.8321.2=16 0a 39 36 39 32 38 31 38 30 2d 35
X509v3 Certificate Policies: Policy: 1.3.6.1.4.1.8658.5 CPS: http://www.ecertchile.cl/CPS.htm
User Notice:
Explicit Text: Certificado Firma Electrónica Avanzada. PSC acreditado según R.A Exenta N317 de 14-08-03 de la Subsecretaría de Economía.
Signature Algorithm: sha2WithRSAEncryption

bd:ae:ef:98:fb:85:51:b9:5d:41:0d:ee:aa:23:ca:30:9d:ab:6a:da:4b:5f:fa:7a:50:de:17:94:02:8
6:4b:50:52:ec:c3:17:63:5b:23:94:79:6b:6c:44:55:01:25:a4:18:6a:c0:a5:ca:a4:30:60:f5:f7:3f:
c6:f9:77:c1:6:bb:fb:57:e2:ff:46:d1:f6:d6:b7:9f:4a:c3:92:cf:0e:85:ef:ff:94:6b:c7:1e:ee:74:0b:
ec:13:03:cb:8c:9e:90:9f:e5:4a:e1:be:01:d2:b9:7e:42:79:29:b9:b4:0c:cb:93:d0:a1:b1:57:6d:
aa:c4:d2:af:56:cf:cc:35:87:af:70:ce:69:20:05:cb:d5:81:96:00:cd:70:6e:85:bd:c4:e0:ab:df:c5:
81:6e:04:99:92:53:3e:33:3e:68:1a:e1:01:63:18:47:f1:59:e9:f4:30:99:33:dd:4e:ff:d1:f0:98:9
5:f9:3b:9b:14:1d:cd:9a:a6:09:d5:9d:6b:bb:e3:a7:08:cc:41:ad:22:ec:c0:58:70:23:36:9a:f6:14
:d2:1d:08:99:5e:79:3c:3c:82:6c:c8:6c:cd:c9:64:3b:e1:50:8c:13:83:db:59:05:3d:dd:b7:72:aa:
cb:3e:74:e7:72:5a:0f:24:fb:61:9a:5d:ef:3c:42:30:90:f9:71

-----BEGIN CERTIFICATE-----
MIIGGDCCBQCgAwIBAgIKP7eZ7AAAAAABOzANBgkqhkiG9w0BAQUFADCB1DELMAkG
A1UEBhMCQ0wxHTAbBgNVBAgTFFJlZ2lvbiBNZXRyb3BvbGl0YW5hMREwDwYDVQQH
EwhTYW50aWFnbzEUMBIGA1UEChMLRS1DRVJUQ0hJTEUxIDAeBgNVBAsTF0F1dG9y
aWRhZCBDZXJ0aWZpY2Fkb3JhMTIwMAYDVQQDEylFLUNFUlRDSElMRSBDQSBGSVJN
QSBFTEVDVFJPTklDQSBBVkFOWkFEQTEnMCUGCSqGSIb3DQEJARYYc2NsaWVudGVz
QGUtY2VydGNoaWxlLmNsMB4XDTExMTAyNjE1MDQ1OFoXDTE0MTAyNTE1MDQ1OFow
gdMxCzAJBgNVBAYTAkNMMRcwFQYDVQQIEw5NZXRyb3BvbGl0YW5hIDERMA8GA1UE
BxMIU2FudGlhZ28xLjAsBgNVBAoTJU5hY2lvbmFsIGRlIENlcnRpZmljYWNpb24g

