PO01
Políticas de Certificados
CP - Firma Electrónica Avanzada
Documento Público

Acepta.com S.A.

Versión 1.2 - Mayo 2005

Contactos:

Enrique Velasco Aguirre
Product Manager Firma Electrónica
Enrique.velasco@acepta.com

Roberto Opazo Gazmuri
Gerente General de Acepta.com
roberto@opazo.cl

CODIGO: SC-P-04
VERSION: 1.2
2005-05-30

La referencia válida a este documento se encuentra en:

\\Nts_cus_arch01\Comun\Sistema de Calidad\Gerencia de Servicios de Certificación\Otros Documentos\SC-O-02 PO01 - CP FA.doc

Si este documento es impreso, no es un documento controlado.

Paseo Bulnes 241, piso 5, Santiago, Chile.
Fono: (56 2) 496 8100 Fax: (56 2) 496 8130
www.acepta.com
info@acepta.com

PROPIEDAD INTELECTUAL

El presente documento es propiedad intelectual de Acepta.com.

Se autoriza su lectura, publicación y reproducción total, por cualquier medio, en forma pública o privada, sin necesidad de autorización previa.

Su reproducción parcial se encuentra estrictamente prohibida, a menos que exista una autorización previa y escrita, firmada por representantes legales de Acepta.com cuya firma conjunta sea suficiente para actuar en representación de la empresa.

El único fin para el cual podrá copiarse en forma parcial este documento, sin contar con autorización previa, será cuando se esté citando el documento.

En particular, de deja expresa constancia de que Acepta.com no autoriza la copia de segmentos de este documento para incluirlos en otros documentos que no citen la fuente de la información.

DECLARACIÓN DEL EMISOR

Las políticas de certificados de firma electrónica avanzada y prácticas de certificación de Acepta.com se encuentran públicamente disponibles en www.acepta.com y detallan el funcionamiento, las obligaciones y los derechos de los titulares y receptores de este tipo de certificados, así como de Acepta.com en su calidad de Prestador de Servicios de Certificación. A continuación se resumen los aspectos más importantes señalados en los documentos citados:

- Acepta.com emplea métodos idóneos para verificar la identidad de los solicitantes y apoyar el proceso de uso de certificados de firma electrónica, incluyendo emisión, búsqueda, consulta y revocación de certificados.
- El Plan de Seguridad y el Manual de Operaciones de Acepta.com protege el acceso físico y lógico a los recursos de la empresa para asegurar el fiel cumplimiento de las políticas y prácticas establecidas.
- El Ministerio de Economía acredita los documentos y el funcionamiento de Acepta.com como Prestador de Servicios de Certificación para Firma Electrónica Avanzada según lo establecido en la Ley 19.799.
- Es obligación del titular de los certificados de firma electrónica avanzada almacenar la llave privada de su certificado en un dispositivo especializado y certificado según el estándar internacional FIPS-140-1 nivel 2 o superior.
- En caso de disputa legal, Acepta.com está obligada a demostrar su correcto funcionamiento, especialmente en el proceso de registro presencial hecho en forma previa a la emisión del certificado.
- Acepta.com no se responsabiliza del mal uso que los usuarios titulares le puedan dar a sus certificados.

ÍNDICE

1.- INTRODUCCIÓN

En este capítulo se introducen y describen las Políticas de Certificados de Firma Electrónica Avanzada de Acepta.com. Se muestra un resumen del proceso de certificación, entidades involucradas, y uso de certificados. Por último, se detallan contactos donde obtener información o ayuda adicional.

1.1.- Resumen

1.1.1.- CP y CPS

Las políticas y prácticas de certificación (CP y CPS), así como las políticas de privacidad, contienen la información más importante que una comunidad de usuarios debe conocer para definir el nivel de confianza que le asigna a cada tipo de certificados. Estos documentos se hacen públicos, para que cualquier usuario tenga acceso a esta información relevante.

Adicionalmente, existen otros documentos importantes para la operación de una empresa que presta servicios de certificación, entre ellos están la evaluación de riesgos, las políticas de seguridad, las políticas del personal, el plan de continuidad operacional y otros que apoyan el correcto funcionamiento de todas las funcionalidades anunciadas en los documentos públicos de la empresa. Estos documentos no son públicos porque su difusión puede comprometer el nivel de seguridad del servicio prestado. Sin embargo, estos documentos existen y son auditados por organismos independientes, especializados y que son de confianza para toda la comunidad de usuarios.

Acepta.com ha pasado por varios procesos de acreditación realizados por los siguientes organismos independientes de acreditación: Servicios de Impuestos Internos, Servicio Nacional de Aduanas y Ministerio de Economía de Chile. Estas entidades han tenido acceso a todos los documentos de la empresa, han podido revisar los procedimientos seguidos, han entrevistado y evaluado al personal, resolviendo acreditar a Acepta.com.

Las acreditaciones mencionadas son una declaración pública, orientada a que la comunidad de usuarios pueda tener confianza, en que tanto las políticas como las prácticas de certificación coincidan con lo que Acepta.com realmente hace y además, indica que estas políticas y prácticas son suficientemente exigentes como para confiar en los certificados de Acepta.com.

La diferencia entre políticas y prácticas de certificación consiste en que las políticas (CP) son específicas para cada tipo de certificado y muestran información general con respecto a “QUE” es lo que el PSC hace para emitir este tipo particular de certificados. En cambio, las prácticas (CPS) contienen

información más precisa sobre "COMO" el PSC realiza ciertas funciones. Las prácticas son comunes para todos los tipos de certificados emitidos.

Las CP no detallan COMO o con que MECANISMOS se cumplen los requisitos establecidos. De esta forma, es posible definir CP que sean compatibles entre distintos PSC que cumplen con estos requisitos usando MECANISMOS diferentes, como ocurre con la firma electrónica avanzada, regulada por la Ley 19.799 de la República de Chile.

Los MECANISMOS y detalles operacionales utilizados para cumplir con cada política señalada en las CP de cada tipo de certificados son explicados en los manuales operacionales del PSC. Estos documentos y los elementos de software y hardware de apoyo correspondientes también son auditados por los organismos acreditadores.

Para poder comparar CP y CPS es necesario que exista algún punto de referencia común que guíe la evaluación. Es por eso que Acepta.com, en su deseo de promover la transparencia y calidad de los certificados que emite, ha adoptado criterios internacionalmente reconocidos en la definición, estructura y presentación de estas prácticas de certificación. Específicamente, es consistente con las recomendaciones surgidas en la Internet Engineering Task Force (IETF)[1] expresadas en el documento denominado "Marco estructural para políticas y prácticas de certificación"[2], las cuales han sido internacionalmente apreciadas por organismos como el Departamento de Defensa de U.S.A y otras agencias federales[3], comisiones de la Comunidad Europea como la Iniciativa para la Estandarización de Firmas Digitales (EESSI)[4], gobierno de Canadá, grupos de trabajo de la APEC[5] como el Electronic Authentication Task Group y variadas

[1] Comunidad internacional compuesta por gran cantidad de ingenieros, diseñadores, vendedores y expertos que investigan y promueven las distintas tendencias, estándares e investigaciones relacionadas con Internet. Entre los estándares que han surgido desde la IETF destacan:

[2] Referenciado como el documento RFC 2527.

[3] Modelo recomendado por el Federal PKI Steering Committee, grupo de expertos trabajando en definir un modelo para agencias federales en U.S.A.

[4] European Electronic Signature Standardization Initiative (EESSI).

[5] Asia Pacific Economic Cooperation (APEC). Grupo que incluye las mayores economías de la región de Asia y el Pacífico, contando actualmente con 21 países miembros. En el Electronic Authentication Task Group han identificado el modelo propuesto en el documento RFC2527 como estándar para las CPS.

autoridades certificadoras internacionales como Entrust, PSCE y Camerfirma de España, IDSafe, BelSIgn, Digital Signature Trust (DST) y NetTrust.

Una política de certificado está definida, según el estándar internacional "ISO/IEC 9594-8/ITU-T Recomendación X.509", como "un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad en particular y/o clase de aplicación con requerimientos de seguridad comunes".

Tales políticas son las que se prosigue en detallar, y están disponibles en el Sitio WEB de Acepta.com (www.acepta.com) para conocimiento público.

