POLÍTICAS PARA CERTIFICADOS (CP) CLASE 3

PERSONA NATURAL

Versión 1.0

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

©2001-2000 ACEPTA.COM, TODOS LOS DERECHOS RESERVADOS

TABLA DE CONTENIDO

ÍNDICE DE TABLAS Y FIGURAS

AGRADECIMIENTOS

Se reconoce la participación en la creación, desarrollo y revisión de este documento al Sr. Roberto Opazo Gazmuri, Director y Gerente General de **Acepta.com**, y al Sr. Juan Carlos Pérez Aguayo, Gerente de Tecnología de **Acepta.com**.

1 INTRODUCCIÓN

En este documento se definen y detallan las políticas de certificado aplicables a los certificados de clase 3 persona natural, emitidos por **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 Sobre las Políticas de certificados

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".

Una explicación detallada de las prácticas que Acepta.com emplea para emitir y gestionar certificados, y que implementa y soporta los requerimientos de estas políticas de certificado, se encuentra en el documento "Prácticas de Certificación (CPS) de Acepta.com".

Estas políticas de certificado o CP, en conjunto con las CPS, son los únicos instrumentos que establecen las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión, y revocación de los certificados, así como las restricciones y aplicaciones en las cuales se deben utilizar dichos certificados clase 3 de persona natural.

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, detallándose los aspectos pertinentes a los certificados clase 3 de persona natural.

1.2 Identificación

El presente documento se denomina "Políticas de Certificado de clase 3 persona natural de Acepta.com", las que internamente se citan como CP.

1.3 Comunidad de usuarios y utilización de los certificados

Los certificados digitales de clase 3 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 presentación en persona del suscriptor junto con su Cédula Nacional de Identidad.

- **Integridad de mensajes:** los mensajes firmados con identidades digitales de clase 3 de persona natural permiten validar si el contenido de mensaje ha sido alterado en el tiempo transcurrido entre su envió y su recepción efectiva,
- **Firmas digitales:** las firmas digitales producidas con identidades de clase 3 persona natural ofrecen los medios de respaldo frente a que una persona deniegue de la autoría y contenido de un mensaje en particular, sí dicha persona a firmado digitalmente dicho mensaje.
- **Privacidad:** las identidades digitales de clase 3 persona natural permiten cifrar mensajes de forma que al ser transmitidos sean solo observados por el remitente correspondiente.

Estos certificados pueden ser utilizados en los siguientes campos de aplicación general, sin excluir otros posibles usos específicos:

- Certificado para identificación de persona
- Certificado para uso en la banca
- Certificado para importar y exportar
- Certificado para declaraciones previsionales
- Certificado para uso comercial
- Certificado para pago tributario
- Certificado para pagos
- Certificado para otros usos reconocidos por las partes de procesos en la red
- Certificado para uso tributario

En una extensión del propio certificado, para visualización y conocimiento por parte de quien use dicho certificado, se muestra una notificación descriptiva sobre su uso (ver Cap. 7 sobre extensiones)

Por otro lado, también se incluye en el certificado emitido una extensión con un "comentario del suscriptor", en donde el suscriptor puede registrar alguna observación que él requiera que aparezca en el certificado. Esta información puede ser proporcionada en el momento de solicitar el certificado en **Acepta.com**, autoridad de registro, o certificadora acreditada.

La información de "comentario del suscriptor" es incorporada al certificado sólo como referencia; ni **Acepta.com** ni sus Autoridades de Registro o Autoridades Certificadoras acreditadas por **Acepta.com** asumen compromiso o avalan la fiabilidad de la información anterior que declare el suscriptor. No se realiza ningún tipo de validación respecto a dicha información, por lo que su veracidad y validez es de exclusiva responsabilidad del suscriptor.

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) 688 64 99

Fax: +56 (2) 672 90 87

e.-mail: info@acepta.com

Web : http://www.acepta.com

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 clase 3 persona natural, 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 como autoridad certificadora

Acepta.com, en su calidad de Autoridad Certificadora, se obliga a cumplir los requerimientos detallados en las CPS de Acepta.com. Específicamente, al emitir certificados de clase 3 persona natural se obliga a lo siguiente:

- Resguardar una copia electrónica fiel de la Cédula Nacional de Identidad por ambos lados, y del contrato de suscripción firmado con la huella holográfica del suscriptor.
- Resguardar una copia electrónica de la solicitud de revocación cuando se solicite, el la cual se especificará la fecha y hora en que se recibió dicha solicitud
- Resguardo de un registro electrónico con la lista de los certificados revocados y/o suspendidos, el cual puede ser consultado públicamente
- 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 mantenidas por **Acepta.com**.

2.1.2 Obligaciones de autoridades de registro o certificadoras acreditadas

Cada AR o AC acreditada por Acepta.com deberá cumplir las normas y ser consistente con lo establecido en las CPS de Acepta.com.

2.1.3 Obligaciones de los suscriptores

Los suscriptores que soliciten certificados de clase 3 de persona a **Acepta.com**, se obligan a cumplir con los siguientes requerimientos:

- 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 o alguna de sus AC acreditadas.
- Conocer y aceptar el propósito y alcance de un certificado obtenido en **Acepta.com** o en alguna Autoridad Certificadora acreditada, acorde a lo estipulado en este documento, y a las prácticas de certificación definidas por Acepta.com. Particularmente, en caso que el suscriptor hubiese definido un monto máximo de responsabilidad para uso de su certificado en transacciones comerciales, se obliga a no utilizarlo en transacciones que excedan dicho valor, el cual queda registrado en el propio certificado.
- Al solicitar su certificado, presentar su Cedula Nacional de Identidad original emitida por el Servicio de Registro Civil e Identificación del Estado de Chile, y firmar el contrato de suscripción con la firma que corresponda a su CNI.
- Protección de la clave de activación o PIN, definida y digitada por el mismo suscriptor en el proceso de 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.
- Notificación a Acepta.com (o la Autoridad de Registro, o Autoridad Certificadora acreditada correspondiente) de cualquier modificación de sus antecedentes, que como consecuencia pudiese invalidar uno o más certificados para tal suscriptor.