RWxlY3Ryb25pY2ExIzAhBgNVBAsTGkNlcnRpZmljYWNpb24gRWxlY3Ryb25pY2Eg
MR0wGwYDVQQDExRQcmlzY2lsYSAgUGVyZXogVmVnYTEkMCIGCSqGSIb3DQEJARYV
cHBlcmV6QGUtY2VydGNoaWxlLmNsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCrfBtkH8Lk+DAeQkPzRhgvGEF2wgeuAJBSIZ+085LL9+Rdks7yurX/TX2XxPaB
VPzUOOYUtAMxNsKjN7yAnU1M18xg6TUw1Gr50j5LfIVuX/3NMoktTnYaeFNId8oZ
DF6XoFOCyIAM0GOLJJRSb40q8RJdtxMtrydOGwXS0T088QIDAQABo4ICbTCCAmkw
CwYDVR0PBAQDAgTwMB0GA1UdDgQWBBSBep0nuRILjQVR4Ypf1KHufdiqQzAfBgNV
HSMEGDAWgBTMSfaVWHgWdEuHT4cCHhule3esAzA+BgNVHR8ENzA1MDOgMaAvhi1o
dHRwOi8vY3JsLmUtY2VydGNoaWxlLmNsL2VjZXJ0Y2hpbGVjYUZFQS5jcmwwPQYJ
KwYBBAGCNxUHBDAwLgYmKwYBBAGCNxUIgtyDL4WTjGaF1Z0XguLcJ4Hv7DxhgZiH
SYfv/CgCAWQCAQMwIwYDVR0RBBwwGqAYBggrBgEEAcEBAaAMFgoxNTYxOTYzNy0x
MCMGA1UdEgQcMBqgGAYIKwYBBAHBAQKgDBYKOTY5MjgxODAtNTCCAU8GA1UdIASC
AUYwggFCMIIBPgYIKwYBBAHDUgUwggEwMC0GCCsGAQUFBwIBFiFodHRwOi8vd3d3
LmUtY2VydGNoaWxlLmNsL0NQUy5odG0wgf4GCCsGAQUFBwICMIHxHoHuAEMAZQBy
AHQAaQBmAGkAYwBhAGQAbwAgAEYAaQByAG0AYQAgAEUAbABlAGMAdAByAPMAbgBp
AGMAYQAgAEEAdgBhAG4AegBhAGQAYQAuAFAAUwBDACAAYQBjAHIAZQBkAGkAdABh
AGQAbwAgAHMAZQBnAPoAbgAgAFIALgBBACAARQB4AGUAbgB0AGEAIABOADMAMQA3
ACAAZABlACAAMQA0AC0AMAA4AC0AMAAzACAAZABlACAAbABhACAAUwB1AGIAcwBl
AGMAcgBlAHQAYQByAO0AYQAgAGQAZQAgAEUAYwBvAG4AbwBtAO0AYTANBgkqhkiG
9w0BAQUFAAOCAQEAva7vmPuFUbldQQ3uqiPKMJ2ratpLX/p6UN4XlAKGS1BS7MMX
Y1sjlHlrbERVASWkGGrApcqkMGD19z/G+XfBxrv7V+L/RtH21refSsOSzw6F7/+U
a8ce7nQL7BMDy4yekJ/lSuG+AdK5fkJ5Kbm0DMuT0KGxV22qxNKvVs/MNYevcM5p
IAXL1YGWAM1wboW9xOCr38WBbgSZklM+Mz5oGuEBYxhH8Vnp9DCZM91O/9HwmJX5
O5sUHc2apgnVnWu746cIzEGtIuzAWHAjNpr2FNIdCJleeTw8gmzIbM3JZDvhUIwT
g9tZBT3dt3Kqyz5053JaDyT7YZpd7zxCMJD5cQ==
-----END CERTIFICATE-----

Nota: DN = Distinguished Name

Para el caso de los Notarios, Conservadores y Archiveros Judiciales se utiliza el campo OU para especificar el cargo y si su nombramiento está en calidad de titulares, suplentes o interinos. Además se incluye la identificación de resolución emitida por el Secretario de la Corte de Apelaciones respectiva, o quien lo reemplace que acredita el nombramiento.

Por lo tanto el campo OU quedará: OU= Cargo+" "+Nombramiento+" "+"Dto:"+Numero Resolución

Formulario Solicitud de FIRMA ELECTRÓNICA AVANZADA (Entidad de Registro ER)

- Nombre del Titular
- Apellido Paterno del Titular
- Apellido materno del titular
- Cédula de identidad
- Dirección
- Región
- Ciudad
- Comuna
- Correo Electrónico
- Repetir correo Electrónico
- Teléfono

- Nombre de la empresa
- RUT de la empresa
- Dirección de la empresa
- Ciudad
- Comuna

Área o departamento (Para el caso de los Notarios, Conservadores y Archiveros Judiciales titulares, suplentes e interinos, tienen un campo diseñado para el cargo, Instancia y Certificado de la corte de apelaciones)

Formulario prevalidación de la Política FEA, Aceptación (ER)

- Fecha de solicitud
- Rut Empresa
- Rut Cliente
- Tipo Certificado
- Razón Social
- Nombre Cliente
- Rut usuario

Formulario Pre validación de la Política FEA, Verificación (ER)

- Nombre
- E-mail
- Localidad (Ciudad)
- Organización
- Provincia (Región)
- Rut usuario

Formulario Pre validación de la Política FEA, Alta (ER)

- Nombre
- Email
- Localidad (Ciudad)
- Organización
- Provincia (Región)
- Rut usuario

Para el caso de los Notarios, Conservadores y Archiveros Judiciales titulares, suplentes e interinos, se debe presentar certificado de la condición de tales emitidas por el Secretario de la Corte de Apelaciones respectiva, o quien lo reemplace.