1.1.2.- Estructura de este documento

La estructura de este documento es análoga a la de las CPS de Acepta.com, pero su contenido presenta sólo los aspectos pertinentes a los certificados de firma electrónica avanzada.

Estos aspectos no son presentados en el documento de CPS de Acepta.com, el cual es un documento común para todos los tipos de certificados emitidos por la empresa.

1.2.- Identificación

El presente documento se denomina "Políticas de Certificado de Firma Electrónica Avanzada de Acepta.com", las que internamente se citan como CP o CP-FA y están registradas con el número único internacional (OID) 1.3.6.1.4.1.6891.3.

En las CPS de Acepta.com, sección "1.2 Identificación", se presenta la lista completa de OIDs administrados por Acepta.com.

1.3.- Comunidad de usuarios y utilización de los certificados

En las CPS de Acepta.com se presenta un esquema general de operación para cualquier tipo de certificado de clave pública.

Los certificados de firma electrónica avanzada de persona natural son emitidos para soportar las siguientes necesidades de seguridad:

- **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 e imponer que el almacenamiento de la llave privada sea en un dispositivo especializado y acreditado según la norma internacional FIPS-140 nivel 2.
- **Integridad de mensajes:** los mensajes firmados con certificado de firma electrónica avanzada permiten validar si el contenido de mensaje ha sido alterado en el tiempo transcurrido desde su generación.

- **Firmas digitales:** las firmas digitales producidas con certificados de firma electrónica avanzada ofrecen los medios de respaldo para demostrar fehacientemente, incluso en tribunales, la autenticidad de un mensaje o documento electrónico.
- **Privacidad:** Los certificados de firma electrónica avanzada permiten cifrar mensajes de forma que al ser transmitidos sean visibles sólo por el remitente correspondiente. Sin embargo, Acepta.com recomienda usar otros certificados para estos fines, con una duración de al menos 10 años. La expiración o revocación de los certificados de firma electrónica avanzada no provocan consecuencias con las firmas electrónicas generadas en forma previa al término de la vigencia del certificado, pero en el caso de mensajes cifrados, se genera un problema al expirar el certificado, ya que este se debe conservar durante todo el período de tiempo en el que se desee poder descifrar los mensajes protegidos.

A continuación se listan las principales entidades involucradas en el ciclo de vida de los certificados de firma electrónica avanzada. Todas estas entidades desempeñan una función definida en detalle en la "Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma".

1.3.1.- Titular, usuario o suscriptor

Persona que utiliza bajo su exclusivo control un certificado de firma electrónica avanzada. Las Políticas de Firma Electrónica Avanzada sólo permiten certificar a personas naturales y que tengan RUN emitido por el Servicio de Registro Civil e Identificación de Chile.

1.3.2.- Solicitante

Persona que solicita un certificado de firma electrónica avanzada. No necesariamente es un usuario o titular, pero debe ser una persona natural.

1.3.3.- Autoridad de Registro

Es la organización que se hace cargo de verificar en forma presencial la identidad del solicitante, antes de emitir un certificado de firma electrónica avanzada.

Para los certificados de firma electrónica avanzada Acepta.com sólo trabaja con funcionarios internos que desempeñan el Rol de Operador de Registro y con el Servicio de Registro Civil e Identificación de Chile. En el caso del Registro Civil, las prácticas y mecanismos utilizados para verificar la identidad del solicitante son los mismos que se usan cuando un ciudadano solicita una cédula de identidad o pasaporte.

1.3.4.- Prestador de Servicios de Certificación

Acepta.com y otros Prestadores de Servicios de Certificación que sean acreditados por la Entidad Acreditadora.

1.3.5.- Parte que confía

Persona o sistema que recibe un certificado de firma electrónica avanzada. Normalmente el certificado se recibe junto con un documento o mensaje y su correspondiente firma electrónica.

En el caso de los certificados de firma electrónica avanzada la parte que confía puede ser cualquiera involucrada en procesos como los siguientes:

- Certificado para identificación de persona
- Certificado para uso en la Banca
- Certificado para realizar operaciones de importación y exportación
- Certificado para declaraciones previsionales
- Certificado para uso comercial
- Certificado para pago tributario, factura electrónica y documentos tributarios electrónicos
- Certificado para pagos
- Certificado para otros usos reconocidos por las partes de procesos en la red

1.3.6.- Entidad Acreditadora

Es la Subsecretaría de Economía, Fomento y Reconstrucción.

1.4.- Contactos

Cualquier consulta respecto a las normas contenidas en este documento, puede ser realizada en la siguiente dirección:

Acepta.com
Paseo Bulnes 241, 5º Piso. Santiago Centro – Chile
Teléfono: +56 (2) 328 8100
Fax: +56 (2) 328 8130
Código Postal : 6520420
e.-mail: info@acepta.com
Web : http://www.acepta.com

Le recomendamos utilizar los formularios de consulta disponibles en nuestro sitio web. Lamentablemente la proliferación del spam (correo electrónico masivo no solicitado, normalmente comercial) hace que los e-mails enviados a info@acepta.com corran el riesgo de ser confundidos con spam.

2.- CONSIDERACIONES GENERALES

En este capítulo se expresan una serie de tópicos legales y generales, como obligaciones, responsabilidades, tarifas, etc. pertinentes a los certificados de firma electrónica avanzada, y relevantes para a todas las partes interesadas directa o indirectamente con los certificados digitales emitidos por Acepta.com o por alguna de sus Autoridades de Registro o Certificadoras acreditadas.

2.1.- Obligaciones

2.1.1.- Obligaciones de Acepta.com

Acepta.com, en su calidad de Prestador de Servicios de Certificación, se obliga a cumplir los requerimientos detallados en las CPS de Acepta.com y la "Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma". Específicamente, al emitir certificados de firma electrónica avanzada se obliga a lo siguiente:

- Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano;
- Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento de la Ley 19.799. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley Nº 19.628, sobre Protección de la Vida Privada;
- En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad;
- Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten;

- En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante;
- Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores;
- Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que vaya a dar a los datos de los certificados especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;
- En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;
- Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos.
- Cumplir con las demás obligaciones legales, especialmente las establecidas por la Ley 19.799, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores y Nº 19.628, sobre Protección de la Vida Privada.
- Ejecutar todas sus actividades de certificación acorde a las normas estipuladas en éstas CP y CPS.
- Expedir o emitir los certificados con mecanismos tecnológicos y criptográficos que garanticen que el proceso de certificación es realizado adecuadamente.
- Revocar unilateralmente los certificados, en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido, y notificar a las partes correspondientes acorde a las normas estipuladas en éstas CP
- Mantener los resguardos tecnológicos para evitar cualquier falsificación y adulteración de las llaves privadas que Acepta.com utiliza para firmar los

certificados, listas de revocación y respuestas en línea a consultas sobre el estado de los certificados.

- Notificar por e-mail al solicitante o titular de un certificado ante los siguientes eventos:
  - Cuando su solicitud fue aceptada.
  - Cuando su solicitud fue rechazada.
  - Cuando su certificado fue revocado.
  - Cuando su certificado fue suspendido.
  - Cuando su certificado fue reactivado.
  - Cuando la información de respaldo del certificado sea entregada a la justicia en caso de juicio.
- Actualizar el repositorio público de certificados cada vez que un certificado es emitido.
- Actualizar las listas de revocación con una frecuencia de al menos 24 horas.

2.1.2.- Obligaciones de autoridades certificadoras acreditadas

En el caso de certificados de Firma Electrónica Avanzada, Acepta.com no trabaja con Autoridades Certificadoras Acreditadas.

2.1.3.- Obligaciones de autoridades de registro

El Registro Civil es el único organismo externo a Acepta.com que puede realizar el registro presencial. En este caso, se deben seguir los mismos procedimientos de verificación de identidad utilizados por este Servicio en los trámites de obtención de cédula de identidad o pasaporte.

Toda la información de verificación de identidad enviada por el Registro Civil a Acepta.com es firmada electrónicamente y transmitida usando un canal seguro que cifra las comunicaciones con SSL aplicando al menos 128 bits desconocidos.

2.1.4.- Obligaciones de los suscriptores

Los suscriptores que soliciten certificados de Firma Electrónica Avanzada a Acepta.com, se obligan a cumplir con los siguientes requerimientos:

- Conocer el contenido de la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Conocer las normas estipuladas en las CPS y CP de Acepta.com, y aceptar lo que allí se estipule en forma previa a la instalación y eventual aceptación de un certificado digital emitido por Acepta.com.