2.1.4 Obligaciones de usuarios de certificados

Los usuarios de certificados emitidos por Acepta.com, o cualquier entidad que deposite su confianza en dichos certificados, se obligan a cumplir lo s requerimientos comunes estipulados en las CPS.

2.1.5 Obligaciones respecto a publicación de información de certificados y revocaciones

Corresponden a los requerimientos comunes establecidos en las CPS, sección 2.1.5.

2.2 Responsabilidades de Acepta.com como autoridad certificadora y de sus Autoridades acreditadas

2.2.1 Responsabilidades asumidas

Junto con las responsabilidades comunes especificadas en las CPS, Acepta.com es responsable de proporcionar los siguientes mecanismos de prueba, necesarios para dilucidar responsabilidades en caso de cualquier conflicto o perjuicio que se derive por la utilización de los certificados digitales de clase 3 de persona:

- Cuando un suscriptor acepta e instala un certificado recién emitido, queda registrado el período de validez de dicho certificado, tanto en el certificado mismo, como en el contrato de suscripción firmado por el suscriptor. Una copia digital de éste contrato es resguardada en Acepta.com.

- Si un usuario solicita revocar o suspender un certificado, queda un registro con la fecha y hora en que se realizó la notificación, ya sea vía e-mail o comprobante impreso si se solicitó personalmente. También queda registrada la fecha y hora a partir de la cual el certificado será publicado como inválido, no pudiendo superar ésta última a 12 horas desde la notificación. La fecha de revocación efectiva es comunicada al suscriptor vía e-mail firmado digitalmente.

- Si un usuario consulta por el estado de un certificado, y éste es reportado por Acepta.com - a través de una respuesta firmada digitalmente - erróneamente como válido, siendo que fue revocado previamente, fácilmente se puede determinar la responsabilidad de Acepta.com, contrastando dicha respuesta con el comprobante emitido por Acepta.com en el que se estipula a partir de que momento el certificado debiera haber sido reportado como revocado.

- Por otro lado, Acepta.com y sus AC acreditadas mantienen un registro con la firma manuscrita, huella holográfica y foto del suscriptor tomadas al momento de solicitar el certificado, como mecanismos de prueba de la identidad del suscriptor, ante cualquier situación de repudiación de la identidad asociada a un certificado digital.

2.2.2 Exclusiones de responsabilidad

Acepta.com no será responsable de cualquier perjuicio que derive de una utilización negligente o no acorde con las políticas establecidas en estas CP y las CPS por parte de los suscriptores o terceras partes interesadas.

2.3 Responsabilidades financieras

2.3.1 Indemnizaciones

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 de clase 3 de persona, 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, se establece que Acepta.com se hace responsable por la validez de dicha respuesta, y delimita su responsabilidad hasta 5000 US$ 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 aplican tanto para el suscriptor o signatario titular del mismo y del tercero o receptor confiado que acepte su valor y adhiera a estas CP.

2.4 Normas respecto a aplicabilidad de estas CP

Los estatutos legales que rigen la aplicabilidad de las Políticas de Certificado establecidas por Acepta.com están estipuladas en las CPS.

2.5 Tarifas

2.5.1 Tarifas para emisión de certificados

Las tarifas asociadas a la emisión de certificados están compuestas por 2 valores:

1.-Tarifa por recepción y validación de antecedentes, la cual eventualmente puede ser cancelada a una de las autoridades de Registro acreditadas, y

2.-Tarifa por la emisión, publicación y mantención de los certificados, que le corresponde a Acepta.com o a una AC acreditada por **Acepta.com**.

El usuario o suscriptor cancelara el valor total considerando ambos valores a la autoridad a quien solicite el certificado. En caso de solicitarse a una autoridad de registro acreditada, ésta cancelará posteriormente el valor de la emisión a la autoridad certificadora correspondiente.

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

2.6 Publicaciones

Acepta.com publica en su sitio Web en www.acepta.com, las políticas de certificado aplicaples a los certificados de clase 3 de persona, 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.

3 IDENTIFICACION Y AUTENTIFICACIÓN

En este capítulo se presentan las prácticas y especificaciones seguidas por Acepta.com y sus AR o AC acreditadas, para autentificar fielmente la identidad de las entidades a las cuales se le emitirá un certificado de persona de clase 3, previamente a la emisión propiamente tal.

3.1 Registro inicial

3.1.1 Tipos, interpretación y unicidad de nombres

En los certificados se incluirá el nombre completo de la persona estipulado en su Cédula Nacional de Identidad, así como el RUT, en un formato consistente con las especificaciones para certificados X.509v3.

El RUT es único para cada suscriptor de Acepta.com.

3.1.2 Método para probar posesión de la llave privada

La llave privada asociada a un certificado digital de clase 3 de persona emitido por **Acepta.com** o alguna de sus AC acreditadas es siempre generada exclusivamente en el equipo computacional del suscriptor del certificado.

Dicha llave es generada en el equipo del suscriptor por el programa *Acepta.exe*, durante el proceso de instalación del certificado. 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 se genera el par de llaves pública y privada, y se envía la llave privada a Acepta.com, la cual será la que aparezca en el certificado correspondiente.

3.1.3 Autentificación de identidades individuales

El instrumento principal para garantizar la identidad de los individuos que soliciten certificados es la Cédula Nacional de Identidad, cuya presentación (cédula vigente) será requisito fundamental previa a la emisión de cualquier certificado. Dicha cédula es otorgada por el Servicio de Registro e Identificación Civil del Estado de Chile.

Para todos los certificados de clase 3 de persona, se incluirá en los certificados emitidos el RUT correspondiente que aparece en la Cédula Nacional de Identidad, en una extensión del certificado. (mas detalles sobre los formatos de los certificado en la sección 7.1).