Generación de Certificado (Entidad de Certificación EC)

- Identificación
- Password

Perfil de CRL

Versión	V2	
Emisor	email	E=email@email.cl
	País	C=CL
	Organización	O=E-CERTCHILE
	Unidad Organizacional	OU=Empresa Nacional de Certificación Electrónica

	Nombre Firmante de la CRL	CN=E-CERTCHILE CA FEA
	Localidad (Ciudad)	L=Santiago
	Estado (Región)	S=Región Metropolitana
Fecha Efectiva		
Próxima		
Algoritmo de firma	Sha2RSA	
EXTENSIONES		
Número de la CRL		
Authority Key		
Lista de Revocación	Certificados revocados	
		Número de Serie
		Fecha de Revocación
		Código de Razón de la lista de revocación de certificados

Identificación de CRL

La lista de revocación se encuentra disponible en la dirección

URL= http://crl.ecertchile.cl/ecertchilecaFEA.crl que es de Acceso Público. La estructura y componentes de la lista es la siguiente

Versión	V2	
Emisor	Email	E=email@e-mail.cl
	País	C=CL
	Organización	O=E-CERTCHILE
	Unidad Organizacional	OU= Autoridad Certificadora
	Nombre Firmante de la CRL	CN=E-CERTCHILE CA FEA
	Localidad (Ciudad)	L=Santiago
	Estado (Región)	S=Región Metropolitana
Fecha Efectiva	Viernes , 25 de Enero de 2019 15:46	
Próxima Actualización	Sábado, 26 de Enero de 2019 15:46	
Algoritmo de firma	sha2RSA	
Número de la CRL		
Authority Key	Id. de clave=	
	Certificados revocados	

Lista de Revocación		Número de Serie
		Fecha de Revocación
		Código de Razón de la lista de revocación de certificados

5 ADMINISTRACIÓN DE LA ESPECIFICACIÓN DE LA CP

La EC podrá modificar las estipulaciones de la presente CP, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación y, siempre y cuando, toda modificación se justifique desde el punto de vista jurídico, técnico y comercial.

Los procedimientos de Publicación y notificación, son los descritos en las CPS.

6 REVOCACIÓN DE CERTIFICADOS

La revocación de Certificados son mecanismos a utilizar en el supuesto de que por alguna causa establecida en la presente CP se deje de confiar en el Certificado antes de la finalización de su período de validez originalmente previsto.

6.1 SUPUESTO DE REVOCACIÓN

Los Certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del suscriptor.
- Pérdida o inutilización por daños del soporte del Certificado.
- Fallecimiento del signatario o de su representado, incapacidad sobreviviente, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Inexactitudes graves en los datos aportados por el signatario para la obtención del Certificado, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado, no se adecuen a la realidad.
- Que se detecte que las claves privadas del suscriptor o de la EC han sido comprometidas, bien por que concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- Por incumplimiento por parte de la ER, EC o el suscriptor de las obligaciones establecidas esta CP.

- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene conforme a derecho.
- Por la concurrencia de cualquier otra causa especificada en la presente CP o en la CPS.

6.1.1 Efectos de la renovación.

El efecto de la revocación del Certificado es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un Certificado impide el uso legítimo del mismo por parte del suscriptor.

La revocación del Certificado por causa no imputable al suscriptor originará la emisión de un nuevo Certificado a favor del suscriptor por el plazo restante para concluir el periodo original de validez.

La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación del mismo.

6.2 PROCEDIMIENTO DE REVOCACIÓN

6.2.1 Legitimación Activa

Deberán solicitar la revocación en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado 6.1 anterior:

• El suscriptor del Certificado así como la persona natural o jurídica representada por éste.

• La ER, respecto a aquellos Certificados en cuya emisión hayan participado.

• La persona jurídica que conste en el Certificado.

Asimismo, podrá solicitar la revocación cualquier tercero con un interés legítimo en caso de que tenga conocimiento de la existencia alguna de las siguientes causas:

- Pérdida del soporte del Certificado.
- Fallecimiento del signatario.
- Incapacidad sobreviviente, total o parcial.
- Inexactitudes en el Certificado.