- Protección de la clave de activación o PIN, definida en el momento del registro de antecedentes, la cual es personalísima y confidencial.
- Protección y confidencialidad de su llave privada asociada a la llave pública. Dicha llave es personalísima y confidencial, generada exclusivamente en el equipo del suscriptor y tenedor del certificado. En caso de su pérdida o cualquier circunstancia que comprometa la confidencialidad de dicha llave, deberá acudir personalmente a las oficinas de Acepta.com o enviar un correo electrónico, firmado digitalmente, notificando de tal circunstancia. La administración de la llave privada es de exclusiva responsabilidad del tenedor o suscriptor del certificado.
- Almacenar la llave privada de su certificado en un dispositivo especializado y acreditado según el estándar internacional FIPS-140-1 nivel 2 o superior.
- Notificación a Acepta.com de cualquier modificación de sus antecedentes entregados en el momento del registro presencial.
- Suspender o Revocar el certificado en caso de que el acceso a la llave privada haya dejado de estar bajo su exclusivo control.

2.1.5.- Obligaciones de usuarios de certificados

Los usuarios de certificados de firma electrónica avanzada emitidos por Acepta.com, o cualquier entidad que deposite su confianza en dichos certificados, se obligan a cumplir los requerimientos comunes estipulados en las CPS y a tomar las siguientes medidas de seguridad:

- Brindar declaraciones exactas y completas en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación y a actualizar sus datos en la medida que éstos vayan cambiando.
- Custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador.
- Utilizar software que valide automáticamente las firmas electrónicas y certificados electrónicos asociados a mensajes recibidos.
- En el caso del correo electrónico, además del punto anterior, se debe verificar que la casilla de correo electrónico corresponda con la casilla informada en el certificado emitido por Acepta.com. Si la herramienta de correo electrónico no realiza esta validación en forma automática, entonces el usuario será responsable de realizarla en forma visual.

- Siempre se debe revisar que el nombre de la persona que firma el documento o mensaje coincida con el nombre de la persona informada en el certificado emitido por Acepta.com.
- Si las herramientas de software utilizadas no validan automáticamente la vigencia de los certificados, entonces esta validación debe ser hecha por inspección visual utilizando alguno de los mecanismos habilitados para tal efecto: Consulta en página web, consulta de CRL o consulta en línea usando OCSP.
- Recordar que Acepta.com cuenta con un seguro de responsabilidad civil que le permite responsabilizarse como máximo por un monto de UF 5.000. En consecuencia, es responsabilidad de la parte que confía decidir cuando aceptará firmas electrónicas que se validen con certificados de Acepta.com en el contexto de transacciones que superen este límite.
- Al instalar el certificado raíz de Acepta.com verificar que la clave pública del certificado raíz sea la siguiente:

```
30 82 01 08 02 82 01 01 00 c1 18 43 f3 7c b3 d3 c3 46 b4 5a a8 a6 c7 18 39 4d f4 b3 fb f8 4d
c7 27 43 e8 03 22 ba 80 e2 57 c9 57 91 64 72 c0 d5 50 d2 e4 82 66 48 a9 9c e4 12 bc f0 3b 6b
8e 29 00 d1 a5 ec ef a0 04 01 24 cf 72 fb a1 d4 af b2 41 16 7d 30 53 df 06 ec 45 91 6c 8b 4e
85 c7 91 6a b9 89 ad 96 d1 81 b2 04 88 24 6b dc dd 70 29 9d 2a bf 29 8e 80 2e 3e 0c 4c 7d 5a
3b df 02 95 7a 62 62 8e 30 c6 d6 2a 38 a9 47 37 47 2f 48 94 2d 55 da 7e bc e1 44 80 fa 06 70
d1 89 b1 ed ce 04 4c 87 e8 cb 95 31 21 5c d0 8a 4b e6 a9 0f 2b bb f5 c0 f5 0e 6b c6 6f 40 02
d3 b9 ea 04 cc bc fe ba b2 e5 3f c3 02 05 91 a3 54 39 b9 d6 16 fd ac ec d1 5f 1d 33 89 de b3
73 06 09 d8 1d 3c 18 5f 02 92 d4 d4 19 76 c3 8f ca 4e f8 8a 08 e6 54 f4 e1 05 a7 12 b5 36 d3
1f dd 54 67 f8 46 71 50 78 21 c5 94 b5 bd c7 d6 6b 02 01 03
```

2.1.6.- Obligaciones del repositorio

El repositorio público de Acepta.com debe permitir realizar las siguientes consultas:

- **Consulta por un certificado emitido a través de una página Web**: Los usuarios cuentan con una página web en la que pueden ingresar el e-mail o RUT del suscriptor, siendo ésta:

  http://www.acepta.com/ac/servlet/consultacertificado

  El sistema no permite la búsqueda utilizando comodines.

- **Consulta on-line automática vía el protocolo OCSP**[6]. Este es un mecanismo que permite la consulta en línea y que proporciona todas las respuestas respecto al estado de un certificado firmadas digitalmente, lo que ofrece considerables garantías de confiabilidad.

  La dirección OCSP de Acepta.com es: http://ocsp.acepta.com/

[6] Corresponde a las siglas en Inglés de On-line Certificate Status Protocol (OCSP),

- **Consulta de CRL**.[7] Este es un archivo que está firmado digitalmente por el Prestador de Servicios de Certificación y que contiene una lista con los certificados revocados en un periodo de tiempo determinado. Las CRL de Acepta.com se actualizan cada 24 horas.

  La dirección de la CRL para la Firma Electrónica Avanzada es: http://crl.acepta.com/FA.crl

2.2.- Responsabilidades

Acepta.com será responsable de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. Corresponderá al prestador de servicios demostrar que actuó con la debida diligencia en el proceso de emisión de certificados de firma electrónica avanzada.

Sin perjuicio de lo dispuesto en el párrafo anterior, Acepta.com no será responsable de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica.

En ningún caso la responsabilidad que pueda emanar de un certificado de firma electrónica avanzada comprometerá la responsabilidad pecuniaria del Estado.

2.3.- Indemnizaciones

Acepta.com deberá contratar y mantener un seguro, que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento.

Tanto respecto de los suscriptores que contraten los servicios de certificación digital y que acepten las presentes CP y CPS, como respecto de los terceros que adhieran a ella, Acepta.com declara que en la eventualidad de haberse consultado por el estado de un certificado revocado de firma electrónica avanzada, por medio de los servicios de consulta electrónica vía el protocolo OCSP que Acepta.com proporciona, y que habiéndose obtenido una respuesta electrónica firmada digitalmente por Acepta.com respecto al estado de tal certificado en la que se informe equivocadamente el estado vigente, se establece que Acepta.com se hace responsable por la validez de dicha respuesta, y delimita su responsabilidad hasta UF 5.000 como monto máximo o de tope, con total independencia del número de firmas digitales y de transacciones para las cuales sea utilizado dicho certificado.

Las responsabilidades limitadas en la forma señalada, rigen y se aplica para toda clase de daños y perjuicios, cualquiera sea su clase y naturaleza. Estos se

[7] Corresponde a las siglas en Inglés de Certificate Revocation List (CRL)),

aplican tanto para el suscriptor o signatario titular del mismo y del tercero que confía y adhiera a estas CP.

2.4.- Interpretación y Legislación aplicable

Acepta.com declara efectuar sus actividades en conformidad con los principios generales de la legislación chilena y dando cumplimiento a todas y cada una de las leyes aplicables a las actividades desarrolladas por Acepta.com.

En particular, para certificados de firma electrónica avanzada, declara dar estricto cumplimiento a la Ley 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; Ley Nº 19.496, sobre Protección de los Derechos de los Consumidores; y Nº 19.628, sobre Protección de la Vida Privada.