Adicionalmente, se requiere la presencia y concurrencia personal (física) de los individuos solicitantes. Dicha presencia se registrará mediante la huella dactilar, fotografía y firma ológrafa de la persona. Posteriormente, en la autoridad certificadora se validará que la Cédula Nacional de Identidad esté vigente y no bloqueada, consultando para ello a bases públicas como DICOM.

3.2 Renovación de Certificados

Los certificados tendrán un período de vigencia que será indicado en el contrato y en el mismo certificado emitido. Dichos certificados caducarán automáticamente al finalizar dicho 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 por **Acepta.com**.

Al vencimiento del certificado podrá el suscriptor o signatario titular renovarlo por un período de un año , en cuyo caso deberá así solicitarlo mediante e-mail dirigido al administrador del sitio de **Acepta.com** (e-mail: admin@acepta.com) con una antelación mínima de 30 días a la fecha de su caducidad, o llenando el formulario que al efecto se contenga en el sitio web de Acepta.com.

En el evento que hayan transcurrido más de cuatro (4) años desde la emisión del primer certificado, esto es, la emisión de un certificado y tres renovaciones posteriores, no se dará curso a una nueva solicitud de renovación y el suscriptor o signatario deberá solicitar un nuevo certificado.

La opción de renovación de certificados se establece para los casos en que un certificado vaya a caducar y el suscriptor o signatario quiera utilizar un certificado de las mismas características que el usado válidamente hasta esa fecha. Será responsabilidad del suscriptor, el informar a Acepta.com si algunos de los datos registrados o contenidos en el certificado anterior han cambiado.

3.3 Re-emisión de llaves después de una revocación

La revocación del certificado digital tiene como consecuencia principal la terminación inmediata del período operativo del certificado, el que legalmente pasa a ser "inválido".

La revocación del certificado digital acarrea como consecuencia, además, que no puedan crearse o generarse válidamente firmas digitales.

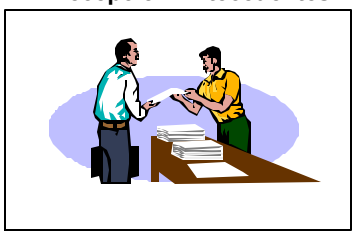
Los procedimientos aplicables para la revocación o suspensión de certificados se detallan en el punto 4.5.

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 clase 3. Además, se describe el mecanismo de revocaciones y/o suspensiones, así como los procedimientos de auditoría y registros de datos aplicables.

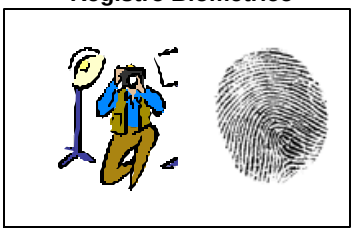
4.1 Requerimientos para solicitar certificados de clase 3 de persona

Recepción Antecedentes



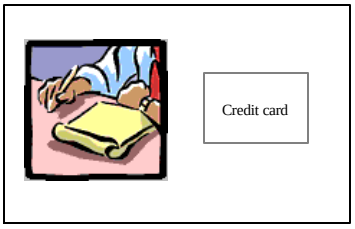
Persona acredita personalmente su identificación presentando su Cédula Nacional de Identidad, y proporciona otros antecedentes necesarios.

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

La información que el suscriptor debe proporcionar al solicitar un certificado de clase 3 de persona, así como el mecanismo de entrega de dichos antecedentes son los siguientes:

SOLICITUD DE CERTIFICADO CLASE 3 PERSONA	
INFORMACIÓN REQUERIDA	***RECEPCIÓN DE ANTECEDENTES***
Rol Único Tributario (RUT) del suscriptor Nombres y apellidos del suscriptor Calle, ciudad, país (de residencia) Número telefónico de residencia(opcional) Teléfono móvil (opcional) Dirección de correo electrónico Monto máximo de responsabilidad para el uso del certificado en transacciones comerciales (opcional) Comentario a incluir en el certificado (opcional)	El individuo debe presentarse personalmente en las oficinas de Acepta.com, de alguna Autoridad de Registro o Autoridad Certificadora acreditada por Acepta.com. Debe presentar el documento original del RUT.

Tabla Nº 1 – Solicitud de certificado clase 3 de persona

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 a la autoridad certificadora 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 se autentifica con una identidad digital especial, emitida por **Acepta.com** para dichos fines. Además, todos los antecedentes son firmados digitalmente con dicho certificado de operador, y enviados de manera cifrada a **Acepta.com**, lo que garantiza que se mantiene la autenticidad, integridad y confidencialidad de dicha información durante todo el proceso.

Luego de registrados todos los antecedentes de la persona, se incorporan en una solicitud de certificado, a la que se le asigna automáticamente un Nº de solicitud, el cual es único para cada certificado requerido, y que luego de aprobada la solicitud autorizando la emisión del certificado correspondiente, se notifica de tal aprobación al suscriptor vía e-mail adjuntando el Nº de la solicitud correspondiente. Por otro lado, en esta etapa de registro el individuo debe proporcionar una clave de activación o PIN, la cual es personalísima y confidencial. Este PIN, junto al Nº de solicitud serán requeridos posteriormente para poder instalar su certificado.

Cabe señalar que cada suscriptor que adquiera un certificado digital de identidad con **Acepta.com** obtiene una licencia del software *Acepta.exe*? , para apoyarlo en el proceso de instalación y posterior administración de sus certificados.

Para finalizar esta etapa, el suscriptor debe pagar el valor asociado al registro y emisión del certificado, así como firmar un "Contrato de suscripción", estampando en éste su firma y huella holográfica. Este documento es luego escaneado y registrado digitalmente junto con los otros antecedentes.