- Compromiso de la fiabilidad del Certificado.
- Compromiso de las claves.
- Cese del representante en el caso de los certificados con poderes.
- Extinción de la persona jurídica representada.
- Revocación de la autorización de la entidad que conste en el Certificado en el caso de los Certificados sin poderes.

En todo caso, la EC podrá iniciar de oficio el procedimiento de revocación de Certificados, en cualquiera de los casos previstos en el apartado 6.1 anterior.

6.2.2 Recepción de Solicitudes de Revocación

Se establece el siguiente procedimiento para la solicitud de revocación de un Certificado:

a) Notificación de la revocación, identificándose e indicando los motivos, por medio de uno de los siguientes mecanismos:

- Comunicación telefónica a través del siguiente número: 56 2 2818 5760
- Vía e-mail: sclientes@e-certchile.cl
- Fax a través de este número: 56 2 26649699
- Vía web en la dirección: http://www.e-certchile.cl

Sólo el suscriptor del certificado puede utilizar alguno de los medios anteriores, en el caso de que fuera otra persona el solicitante, deberá concurrir personalmente a la oficina de E-certchile para realizar su solicitud.

En el caso de que la solicitud sea realizada por alguno de los medios detallados en el apartado 6.2.2 anterior, E-Certchile procederá a Revocar el certificado, a la espera de su ratificación.

El suscriptor (o un usuario) dispone de 48 horas desde su solicitud para presentarse ante E-Certchile para ratificar su solicitud de Suspensión/Revocación. El Suscriptor deberá presentar su RUT para identificarse y se le hará entrega del formulario de ratificación de revocación de certificado, en donde deberá señalar el motivo de revocación, firmar y estampar su huella dactilar.

b) Mediante la presencia física del usuario en la ER donde realizó la solicitud del Certificado, ratificando la revocación.

Cualquier otra forma no contemplada será resuelta por la ER o EC.

El inicio del proceso de revocación se realizará en forma inmediata al ser recibida la solicitud.

Cuando la persona que solicita la revocación del Certificado no sea el propio suscriptor, deberá dirigirse en persona a cualquiera de las oficinas de la EC o las ER.

Las conversaciones telefónicas que se mantengan podrán ser grabadas y registradas por E-CERTCHILE a efectos probatorios.

6.2.3 Decisión de Revocar.

Una vez recibida y autenticada la solicitud de revocación, E-CERTCHILE efectuará la revocación efectiva del Certificado. La decisión de revocar un Certificado corresponde a la EC.

6.2.4 Comunicación y publicación de la renovación.

La decisión de revocar el Certificado será comunicada por la EC al suscriptor mediante e- mail firmado digitalmente, y en el caso de solicitar la revocación vía Web la confirmación le será desplegada automáticamente indicando el código de revocación.

Igualmente, se publicará la revocación del Certificado en la CRL.

La revocación comenzará a producir efectos a partir de su publicación por parte de la EC, salvo que la causa de revocación sea el cese de la actividad de la EC, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

Para el caso de los Notarios, Conservadores y Archiveros Judiciales, titulares, suplentes e interinos, podrá solicitar el código de revocación el cual podrá presentar en junto con el aviso de extravío a la Corte de Apelaciones.

7 SOLICITUD DE TÉRMINO DE CONTRATO

El suscriptor del certificado podrá dar término al contrato de prestación de servicios de certificación de FEA, enviando carta certificada, indicando los motivos del término de contrato, dicha carta deberá estar dirigida a: “Empresa Nacional de Certificación Electrónica “ Monjitas 392 , piso 17. El término del contrato no implica devolución de los valores involucrados en la transacción original y no implica la revocación del certificado por el periodo de vigencia restante a menos que el suscriptor lo solicite expresamente.

E-certchile se reserva el derecho de comprobar la validez de la carta de término de contrato.

Las renovaciones de certificados de firma avanzada se realizarán automáticamente una vez cumplido el periodo de vigencia del certificado a menos que el suscriptor declaré explícitamente en la carta de “Término de Contrato” su voluntad de no continuar utilizando el servicio.

8 JERARQUÍA DE NORMAS

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

9 OBJETIVO DE SEGURIDAD PARA RESGUARDO DE LLAVES CRIPTOGRÁFICAS

El objetivo de resguardar las llaves criptográficas de la AC es tener la capacidad de poder restaurar el servicio completo en caso de desastre. Este respaldo debe ser realizado en un lugar con estándares de restricción de acceso, tal como la sala de equipos de E-certchile.