2.5.- Precios

El ciclo de vida de un certificado de firma electrónica supone que Acepta.com mantenga en pleno funcionamiento toda la infraestructura de apoyo a estos procesos. En este ciclo de vida existen varios puntos de contacto, tanto del titular del certificado, como de las partes que confían en los certificados, con Acepta.com. A continuación se identifican estos puntos de contacto y se señala cuando corresponde cancelar por los servicios utilizados:

- **Registro presencial y vigencia del certificado**: El solicitante debe cancelar el valor del registro presencial y del período de vigencia contratados en el momento que haya acordado con Acepta.com.
- **Renovación del certificado**: La renovación de los certificados es tratada comercialmente como un tipo especial de registro presencial y pago por un nuevo período de vigencia del certificado, por lo que también se debe cancelar lo que el solicitante acuerde con Acepta.com en el momento de la renovación.
- **Consulta del repositorio público de certificados emitidos**: Puede ser consultado sin costos, tanto por los titulares como por las partes que confían.
- **Consulta del repositorio público de listas de revocación (CRL)**: Puede ser consultado sin costos, tanto por los titulares como por las partes que confían.
- **Consulta en línea del estado de un certificado (OCSP)**: Puede ser consultado sin costos, tanto por los titulares como por las partes que confían.
- **Sitio web de Acepta.com**: El sitio Web de Acepta.com, sus políticas y sus prácticas de certificación pueden ser consultados sin costos, tanto por los titulares como por las partes que confían.

- **Revocación de certificados**: Para revocar un certificado es necesario firmar electrónicamente una solicitud de revocación. Si el titular del certificado conserva su llave privada podrá hacerlo sin costos adicionales. En caso de que el titular del certificado haya perdido su llave privada, deberá cancelar un nuevo certificado para solicitar la revocación del certificado anterior, y si lo desea, del certificado recién emitido.
- **Suspensión de certificados**: La suspensión de certificados por 48 horas puede ser hecha con un e-mail simple o llamado telefónico. En ambos casos, el servicio es brindado sin nuevos costos.
- **Soporte**: Acepta.com se reserva el derecho de habilitar servicios pagados de soporte, sobre el uso de certificados de firma electrónica. Los únicos servicios que Acepta.com se obliga a brindar sin cobros adicionales a los asociados con el registro presencial y el período de vigencia de los certificados, son aquellos marcados sin costo en los puntos anteriores de esta sección.

Las tarifas correspondientes a la emisión de certificados están disponibles en el sitio Web www.acepta.com .

2.6.- Publicaciones

Acepta.com publica en su sitio Web www.acepta.com, las políticas de certificado aplicables a los certificados de firma electrónica avanzada, así como las Prácticas de Certificación (CPS), las cuales están a disposición de los usuarios sin cargo alguno.

En caso de modificarse dicho documento, se le notificara a los usuarios por e-mail, en la dirección por ellos establecida durante los procesos de certificación.

La frecuencia de actualización de los repositorios públicos de Acepta.com se encuentra definida en sus Prácticas de Certificación (CPS).

2.7.- Auditoría y acreditación

Las políticas de certificación de firma electrónica avanzada y las prácticas de certificación de Acepta.com son acreditadas por la Subsecretaría de Economía, Fomento y Reconstrucción, en su calidad de Entidad Acreditadora, definida en la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

Adicionalmente, las prácticas de certificación y los procedimientos generales de Acepta.com, se encuentran acreditados por otros organismos que han acreditado otras políticas de certificados emitidos por Acepta.com.

2.8.- Confidencialidad

Acepta.com, adhiere y efectúa sus operaciones en conformidad con lo establecido por la Nº 19.628, sobre Protección de la Vida Privada.

Las políticas de privacidad de Acepta.com se encuentran publicadas en www.acepta.com.

2.9.- Derechos de propiedad intelectual

Aplica lo indicado en las CPS.

3.- IDENTIFICACIÓN Y AUTENTICACIÓN

En esta sección se presentan juntas, las políticas y prácticas que Acepta.com emplea en la validación de la identidad de las personas que solicitan un certificado de firma electrónica avanzada.

3.1.- Registro inicial

3.1.1.- Tipos de nombres asignados al titular

Los certificados de firma electrónica avanzada contienen los siguientes datos del titular:

- **RUN**: Rol Único Nacional asignado por el Servicio de Registro Civil e Identificación de Chile. Los ciudadanos extranjeros deberán obtener un RUN antes de solicitar un certificado de firma electrónica avanzada de Acepta.com.
- **Nombre**: Los nombres y apellidos del solicitante, tal como fueron registrados por el Registro Civil, pero eliminando los acentos y reemplazando las "ñ" por "n". Estos reemplazos le molestan a muchos usuarios, pero son necesarios, ya que se trata de caracteres no soportados por el estándar X.509 en los campos de identificación de usuario. Por lo tanto, al incluir estos caracteres, en algunas plataformas se presentan problemas, aunque en otras funcionan adecuadamente. Acepta.com no violará el estándar X.509 aún cuando el usuario lo solicite expresamente.
- **e-mail**: Un e-mail declarado por el solicitante. El estándar X.509 permite la inclusión de varias casillas de correo electrónico, pero las pruebas de compatibilidad con clientes de correo electrónico hechas por Acepta.com muestran que la mayoría de los clientes de correo electrónico no son capaces de reconocer certificados X.509 con varias casillas de e-mail.

3.1.2.- Registro presencial

La identidad del solicitante debe ser validada en forma presencial por un operador de registro de Acepta.com o por un funcionario del Servicio de Registro Civil e Identificación de Chile.

En el caso de que el registro presencial sea realizado por un operador de registro de Acepta.com, este puede reunirse con el solicitante en una de las oficinas de registro de Acepta.com, anunciadas en www.acepta.com y también es posible acordar un registro presencial en dependencias del solicitante. Acepta.com se reserva el derecho a definir la cobertura disponible para este efecto. En la información capturada por el operador de registro se incluye el RUN, nombre, fecha de nacimiento, e-mail, foto, firma manuscrita, impresión dactilar y datos de contacto del solicitante.

Si el registro presencial es hecho por el Registro Civil, entonces se utilizan los mismos procedimientos de verificación de identidad utilizados por este organismo para la emisión de cédulas de identidad y pasaporte. El Registro Civil le comunica a Acepta.com los datos de la identidad del solicitante a través de un canal seguro y utilizando mensajes firmados electrónicamente. En la información enviada por el Registro Civil se incluye el RUN, nombre, fecha de nacimiento, e-mail, foto, digitalización de la firma manuscrita, impresión dactilar y datos de contacto del solicitante.

Acepta.com no implementa procedimientos de control a las actividades del Registro Civil, ya que se trata de la máxima Autoridad en Chile en verificación de identidad.

3.1.3.- Método para probar posesión de la llave privada

La llave privada asociada a un certificado de firma electrónica avanzada emitido por Acepta.com es siempre generada exclusivamente en un dispositivo especializado en almacenamiento de llaves privada certificado según el estándar FIPS-140-1 nivel 2 o superior.

Dicha llave es generada en el equipo del suscriptor usando las herramientas que provea el browser del usuario y los programas del dispositivo utilizado. Este programa se comunica con el sitio Web de Acepta.com, y para autentificar que el usuario que está ejecutando el programa es el que corresponde, se requiere previamente que el suscriptor digite un Nº de solicitud y clave de activación o PIN válidos para iniciar el proceso de instalación. El PIN fue definido por el suscriptor en el momento de solicitar el certificado y registrar sus antecedentes, y el Nº de solicitud se le envía por e-mail una vez aprobada la solicitud de certificado correspondiente. En el sitio Web de Acepta.com se valida que dichos datos correspondan a una solicitud pendiente, y sólo entonces se continúa con el proceso. Luego, el dispositivo del usuario genera el par de llaves pública y privada, y se envía la llave pública a Acepta.com siguiendo el estándar PKCS#10. En Acepta.com se transforma el archivo PKCS#10 en un certificado X.509 y este es enviado de vuelta al usuario en formato PKCS#7. El proceso concluye cuando el certificado X.509 queda registrado en el dispositivo del usuario.

El archivo enviado a Acepta.com no contiene la llave privada del usuario. Acepta.com no manipula las llaves privadas de los usuarios en ningún momento.

3.2.- Pérdida del PIN del usuario

Si el usuario olvida o pierde su PIN (password de activación), el personal de Acepta.com no cuenta con lo medios para modificarlo, esto es por razones de seguridad. Entonces, se debe repetir el registro presencial y definir un nuevo PIN.

El costo de este registro presencial debe ser cancelado por el usuario, pero el valor cancelado previamente por los servicios de certificación no será cobrado nuevamente. Acepta.com publica en su lista de precios el valor de un registro presencial sin servicios de certificación incluidos.