Dado que el proceso de registro inicial puede ser llevado a cabo tanto en una AC como en una AR acreditada por **Acepta.com**, en el caso que se realice mediante una autoridad de registro, ésta validará los antecedentes y los enviará posteriormente a la autoridad certificadora. Esto es realizado a través de

un canal seguro y con procedimientos previamente establecidos, los cuales deben estar en conformidad con las directrices estipuladas en éstas CPS.

4.2 Validación y aprobación de certificados

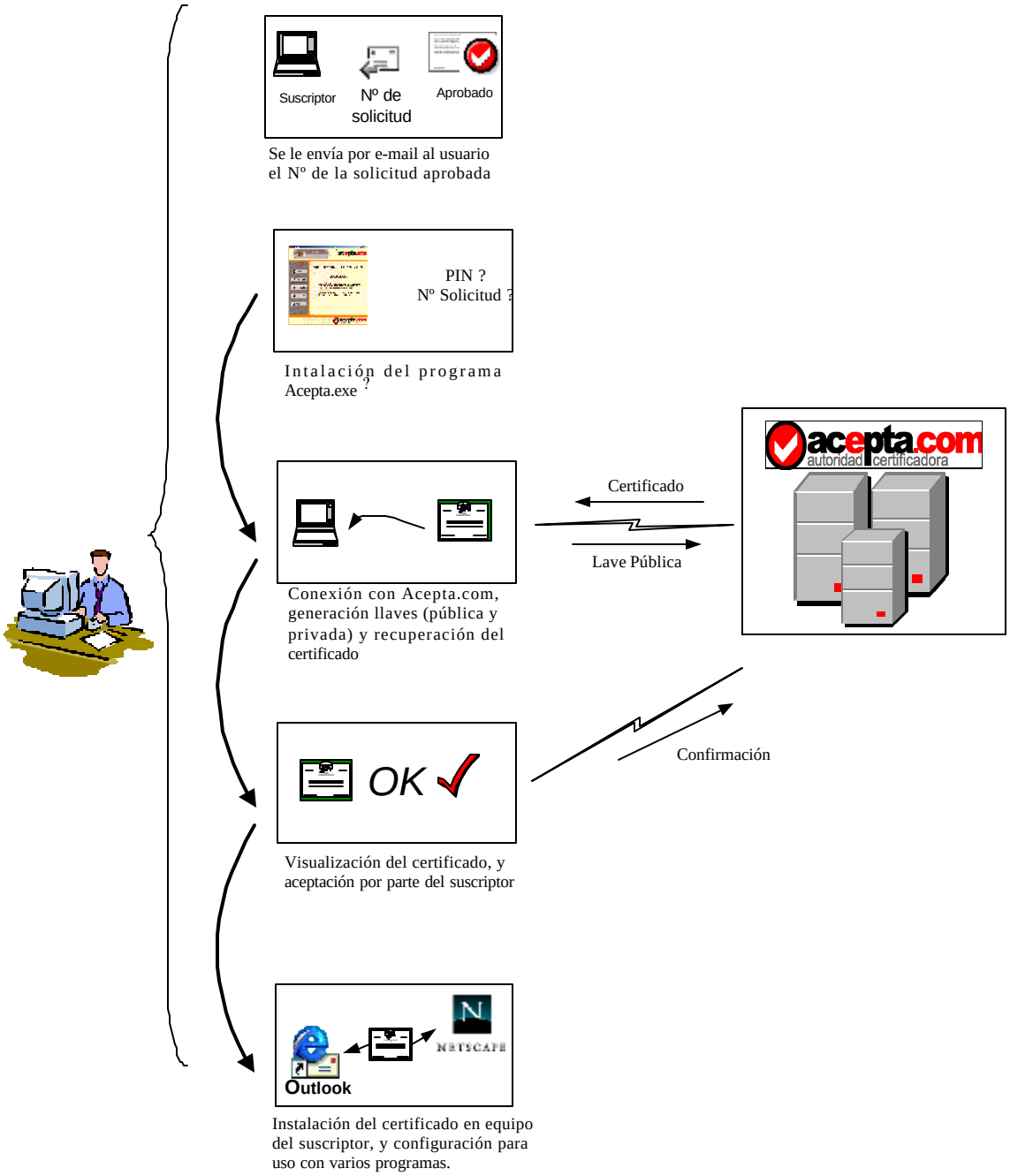
Luego que los antecedentes del suscriptor son remitidos a **Acepta.com**, se procede a su validación necesaria para verificar la consistencia de dichos antecedentes en relación con la solicitud de certificado correspondiente. Para ello, un operador calificado obtiene y revisa las solicitudes pendientes,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

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

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 Nº de la solicitud y notificando que ésta ha sido aprobada.

4.3 Emisión e instalación

El proceso seguido para la emisión, recuperación e instalación de un certificado de clase 3 de persona 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 procede a ejecutar el programa *Acepta.exe*? , para recuperar e instalar su certificado. Al iniciar el programa, éste se conecta automáticamente al sitio Web de **Acepta.com**, de donde obtiene y actualiza una versión renovada del programa en caso que se requiera, lo cual se efectúa de manera automática.

Luego, el suscriptor deberá proporcionar la clave de activación (PIN) y el número de solicitud definida en las etapas anteriores. Dicha información es enviada 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, el programa *Acepta.exe*? obtiene los antecedentes del certificado requerido, y procede a generar el par de llaves pública y privada, lo que es realizado íntegramente en el equipo computacional del suscriptor. Luego se procede a enviar de manera segura al sitio de **Acepta.com** la información correspondiente de la llave pública, en el formato estándar PKCS#10. Luego de verificada la información, se inicia automáticamente el proceso de emisión del certificado, el cual luego de emitido es recuperado por *Acepta.exe*? y presentado visualmente al suscriptor. En ese instante el suscriptor podrá revisar el certificado, y en caso de tener algún reparo, comunicarse con **Acepta.com**.