3.3.- Renovación de Certificados

Los certificados tendrán un período de vigencia que será indicado en el mismo certificado emitido. Dichos certificados caducarán automáticamente al finalizar este período y de pleno derecho ocasionando la invalidez del certificado, el cese permanente de su operatividad y el término de la prestación de los servicios de certificación prestados por Acepta.com.

Durante el período de vigencia y también una vez que haya expirado el certificado, el titular podrá siempre solicitar otro certificado sin necesidad de repetir el registro presencial. El titular podrá enviar un e-mail firmado electrónicamente solicitando un nuevo certificado o conectarse a una página Web usando su password de activación.

En ambos casos, el usuario recibirá un e-mail de Acepta.com comunicándole un nuevo número de solicitud. Con este número de solicitud, su password de activación y su fecha de nacimiento podrá crear un nuevo certificado.

Acepta.com no implementa métodos de renovación de certificados que permitan conservar las claves públicas y privadas de otros certificados.

3.4.- Solicitud de revocación

La revocación de un certificado es un estado permanente que no puede ser modificado.

Para solicitar la revocación de un certificado, el titular deberá enviar un e-mail firmado con firma electrónica avanzada a la casilla info@acepta.com.

Si el titular desea revocar un certificado distinto del usado para firmar el e-mail con la solicitud, entonces deberá señalar en el cuerpo del e-mail cual es el tipo y número de serie del certificado que desea revocar.

Acepta.com enviará al usuario un e-mail de confirmación de lectura cuando se haya recibido la solicitud y un segundo e-mail avisando cuando se haya procesado la solicitud. El plazo transcurrido entre la recepción de la solicitud y su procesamiento no podrá ser superior a 6 horas, considerando lunes a domingo de 9:00 a 19:00 horas.

Las solicitudes de revocación no tendrán costo para el usuario cuando este envíe un e-mail firmado con firma electrónica avanzada.

Si el usuario pierde el control de la llave privada del certificado que desea revocar y no cuenta con otro certificado de firma electrónica avanzada, entonces deberá realizar otro registro presencial solicitando la revocación del certificado. En este caso, corresponderá cobrar por el registro presencial, pero no por el valor completo de la emisión de un certificado. Acepta.com publica en su lista de precios el valor de un registro presencial sin servicios de certificación incluidos.

3.5.- Solicitud de suspensión

La suspensión de un certificado es un estado temporal, después del cual el estado puede ser revocado permanentemente o puede recuperar su estado de vigente.

Para solicitar la suspensión de un certificado, el titular deberá enviar un e-mail simple a la casilla info@acepta.com, indicando el tipo de certificado y número de serie del certificado que desea suspender. La casilla de e-mail usada para este envío debe coincidir con la casilla del certificado.

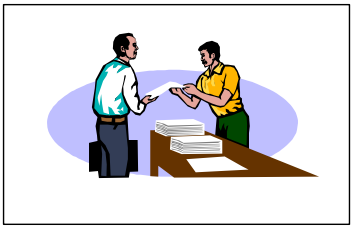
Acepta.com enviará al usuario un e-mail de confirmación de lectura cuando se haya recibido la solicitud y un segundo e-mail avisando cuando se haya procesado la solicitud. El plazo transcurrido entre la recepción de la solicitud y su procesamiento no podrá ser superior a 6 horas, considerando lunes a domingo de 9:00 a 19:00 horas.

Las solicitudes de suspensión no tendrán costo para el usuario.

4.- REQUERIMIENTOS OPERACIONALES

En este capítulo se describen los requisitos operativos pertinentes a las etapas de certificación, conducentes a la obtención de un certificado de persona de firma electrónica avanzada. Además, se describe el mecanismo de revocaciones y/o suspensiones, así como los procedimientos de auditoría y registros de datos aplicables.

Recepción Antecedentes

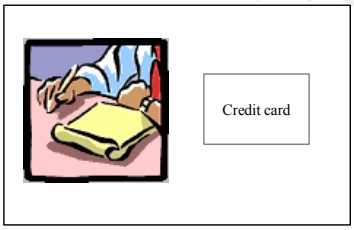


Persona acredita personalmente su identificación presentando su Cédula Nacional de Identidad, y proporciona otros antecedentes necesarios.

Registro Biométrico

Se toma fotografía y registra la huella digital de la persona

Firma de Contrato y Pago



Se firma "Contrato de Suscripción", y cancela valor del certificado, recibiendo el usuario un comprobante al respecto.

PIN y Nº Solicitud

Se le pide al usuario que proporcione una clave de activación (PIN), y se genera un Nº de solicitud, el cual una ves aprobada la emisión se le envía al suscriptor por e-mail. Luego necesitará éstos datos para instalar su certificado.

Fin Registro

Se entrega al suscriptor el Kit de Identidades digitales, el que contiene un instructivo de instalación , Licencia y manual de uso del software Acepta.exe, y una copia de las CPS

4.1.- Solicitud de Certificados

La solicitud de certificados de firma electrónica avanzada puede ser hecha a través de cualquier medio. La exigencia de Acepta.com es que se realice un registro presencial, después del cual, se tengan los siguientes datos del solicitante:

- Datos que se incluirán en el certificado
  - RUN: Rol Único Nacional emitido por el Servicio de Registro Civil e Identificación.
  - Nombres y apellidos, tal como aparecen en la cédula de identidad o pasaporte. Por razones de compatiblidad con X.509v3, las letras acentuadas son reemplazadas por letras sin acento y las "ñ" son reemplazadas por "n".
  - Dirección de correo electrónica.
  - Título o profesión, tal como aparece en la cédula de identidad.
- Datos para validar los antecedentes del solicitante

  Si el registro presencial es hecho por un operador de registro de Acepta.com se capturan los siguientes datos:
  - Imagen escaneada de la cédula de identidad por ambos lados.
  - Foto del solicitante.
  - Contrato de suscripción, con firma manuscrita e impresión dactilar.

  Si el registro presencial es hecho por un funcionario del Registro Civil, se envían los siguientes datos a Acepta.com[8]:
  - RUN
  - Nombres
  - Fecha de nacimiento
  - Foto en formato digital
  - Impresión dactilar en formato digital
  - Digitalización de firma manuscrita
  - Copia de un comprobante en papel firmado en forma manuscrita por el solicitante

[8] Los datos son enviados firmados electrónicamente y cifrados.

- Contraseñade activación
  - Si el registro presencial es hecho por un operador de registro de Acepta.com, entonces el solicitante debe digitar 2 veces una contraseña de activación. La contraseña de activación es almacenada usando una transformación hashing, por lo que ninguna persona o proceso de Acepta.com tiene acceso a la contraseña digitada por el usuario.
  - Si el registro presencial es realizado por un funcionario del Registro Civil, entonces la contraseña de activación es generada en forma aleatoria por el sistema y se le entrega al solicitante impresa en un comprobante asociado a la solicitud. Esta contraseña es enviada cifrada a Acepta.com.
- Datos requeridos para apoyar el proceso de certificación
  - Datos de contacto
  - Información de pago

La recopilación de los antecedentes del individuo se realiza por medio del software desarrollado por Acepta.com denominado *Registro.exe*©, el cual se encarga de adjuntar toda la información necesaria, y posteriormente enviar dicha información al Prestador de Servicios de Certificación correspondiente, para su validación y emisión del certificado requerido.

El programa *Registro.exe*©, realiza toda su operación de una manera segura. Cada operador que utilice el programa debe firmar electrónicamente todos los datos capturados con un certificado de firma electrónica avanzada, emitida por Acepta.com, para dichos fines. Los datos de registro firmados por un operador de registro se denominan solicitud electrónica de firma avanzada. Las solicitudes son enviadas de manera cifrada a Acepta.com, lo que garantiza que se mantiene la autenticidad, integridad y confidencialidad de dicha información durante todo el proceso.

4.2.- Validación y aprobación de certificados

Luego que los antecedentes del suscriptor son remitidos a Acepta.com, se procede a su validación central, necesaria para verificar la consistencia de dichos antecedentes en relación con la solicitud de certificado correspondiente. Para ello, un operador de validación[9] obtiene y revisa las solicitudes pendientes, corroborando la siguiente información:

- Cuando el registro presencial fue hecho por un operador de registro

[9] No se permite que la misma persona sea operador de registro y operador de validación.

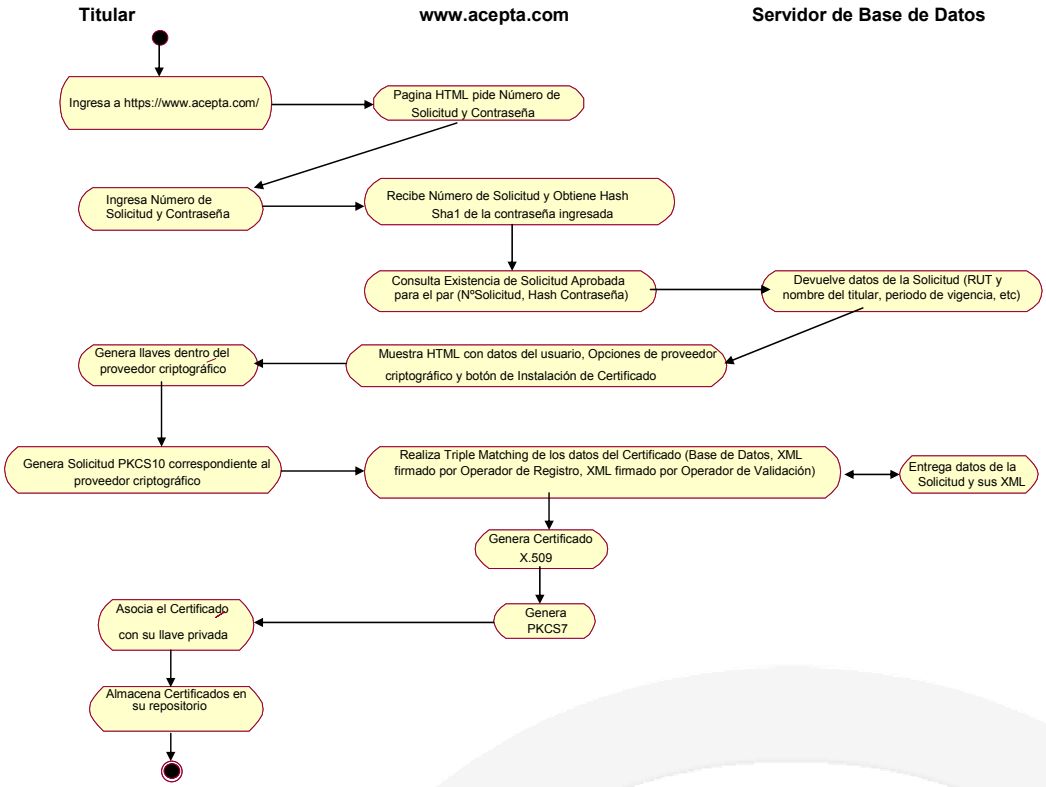
- Verifica que la información del nombre y RUN asociados a la solicitud correspondan con las copias electrónicas de la Cédula Nacional de Identidad.
- Verifica que el nombre, RUN, y dirección de e-mail de la solicitud correspondan a los datos estipulados en la copia electrónica del contrato del suscriptor.
- Verifica que la copia electrónica del contrato de suscripción este debidamente firmada y con impresión dactilar, y que dicha firma corresponda a la de la Cedula Nacional de Identidad.

- Cuando el registro presencial fue hecho por un funcionario del registro civil
  - Verifica que los datos recibidos estén completos y no tengan problemas de formato.

Si las validaciones anteriores son exitosas, entonces el operador aprueba la solicitud, con lo que se envía automáticamente un e-mail al suscriptor con el Número de la solicitud y notificando que ésta ha sido aprobada. Esta etapa además sirve como forma de verificación de la casilla de e-mail declarada por el solicitante, ya que sin este número de solicitud no se podrá emitir el certificado.

4.3.- Emisión e instalación

El proceso seguido para la emisión, recuperación e instalación de un certificado de firma avanzada es descrito a continuación:



Una vez que el suscriptor ha recibido por e-mail la notificación de que su solicitud de certificado ha sido aprobada, éste debe conectarse a una página web de emisión de certificados ubicada en:

www.acepta.com → Servicios On Line → Instalar Certificado

Advertencia de Seguridad 1: El usuario debe escribir la dirección de la portada de Acepta.com directamente en el Browser, **NUNCA DEBE USAR UN LINK INCLUIDO EN ALGUN E-MAIL**, podría ser una página caza password.

Advertencia de Seguridad 2: La página de emisión de certificados cuenta con una conexión segura según el estándar SSL. El usuario debe verificar que el certificado de la página esté firmado por Acepta.com. Lamentablemente, la única forma completamente segura de revisar esto, es asegurándose de que la llave pública de la raíz de Acepta.com (Acepta.com Autoridad certificadora raíz) coincida con lo siguiente:

```
30 82 01 08 02 82 01 01 00 c1 18 43 f3 7c b3 d3 c3 46 b4 5a a8 a6 c7 18 39 4d f4 b3
fb f8 4d c7 27 43 e8 03 22 ba 80 e2 57 c9 57 91 64 72 c0 d5 50 d2 e4 82 66 48 a9 9c
e4 12 bc f0 3b 6b 8e 29 00 d1 a5 ec ef a0 04 01 24 cf 72 fb a1 d4 af b2 41 16 7d 30
```

```
53 df 06 ec 45 91 6c 8b 4e 85 c7 91 6a b9 89 ad 96 d1 81 b2 04 88 24 6b dc dd 70 29
9d 2a bf 29 8e 80 2e 3e 0c 4c 7d 5a 3b df 02 95 7a 62 62 8e 30 c6 d6 2a 38 a9 47 37
47 2f 48 94 2d 55 da 7e bc e1 44 80 fa 06 70 d1 89 b1 ed ce 04 4c 87 e8 cb 95 31 21
5c d0 8a 4b e6 a9 0f 2b bb f5 c0 f5 0e 6b c6 6f 40 02 d3 b9 ea 04 cc bc fe ba b2 e5
3f c3 02 05 91 a3 54 39 b9 d6 16 fd ac ec d1 5f 1d 33 89 de b3 73 06 09 d8 1d 3c 18
5f 02 92 d4 d4 19 76 c3 8f ca 4e f8 8a 08 e6 54 f4 e1 05 a7 12 b5 36 d3 1f dd 54 67
f8 46 71 50 78 21 c5 94 b5 bd c7 d6 6b 02 01 03.
```

Luego, el suscriptor deberá proporcionar la clave de activación (definida en el registro presencia) y el número de solicitud (recibido por e-mail).

Todos los datos digitados por el usuario son enviados de manera segura (cifrada) al sitio de Acepta.com a través de Internet, en donde se realiza la validación necesaria para comprobar que dichos datos correspondan efectivamente a una solicitud previamente requerida, y que hasta ese momento se encuentra en estado pendiente y aprobada. Esto garantiza que el certificado será instalado sólo en el equipo del suscriptor que corresponde a la solicitud, y cuyos antecedentes de registro se encuentran en Acepta.com**.**

Siguiendo con el proceso, Acepta.com le envía al usuario una página con los antecedentes del certificado requerido y se los presenta al usuario para su confirmación.

Si el usuario acepta, se genera el par de llaves pública y privada, lo que es realizado íntegramente en el equipo computacional del suscriptor, dentro del dispositivo de almacenamiento de llaves privadas.

La clave pública generada es enviada de manera segura al sitio de Acepta.com. la información correspondiente de la llave pública, se transmite usando el formato estándar PKCS#10.

En los servidores de Acepta.com se prepara un certificado en formato X.509v3 se envía a servidores de firma. Los servidores de firma son administrados con los más altos niveles de seguridad y no tienen acceso a Internet.

Antes de firmar el certificado X.509v3, en los servidores de firma se realiza un “Triple matching", el cual valida los siguientes elementos:

- Que los datos del certificado que se generará coincidan con los datos de la base de datos que apoyan los procesos de Acepta.com. Esto se hace indirectamente al usar los datos de la base de datos de Acepta.com para preparar el archivo X.509v3 y tomar sólo la clave pública del archivo PKCS#10.
- Que los datos del certificado que se generará coincidan con una solicitud de registro firmada con la firma electrónica avanzada de un operador de registro autorizado por Acepta.com.

- Que los datos del certificado que se generará coincidan con una autorización firmada con la firma electrónica avanzada de un operador de validación central autorizado por Acepta.com.