Posteriormente dicho certificado es instalado en el equipo del suscriptor, o en una tarjeta inteligente en caso que tuviese alguna previamente instalada.

El certificado y la correspondiente llave privada quedan protegidos inicialmente mediante la clave de activación o PIN, teniendo el suscriptor la posibilidad de modificar ésta clave posteriormente.

4.4 Proceso de suspensión y revocación de certificados

Un certificado digital emitido por **Acepta.com** o una de sus Autoridades Certificadoras acreditadas, podrá ser revocado previamente al término del periodo de validez del certificado, cuando concurren algunas circunstancias que generan que la información contenida en el certificado sea inválida. Un certificado revocado queda invalidado permanentemente para su uso. Por otro lado, pueden haber circunstancias menos drásticas que ameriten la necesidad de suspender temporalmente la validez del certificado, el cual puede volver a su estado de vigencia en algún momento posterior.

4.5 Causales y procedimientos para revocar o suspender certificados

Un certificado deberá ser revocado si concurre alguna de las siguientes circunstancias:

- Compromiso de la llave privada del suscriptor del certificado
- Modificación posterior de los antecedentes del suscriptor del certificado
- Falsificación de los antecedentes del suscriptor del certificado

Se podrá solicitar que un certificado sea suspendido sólo como medida precautoria frente a un posible compromiso de la llave privada.

El procedimiento para solicitar la suspensión o revocación del certificado es el siguiente:

1.- Si el suscriptor o titular del certificado todavía mantiene su llave privada asociada al certificado, pero existe el riesgo de su compromiso o perdida de confidencialidad, puede enviar un correo electrónico a admin-revocaciones@acepta.com, mensaje que debe estar firmado digitalmente por el suscriptor. Esto generará la revocación del certificado correspondiente.

2.- Por otro lado, si el usuario no tiene posibilidad de efectuar la revocación por el mecanismo anterior, deberá dirigirse personalmente a los lugares establecidos para tales efectos, los que se publican en www.acepta.com. Allí deberá estampar su firma holográfica en una solicitud de revocación, en la que se establece el momento en que se solicita la revocación junto con los datos del suscriptor.

Una vez recibida la solicitud de revocación en **Acepta.com**, esta es procesada generándose inmediatamente la revocación efectiva del certificado correspondiente, por lo que dicha información estará disponible para consultas on-line en **Acepta.com**.

Adicionalmente, se publicará una lista de revocación con los certificados revocados, con una frecuencia de 12 horas.

4.5.1 Procedimientos de publicación de información de revocaciones

La información pertinente a los certificados digitales suspendidos o revocados será publicada en el sitio Web de Acepta.com (www.acepta.com) o en el de la AC acreditada que corresponda.

La información respecto a la revocación o suspensión de un certificado de clase 3 de persona quedará disponible en el sitio Web de Acepta.com inmediatamente después de completado el proceso de la solicitud de revocación. Es decir, una vez que se le confirme al suscriptor sobre la recepción conforme de la solicitud de revocación, ésta información ya estará disponible en el sitio Web para consulta de cualquier parte que requiera confiar en el certificado del suscriptor.

Para brindar un adecuado servicio de información sobre las revocaciones y suspensiones, Acepta.com y las AC acreditadas soportarán 3 medios para distribuir dicha información, las cuales se detallan a continuación:

4.5.1.1 LISTAS DE REVOCACIÓN (CRL)

Acepta.com y las AC acreditadas mantendrán listas de revocación o CRL con la información de los certificados de clase 3 de persona revocados o suspendidos. Estas listas están en un formato compatible con el estándar X.509.

En cada certificado emitido, en la extensión apropiada se incluirá la información de la ubicación de la lista de revocación para su consulta.

4.5.1.2 CHEQUEO DE REVOCACIÓN ON-LINE (OCSP)

Acepta.com soporta la consulta "on-line" sobre el estado de los certificados por ella emitidos, a través del protocolo OCSP (On-line Certificate Status Protocol). Este es un protocolo estándar ampliamente

reconocido. Información adicional y ayuda respecto a como realizar consultas utilizando dicho protocolo se encuentra disponible en el sitio Web de Acepta.com en www.acepta.com.

4.5.1.3 CONSULTA MEDIANTE EL WEB

También se podrán consultar el estado de los certificados on-line mediante el uso del Web en www.acepta.com .

4.5.2 Frecuencia de la actualización de la información de revocación

Las listas de revocación (CRL) serán actualizadas con una frecuencia de 12 horas entre cada publicación.

4.6 Procedimientos de auditoria de seguridad

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

4.7 Políticas para archivo de registros

4.7.1 Documentos archivados

Con el fin de mantener un adecuado respaldo de la información involucrada en el proceso de certificación, así como para brindar seguridad y garantía a todas las partes involucradas, se almacenaran en un medio seguro los siguientes documentos:

DOCUMENTOS ARCHIVADOS				
Documento	***Descripción***	***Retención***	***Protección***	***Respaldo***
Contrato	Se almacenará copia digital cifrada del contrato. También se almacenará una copia manuscrita	Por un año posterior a vencimiento del certificado	Copia digital se almacenará cifrada en custodia electrónica en Custodium.com	De forma incremental diariamente, y luego se realizará un respaldo semanal y uno completo una vez al mes.
Antecedentes suscriptor	Se almacenará copia digital de todos los antecedentes del suscriptor asociados a la emisión de un certificado.	Por un año posterior a vencimiento del certificado		
Notificación de aceptación del certificado	Se almacenará una copia digital cifrada de la notificación de aceptación del certificado realizada por el suscriptor en el proceso de instalación	Por un año posterior a vencimiento del certificado		
Solicitud de Revocación o Suspensión	Se almacenará una copia digital cifrada de la solicitud de revocación o suspensión de certificados. En caso que se requiera presencia personal del suscriptor, también se almacenará una copia manuscrita firmada por éste.	Por un año posterior a vencimiento del certificado		

TABLA Nº1 – DOCUMENTOS ARCHIVADOS

5 CONTROLES DE SEGURIDAD FÍSICOS, DE PROCEDIMIENTOS Y DE PERSONAL

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 TÉCNICOS

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 persona de clase 3 y llaves asociadas.