La lista de Operadores de Registro y Operadores de Validación autorizados por Acepta.com se encuentra firmada por la AC intermedia de Acepta.com y es generada con los mismos estándares de seguridad con los que se generan los certificados de las Autoridades Certificadoras intermedias de Acepta.com.

Si estas 3 verificaciones resultan exitosas, se firma el certificado X.509v3 y es enviado como respuesta al browser del usuario.

Posteriormente dicho certificado es instalado en el dispositivo de almacenamiento de llave privada de Acepta.com.

4.4.- Proceso de suspensión y revocación de certificados

Los certificados de firma electrónica avanzada podrán ser revocados en las siguientes circunstancias:

- Cuando el titular o dueño del certificado lo solicite en conformidad con los procedimientos indicados en el punto 3.4 y 3.5 sobre revocación y suspensión de certificados. Se entiende por dueño aquella persona natural o jurídica que contrató los servicios de certificación.
- Por fallecimiento del titular.
- Por resolución judicial ejecutoriada.
- Por incumplimiento de las obligaciones del usuario establecidas en la Ley 19.799 artículo 24.
- Cuando no se hayan cancelado los servicios de registro presencial y vigencia del certificado.

Frente a cualquiera de estas circunstancias, un operador de validación de Acepta.com podrá ingresar a una aplicación especial y firmar electrónicamente la autorización de revocación.

Esta aplicación alimenta la base de datos de Acepta.com con la que se generan las listas de revocación (CRL) y respuestas a consultas en línea, ya sea a través del sitio web o de OCSP.

4.4.1.- Causales y procedimientos para revocar o suspender

Los certificados de firma electrónica avanzada podrán ser revocados en las siguientes circunstancias:

• Cuando el titular o dueño del certificado lo solicite en conformidad con los procedimientos indicados en el punto 3.4 y 3.5 sobre revocación y suspensión de

certificados. Se entiende por dueño aquella persona natural o jurídica que contrató los servicios de certificación.

• Por fallecimiento del titular.

• Por resolución judicial ejecutoriada.

• Por incumplimiento de las obligaciones del usuario establecidas en la Ley 19.799 artículo 24.

• Cuando no se hayan cancelado los servicios de registro presencial y vigencia del certificado.

Frente a cualquiera de estas circunstancias, un operador de validación de Acepta.com podrá ingresar a una aplicación especial y firmar electrónicamente la autorización de revocación.

Esta aplicación alimenta la base de datos de Acepta.com con la que se generan las listas de revocación (CRL) y respuestas a consultas en línea, ya sea a través del sitio web o de OCSP.

.

4.5.- Procedimientos de auditoria de seguridad

Los mecanismos de auditoria son los mismos para todos los tipos de certificado, y están estipuladas en las CPS.

4.6.- Políticas para archivo de registros

Las políticas para archivo de registros son las mismas para todos los tipos de certificado, y están estipuladas en las CPS.

4.7.- Procedimientos de auditoria de seguridad

Los procedimientos de auditoria de seguridad son los mismos para todos los tipos de certificado, y están estipuladas en las CPS.

5.- CONTROLES DE PROCEDIMIENTO, PERSONAL Y FÍSICOS

Los controles y procedimientos establecidos para garantizar una operación de los servicios de certificación bajo un ambiente seguro, desde el punto de vista de la seguridad de las dependencias físicas, las conductas y capacidad del personal, así como las capacidades de recuperación frente a desastres, está establecido en las CPS de Acepta.com. Dichos controles se aplican por igual para la emisión de todos los tipos de certificados.

6.- CONTROLES DE SEGURIDAD TÉCNICA

En este capítulo se describen una serie de controles de carácter técnico que permiten mantener un ambiente de operación seguro, tanto en la generación y administración de los certificados de firma electrónica avanzada y llaves asociadas.

6.1.- Generación e instalación del par de llaves del usuario

En el capítulo 4 de estas políticas se explica el procedimiento seguido para generar y entregar el certificado y sus llaves al usuario.

6.2.- Entrega de la llave pública de Acepta.com a usuarios

En las CPS de Acepta.com se establecen los procedimientos generales de distribución de las claves públicas de Acepta.com.

Adicionalmente, en el caso de certificados de firma electrónica avanzada, se puede descargar desde el sitio web de la entidad acreditadora de Chile en www.entidadacreditadora.cl, donde se encuentran los certificados intermedios de todos los Prestadores de Servicios de Certificación Acreditados.

Los usuarios que deseen realizar una inspección visual para validar la llave pública del certificado Raíz de Acepta.com pueden consultar en las CPS de Acepta.com el texto a comparar.

6.3.- Tamaño de las claves

EL tamaño de las llaves y el período de vigencia de los certificados de AC Intermedias de Acepta.com está indicado en las CPS de Acepta.com.

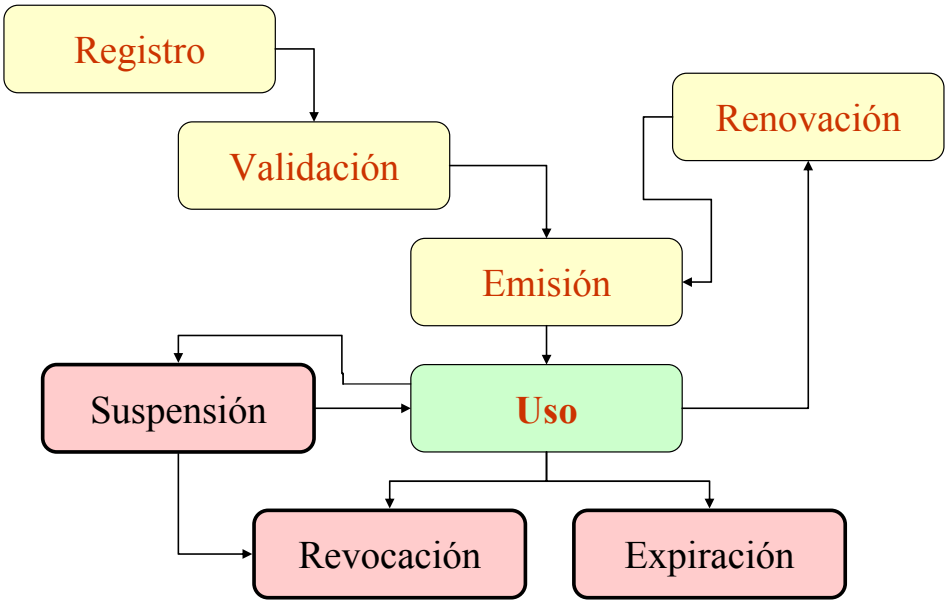
6.4.- Datos de activación

Para los certificados de firma electrónica avanzada, al momento de emitir el certificado, el suscriptor debe ingresa un número de solicitud, fecha de nacimiento y contraseña o clave de activación.

El titular del certificado es responsable de administrar bajo su exclusivo control la contraseña de activación de su certificado.

6.5.- Ciclo de vida de un Certificado

El siguiente diagrama resume el ciclo de vida de los certificados de firma electrónica avanzada explicados en estas políticas de certificación:



7.- PERFILES DE CERTIFICADOS Y DEL REGISTRO DE ACCESO PÚBLICO

Este capítulo contiene especificaciones detalladas de los formatos y contenido de los certificados de firma electrónica avanzada (campos, básicos y extensiones). Además se especifica el formato de las listas de revocación (CRL).

7.1.- Composición básica de los certificados

Los certificados de firma electrónica avanzada emitidos por Acepta.com están en conformidad con el formato X.509v3 definido en ITU-T X.509v3 y las recomendaciones de la IETF RFC-3280.