6.1 Generación e instalación del par de llaves

6.1.1 Generación de llaves de los suscriptores de certificados

Las llaves privadas de los suscriptores son generadas de tal forma que sólo es conocida, accedida y mantenida por el correspondiente titular del correspondiente certificado.

Para los certificados de identidad de clase 3 de persona, el par de llaves es generado en el equipo local del suscriptor, a través del programa *Acepta.exe* . Esta generación es hecha de una manera segura, quedando la llave privada protegida con una contraseña definida por el propio suscriptor.

6.1.2 Entrega de llaves pública y privada a suscriptor

Las llave privadas de los suscriptores es generada y mantenida en los propios equipos locales de éstos por el programa *Acepta.exe.* En ningún momento durante la creación son transferidas o almacenadas fuera de su ambiente local.

En primer lugar, el programa autentifica que el usuario sea un suscriptor válido, solicitando la digitación del Nº de solicitud y la clave de activación asociadas a la solicitud de certificado. Luego, valida que dichos datos estén asociadas a solicitudes pendientes y aprobadas, como requisito para continuar con el proceso, en donde el programa Acepta.exe procede a generar el par de llaves en el propio equipo del suscriptor.

Posteriormente el programa *Acepta.exe* envía al sitio Web de **Acepta.com** la llave pública, enviando nuevamente el Nº de solicitud y clave de activación (PIN), para identificar la solicitud de certificado asociada. Estos datos son enviados usando el formato estándar PKCS#10, en donde va incorporada la firma digital del suscriptor, usando para ello la llave privada recién generada.

Entonces se valida que el requerimiento de certificado PKCS#10 esté correcto, validando la firma. Si es así, se procesa dicho requerimiento y se genera inmediatamente el correspondiente certificado. Luego, el certificado es recuperado e instalado en el equipo del suscriptor.

Adicionalmente, el programa *Acepta.exe,* que genera el par de llaves, proporciona la funcionalidad de transportar los certificados junto con la llave privada, para ser instalados en otras locaciones o equipos. Para ello, se hace uso del estándar PKCS#12, diseñado para el transporte seguro de éste tipo de información.

Cabe señalar que todas las comunicaciones entre el programa *Acepta.exe* y la autoridad certificadora son realizadas de manera segura. En envío de datos es realizado usando el protocolo de transporte HTTP, y sobre éste el protocolo SOAP para estructurar los datos y solicitar procesamiento. Usando el

protocolo SOAP se construye un "sobre electrónico", en donde van los datos, los cuales son cifrados usando el algoritmo Rijaendael para mayor seguridad.

6.1.3 Entrega de la llave publica de Acepta.com a usuarios

La llave pública de **Acepta.com** y de la AC acreditada (si corresponde) es proporcionada a los usuarios durante el proceso de instalación de los certificados, el cual es llevado a cabo por el programa *Acepta.exe*, el cual instala automáticamente el certificado raíz de **Acepta.com** el de raíz de clase 3 de persona, y los deja como certificado raíz de confianza en el equipo del suscriptor. De igual forma, al proceder a transportar un certificado de identidad a otro equipo, también se instala el certificado de **Acepta.com** con la correspondiente llave pública.

El transporte y envío de la llave pública de **Acepta.com** es realizado de manera segura, usando el algoritmo Rijaendaell como mecanismo de cifrado de datos, y el formato estándar PKCS#7 para almacenar los certificados.

6.1.4 Tamaño de las claves

Todos los pares de llaves para firma de certificados usados por **Acepta.com** y sus AC acreditadas son de un tamaño de 2048 bits. Las llaves de los suscriptores son de un tamaño de 1024 bits.

6.1.5 Hardware/software para generación de llaves

La generación de las claves de los usuarios o suscriptores es realizada por el programa *Acepta.exe*, el cual contiene módulos criptográficos en conformidad con el estándar FIPS 140-1 nivel 1.

6.1.6 Propósitos para el uso de las llaves

Todos los certificados emitidos por **Acepta.com** o por alguna de sus AC acreditadas, incluyen la extensión KeyUsage, para establecer el propósito de uso de los certificados y las llaves asociadas. Opcionalmente se puede incluir en los certificados la extensión ExtendedKeyUsage para definir restricciones adicionales.

Para mas detalles ver sección 7.1.2.

6.2 Protección de las llaves privadas

La llave privada de **Acepta.com** se encuentra protegida internamente según los mecanismos descritos en las CPS.

Para los suscriptores de certificados de clase 3 de persona, al momento de instalar el certificado éste queda protegido por la clave de activación proporcionada por el mismo suscriptor durante el proceso de enrolamiento. No obstante, éste tiene la opción de cambiar dicha clave posteriormente. Además, el programa *Acepta.exe* le brinda al suscriptor la opción de importar o exportar certificados, junto con la llave privada correspondiente, lo cual le permite mantener el debido resguardo de las correspondientes llaves privadas de sus certificados.

6.3 Otros aspectos de gestión de claves

6.3.1 Archivo de llaves publicas

Las llaves públicas de los suscriptoresson archivadas según el formato estándar PKCS#7.

6.3.2 Periodos de uso de las llaves

El periodo de uso de las llaves es descrito en la sección 7.1

6.4 Datos de activación

6.4.1 Generación y activación de datos de activación

Para los certificados de identidad de clase 3 de persona, al momento de solicitar el certificado el suscriptor proporciona un password o clave de activación (PIN). Este, más el número de la solicitud correspondiente serán requeridos luego por el software Acepta.exe para proceder a la instalación posterior del certificado.

6.4.2 Protección de datos de activación

Los datos de activación requeridos para el manejo de la llave privada de los suscriptores son definidos por éstos mismos, y mantenidos pajo su exclusivo control. Asimismo, para el caso de los datos de activación de **Acepta.com** o sus AC acreditadas, ésta información es mantenida sólo por personal autorizado que ocupa posiciones de confianza dentro de la compañía.

6.5 Controles de seguridad computacionales

Acepta.com implementa una serie de controles que le permiten un adecuado resguardo de sus recursos computacionales, lo que está descrito en las CPS de Acepta.com.

7 FORMATOS DE CERTIFICADOS Y LISTA DE REVOCACIÓN

Este capítulo contiene especificaciones detalladas de los formatos y contenido de los certificados de persona de clase 3 (campos, básicos y extensiones). Además se especifica el formato de las listas de revocación (CRL).

7.1 Composición básica de los certificados

En esta sección se detalla la composición y formato de los certificados emitidos por **Acepta.com** y sus AC acreditadas. Dichos certificados están en conformidad con el estándar internacional ITU-T X.509v3.

FORMATO DE CERTIFICADOS DE CLASE 3 DE PERSONA		
CAMPO	***DESCRIPCIÓN***	***EJEMPLO***
Versión	Versión del certificado, que deberá ser versión 3	3
Nº de Serie	Nº que identifica unívocamente al certificado dentro de los emitidos por Acepta.com	0234865AF87AC87CCB2
Algoritmo de Firma	Algoritmo utilizado por la AC 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 C = País O = Nombre de la autoridad certificadora emisora OU = Nombre de la autoridad certificadora emisora del tipo de certificado E = e-mail de la autoridad certificadora emisora	C = CL O = Acepta.com S.A. OU = Autoridad certificadora Clase 3 persona natural CN = Acepta.com Autoridad certificadora Clase 3 persona natural E = info@acepta.com
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado. Para AC = 10 años, para suscriptores = 1 año, para servidores = 2 años. Codificado en formato YYMMDDHHMMSSZ	Fecha inicio = 01/11/2000 Fecha termino = 01/11/2001
Nombre del titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X..500. Deben incluirse los siguientes tipos: C = País O = Nombre de la autoridad certificadora emisora OU = Tipo de certificado CN = Nombre distintivo del suscriptor T = Profesión E = dirección de correo del suscriptor	C = CL O = Acepta.com S.A. OU = Certificado Clase 3 persona natural T = Ingeniero CN = Andrés Robles Sarmiento E = andres@sarmiento.cl
Clave pública	Clave pública del titular del certificado	3081 8902 8181 00C9 0FA4 CE30 C28C 91BF 4537 EA0E CC8D F580 6B97 A1F2 DA9D 7A40 9CF9 B7D3 30C7 7FEC 7D93 8980 D307 A2B8 8080 2A3B 2234 E037 175F B845 ECED 10C1 8CC4 8DAC C992 B392 651A BB3B 38B4 583B 5910 F5F2 17B0 1EEA 143C A129 3349 2179 3D04 ABD4 4A82 AAF7 EA55 C841 16F1 03B2 75A3 18C8 56C8 06DE F9BE 44AE 8B19 DF07 13C4 58D8 45EB E102 0301 0001

TABLA Nº2 – COMPOSICIÓN BÁSICA DE CERTIFICADOS SEGÚN ESTÁNDAR X509V3

7.1.1 Números de versión(s)

Todos los certificados emitidos corresponden a la versión 3 del estándar X.509

7.1.2 Extensiones

Acepta.com y sus AC acreditadas emiten certificados los cuales contemplan un número de extensiones para mejorar la aplicabilidad, y uso de los certificados. Las extensiones se pueden clasificar en 2 tipos:

- *Extensiones de Restricciones*: Restringen o clarifican el uso de los certificados y las correspondientes claves. Pretenden establecer los limites de uso, políticas aplicables y restricciones adicionales.
- *Extensiones de Información*: Proporciona información adicional a los usuarios de los certificados, pero no limita en cualquier forma el uso de los certificados. Principalmente pretenden brindar información adicional respecto al contenido de los certificados o del sujeto o titular del mismo.

A su vez, éstas pueden ser extensiones estándar o extensiones privadas. Las primeras corresponden a aquellas definidas en el estándar X.509, 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. En ese sentido, se soportan un conjunto de extensiones privadas recomendadas por Microsoft, Netscape y las sugeridas por la IETF.

A continuación se detallan las extensiones incluidas en los certificados de clase 3 de persona. Primero se detallan las extensiones estándar, luego las extensiones privadas. Para cada una, se muestra el número identificador asociada para la extensión (OID: Object Identifier). El OID es un número que permite identificar de manera única y global a través de Internet a cada extensión u objeto al que hace referencia. Además se muestra si es una extensión de carácter informativo (INF) o restrictivo (RES).

EXTENSIONES SEGÚN ESTÁNDAR X.509V3				
Tipo	***Nombre***	***Descripción***	***OID***	***Valor***
RES	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	Digital Signature , Non-Repudiation , Key Encipherment(E0)
RES	BasicConstrains	Permite diferenciar entre un certificado de AC y uno de suscriptor final.	2.5.29.19	Subject Type=End Entity Path Length Constraint=None
RES	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	Client Authentication(1.3.6.1.5.5.7.3.2) Secure Email(1.3.6.1.5.5.7.3.4)
RES	AuthorityKeyIdentifier	Medio para identificar la llave pública de Acepta.com El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier		KeyID=8B50 7988 00E1 6A80 FABE 673B E6AC 86E6 24A9 312A
RES	SubjectKeyIdentifier	Identificador único de la llave pública de la AC, conteniendo el hash de 160bit de la llave pública		8B50 7988 00E1 6A80 FABE 673B E6AC 86E6 24A9 312A
RES	CertificatePolicy	Ver sección 7.1.6		
INF	IssuerAltName	Identificador alternativo del emisor, corresponde al RUT de Acepta.com, en formato análogo a SubjectAltName		
INF	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.		Other Name: 1.3.6.1.4.1.8321.1= 040C 3132 2E35 3233 2E39 3132 2D39
INF	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]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.acepta.com/Clase3Persona.crl