Campo	Descripción	Ejemplo
Versión	Versión del certificado, que deberá ser versión 3	v3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los emitidos por Acepta.com	0090 0001
Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	SHA-1 WithRSAEncryption
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 = e-mail del Prestador de Servicios de Certificación Número de serie = Número identificador del certificado, se utiliza el RUT de Acepta.com. C = País	CN = Acepta.com Autoridad Certificadora Firma Electronica Avanzada E = info@acepta.com SN = 96919050-8 C = CL
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. Para PSC = 10 años, Para suscriptores = 1 a 3 años, Codificado en formato YYMMDDHHMMSSZ	Fecha inicio = 040914140522Z Fecha termino = 050914140522Z
Nombre del titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN = Nombre distintivo del suscriptor T = Profesión E = dirección de correo del suscriptor Número de serie = Número identificador del certificado. Se utiliza el RUT del titular del certificado. C = País	CN = ENRIQUE EDUARDO VELASCO AGUIRRE T = INGENIERO CIVIL E = enrique.velasco@acepta.com SN = 9832793-2 C = CL
Clave pública	Clave pública del titular del certificado	3081 8902 8181 009D ECC1 62F4 FE2D 73DD BE6D 53C3 E578 7F98 38AE ED42 B03D A804 F4D5 CA86 9563 2757 D556 7A4F 0C94 DBBA 8F4E 80B0 C334 6B01 B85D 1872 635F 40C3 F294 24E9 FD92 C97A D3B4 798E 680C 7F92 5889 4786 41DC 1AB0 80D4 CCDE 1280 9334 90F1 A1BE 9E96 72AF AA28 3BEA 2DCC 13BC 685C 7782 E869 A7C4 98B6 9094 43FF 574F 3025 5A2C 8880 3F02 0301 0001

Tabla 1: Composición básica del certificado

7.1.1.- Formato del certificado intermedio

Campo	Descripción	Ejemplo
Versión	Versión del certificado, que deberá ser versión 3	v3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los certificados de firma electrónica avanzada emitidos por Acepta.com.	03
Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	SHA-1 WithRSAEncryption
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 = e-mail de el Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor C = País	CN = Acepta.com. Firma Electronica Avanzada Test CA E = info@acepta.com SN = 96919050-8 C = CL
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. Para PSC = 10 años, para suscriptores = 1 año, para servidores = 2 años. Codificado en formato YYMMDDHHMMSSZ	Fecha inicio = 040201000000Z Fecha termino = 130201000000Z
Nombre del titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN = Nombre distintivo del suscriptor T = Profesión E = dirección de correo del suscriptor C = País	CN = Acepta.com Autoridad Certificadora Firma Electronica Avanzada de Prueba E = info@acepta.com SN = 96919050-8 C = CL
Clave pública	Clave pública del titular del certificado	3081 8902 8181 008D E0D1 13C5 E736 969C 8D2B 047A 243F 8FE1 8EDA D64C DE9E 842D 3669 230C A486 F7CF DDE1 F8EE C54D 1905 FFF0 4ACC 85E6 1093 E180 CADC 6CEA 407F 193D 44BB 0E94 49B8 DBB4 9784 CD9E 3626 0C39 E06A 9472 9997 8C6E D830 0724 E887 198C FEDE 20F3 FBDE 658F A2BD 078B E946 A392 BD34 9F2B 49C4 86E2 0C40 5588 E306 706C 9017 308E 6902 0300 FFFF

Tabla 2: Formato del certificado intermedio

7.1.2.- Extensiones

Los certificados de firma electrónica avanzada emitidos por Acepta.com contemplan un número de extensiones para mejorar la aplicabilidad.

Éstas pueden ser extensiones estándar o extensiones privadas. Las primeras corresponden a aquellas definidas en el estándar X.509v3, y las segundas corresponden tanto a extensiones de uso privado definidas por Acepta.com, o a extensiones definidas por diferentes organismos y las cuales se soportan para efectos de compatibilidad.

A continuación se detallan las extensiones incluidas en los certificados de firma electrónica avanzada.

Nombre	Descripción	OID	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.	2.5.29.15	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (F0).
BasicConstrains	Permite diferenciar entre un certificado de PSC y uno de suscriptor final.	2.5.29.19	Tipo de asunto = Entidad final Restricción de longitud de ruta = Ninguno
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 definidos por esta extensión.	2.5.29.37	Autenticación del cliente(1.3.6.1.5.5.7.3.2) Correo seguro(1.3.6.1.5.5.7.3.4)
AuthorityKeyIdentifier	Medio para identificar la llave pública de Acepta.com El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier		Id. de clave = 5c 5c c7 9a 2a 29 3d 02 30 07 88 43 d8 fa 85 5d 52 6c 51 15
SubjectKeyIdentifier	Identificador único de la llave pública de el PSC, conteniendo el hash de 160bit de la llave pública.		85 f9 cd e2 9f b2 57 fc 58 b3 d2 e6 a2 3e a7 2b 56 42 3d e1
CertificatePolicy	Ver sección 7.1.6		[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.6891.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: http://www.acepta.com/CPS/ [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Referencia de aviso: Organización=Acepta.com S.A. Número de aviso=1

			Texto de aviso=La utilización de este certificado esta sujeta a las políticas de certificado (CP) y prácticas de certificación (CPS) establecidas por Acepta.com, y disponibles públicamente en www.acepta.com.
IssuerAltName	Identificador alternativo del emisor, corresponde al RUT de Acepta.com, en formato análogo a SubjectAltName		Otro nombre: 1.3.6.1.4.1.8321.2 = 16 0c 39 36 2e 39 31 39 2e 30 35 30 2d 38
SubjectAltName	Permite definir términos que identifican al sujeto o titular del certificado, adicionalmente a lo establecido en el campo estándar Subject. Se podrán registrar los siguientes campos adicionales: OtherName: Para certificados de identidad de individuos, aquí se registra el RUT, en la siguiente estructura: Type-id = 1.3.6.1.4.1.8321.1 Value =’xx.xxx.xx-v’ El campo Value es un IA5String con el RUT del individuo titular del certificado. Se incluye el correo electrónico del sujeto como estándar RFC822 Se Incluye el RUT del sujeto en formato de Permanent Identifier utilizando el OID 1.3.6.1.4.1.8321.1 como identificador del RUT		Otro nombre: 1.3.6.1.4.1.8321.1 = 16 09 39 38 33 32 37 39 33 2d 32 Nombre RFC822 = enrique.velasco@acepta.com Otro nombre: 1.3.6.1.5.5.7.8.3 = 30 15 0c 09 39 38 33 32 37 39 33 2d 32 06 08 2b 06 01 04 01 c1 01 01
CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la sgte. estructura: DistribuitonPoint: Un URI para identificar el CRL	2.5.29.31	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://crl.acepta.com/FA.crl
AuthorityInfoAccess	En esta extensión se establece información de acceso a servicios de información de el Prestador de Servicios de Certificación. En este momento, establece el acceso para consultas de revocaciones on-line. Contiene la siguiente estructura: AccessMethod: OID identificando el método de acceso. En este caso, corresponde al protocolo OCSP, con OID=13.6.1.48.1 AccessLocation: Ubicación del servicio de consulta OCSP	13.6.1.5.5.7.1.1	[1]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea(1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://ocsp.acepta.com/

Tabla 3: Extensiones del certificado

7.2.- Composición de la lista de revocación (CRL)

Las listas de revocación de los certificados de firma electrónica avanzada emitidos por Acepta.com están en conformidad con el formato CRLv2 definido en ITU-T X.509v3 y las recomendaciones de la IETF RFC-3280.

Nombre	*Descripción*	*Valor*
Versión	Corresponde a versión 2	2
Issuer	Descripción de el Prestador de Servicios de Certificación emisora de la CRL	CN = Acepta.com Autoridad Certificadora Firma Electronica Avanzada de Prueba E = info@acepta.com Número de serie = 96919050-8 C = CL
Effective Date	Fecha de publicación de la CRL	040914140733Z
Next Update	Fecha de próxima publicación	040915140733Z
Signature algorithm	Algoritmo DE firma de la CRL	Corresponde a Sha1RSA

Tabla 4: Composición de la lista de revocación

Acepta.com usa las siguientes extensiones en las listas de revocación de certificados de firma electrónica avanzada:

Nombre	Descripción
AuthorityKeyIdentifier	Identificador de la clave de el Prestador de Servicios de Certificación

Tabla 5: Extensiones de las listas de revocación

8.- ESPECIFICACIONES DE ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

Este capítulo contiene una descripción de los procedimientos aplicables para las subsecuentes modificaciones de las políticas de certificado de firma electrónica avanzada.

8.1.- Procedimientos para cambios en las CP

Estas políticas son administradas y mantenidas rigurosamente por personal especializado y en posiciones de confianza en la compañía.

8.2.- Publicación y notificación

Cualquier cambio en el contenido de estas CP será comunicado al público y usuarios mediante su publicación en el sitio Web de Acepta.com en www.acepta.com/CPS.

8.3.- Procedimientos de aprobación de las CP

Estas CP y las subsecuentes versiones futuras de éste documento están sujetas a la aprobación del Directorio de Acepta.com.