TABLA Nº3 – EXTENSIONES DE CERTIFICADO SEGÚN ESTÁNDAR X509V3

EXTENSIONES SUGERIDAS POR IETF				
TIPO	***NOMBRE***	***DESCRIPCIÓN***	***OID***	***VALOR***
INF	AuthorityInfoAccessSyntax	En esta extensión se establece información de acceso a servicios de información de la autoridad certificadora. 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]Authority Info Access Access Method=On-line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.acepta.com

TABLA Nº4 – EXTENSIONES DE CERTIFICADO SUGERIDAS POR EL IETF Y SU GRUPO DE TRABAJO PKIX

EXTENSIONES PRIVADAS DE ACEPTA.COM				
TIPO	***NOMBRE***	***DESCRIPCIÓN***	***OID***	***VALOR***
INF	UserComment	En esta extensión se establecen observaciones que el suscriptor desea que aparezcan en el certificado	1.3.6.1.4.1.6891.9	
INF	RADescription	En esta extensión se describe a la Autoridad de Registro que registró al suscriptor	1.3.6.1.4.1.6891.15	

TABLA Nº5 - EXTENSIONES PRIVADAS DE ACEPTA.COM

7.1.3 Objetos identificadores de algoritmos

Bajo la arquitectura definida por estas CPS, todos los certificados emitidos utilizan los siguientes algoritmos y sus correspondientes identificadores (OIDs):

NOMBRE	DESCRIPCIÓN	OID
SHA-1	Algoritmo de generación de hash	1 3 14 2 26 5
RSA	Algoritmo de cifrado de datos	1 3 14 3 2 1 1
RSAWithSHA-1	Algoritmo para firma de certificados. Se usa algoritmo Sha-1 como función hash, y algoritmo RSA para generar la firma.	1 3 14 3 2 15

TABLA Nº6 – OBJETOS IDENTIFICADORES DE ALGORITMOS

7.1.4 Nombres

Ver sección 3.1

7.1.5 Restricciones para los nombres

Para los nombres asociados a correo electrónico, se deberá utilizar el formato según RFC822.

7.1.6 Objeto identificador de las políticas de certificados

Estas políticas de certificado son identificadas mediante un número único, denominado Object Identifier (OID), según el estándar X.509. Dicho número es incluido en el certificado para hacer referencia a éstas políticas.

Para obtener identificadores únicos, **Acepta.com** ha registrado un número que la identifica como empresa, en la Internet Assigned Number Authority (IANA), organización internacional que administra un conjunto de estos números para Internet, y asegura que sean únicos.

El OID para **Acepta.com** es el 1.3.6.1.4.1.6891.

El OID de las políticas de certificado de clase 3 de persona natural es el 1.3.6.1.4.1.6891.2.

7.1.7 Calificadores de política de certificados, sintaxis y semántica

En dicha extensión, se representa la siguiente información:

PolicyIdentifier: identificador de la política de certificados de certificado clase 3 persona natural.

PolicyQualifiers: Calificadores de la política. Acepta.com utiliza los siguientes calificadores:

- CPS Pointer: indica la ubicación de las Prácticas de Certificación (CPS) para ser consultada por los usuarios. Es un URL a una página Web con una declaración concisa de las CPS, y es el siguiente www.acepta.com/PoliticasyPracticas.html .
- UserNotice: Indica ubicación de información textual para ser presentada a los usuarios de certificados. Esta notificación contiene el siguiente texto:

  "El titular ha sido validado en forma presencial. Este proceso no está orientado a validar facultades, por lo tanto no impone ningún tipo de restricción, quedando habilitado el Certificado para uso tributario, pagos, comercio y otros."

7.1.8 Semántica para el procesamiento de extensiones críticas

Para garantizar una adecuada interoperabilidad y procesamiento de los certificados por distintos sistemas de software, todas las extensiones son no-críticas.

7.2 Composición de la lista de revocación (CRL)

7.2.1 Número de versión(s)

Las listas de revocación manejadas por **Acepta.com** y sus AC acreditadas es la versión 2 según el estándar X.509.

7.2.2 Campos básicos

CAMPOS BÁSICOS DE LA LISTA DE REVOCACIÓN		
Nombre	***Descripción***	***Valor***
Versión	Corresponde a versión 2	2
Issuer	Descripción de la autoridad Certificadora emisora de la CRL	E = info@acepta.com CN = Acepta.com Autoridad certificadora Clase 3 persona natural OU = Autoridad certificadora Clase 3 persona natural O = Acepta.com S.A. C = CL
Effective Date	Fecha de publicación de la CRL	
Next Update	Fecha de próxima publicación	
Signature algorithm	Algoritmo DE firma de la CRL	Corresponde a Sha1RSA

TABLA Nº7 – EXTENSIONES SOPORTADAS PARA LA LISTA DE REVOCACIÓN

7.2.3 Extensiones

Acepta.com y sus AC acreditadas usan las siguientes extensiones:

EXTENSIONES SOPORTADAS PARA LA LISTA DE REVOCACIÓN	
Nombre	***Descripción***
AuthorityKeyIdentifier	Identificador de la clave de la autoridad certificadora

TABLA Nº8 – EXTENSIONES SOPORTADAS PARA LA LISTA DE REVOCACIÓN

8 MANTENCION DE ESTAS CP

Este capítulo contiene una descripción de los procedimientos aplicables para las subsecuentes modificaciones de las políticas de certificado de clase 3 persona natural.

8.1 Procedimientos para cambios en las CP

Las políticas de certificado de clase 3 de persona contenidas en este documento, 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**.