Prácticas de Certificación

Modelo de Confianza Bancario

Certinet

Fecha	Versión	Objeto de la Modificación	Modificado por:	Referencia
Mar/2002	V1.0	Primera versión oficial de las CPS Certinet	R. Gutiérrez R. Riveros	
Jun/2002	V1.1	Incorporar los conceptos de Ley y Reglamento, incluyendo: • Posibilidad de Certinet actúe como Registro • Adecuación de AR a ARA (Autorizada) • Eliminación de Solicitante ya que legalmente no es reconocido • Precisar la Aceptación del Certificado para establecer claras responsabilidades	R. Gutiérrez R. Riveros	
Sep./2003	V1.2	Adecuación de las prácticas para ser utilizables por Certinet	R. Riveros	
Nov./2003	V1.3	Adecuación para eliminar referencias a certificados de empresa	R. Riveros	
Mayo/2004	V1.4	Adecuación al modelo Bancario definido por el grupo de Bancos	R. Riveros R. Gutiérrez	
Agosto 2006	V 1.5	Incorporación de conceptos de Firma Electrónica Avanzada	R. Gutiérrez R. Riveros	
Noviembre 2010	V1.6	Eliminación de referencias a firma electrónica no avanzada y cambio domicilio de Certinet.	R. Riveros	
Enero de 2016	V1.7	Actualiza Algoritmo de Firma de los certificados Sha1 a Sha2	A. Carreño R. Riveros	
Abril de 2019	V1.8	Actualiza CPS e incorpora mecanismo de custodia de Certificados de acuerdo con el Decreto Supremo N°24 de 2019 del MINECON, que aprueba norma técnica para la prestación del servicio de certificación de firma electrónica avanzada.	A. Carreño R. Riveros	

Contenido

1. Introducción

El presente documento contiene las estipulaciones que constituyen las Prácticas de Certificación de Certinet S.A. para implantar por un grupo de bancos establecidos en Chile, el Modelo de Confianza Bancario para Firma Electrónica Avanzada en adelante "CPS Certinet". Estas Prácticas fueron desarrolladas por Certinet en conjunto con los Bancos: BBVA, Banco Chile, BCI, Banco Estado, Banco Santander-Santiago, Banco Security, Corpbanca y Scotiabank Sud Americano a partir de las Prácticas de Certificación Bancarias (Certinet) de propiedad de los Bancos BCI, Banco de Chile, Scotiabank Sudamericano, Banco Santander Santiago y Banco Estado.

La "CPS Certinet" supone que el lector conoce las nociones básicas de certificado digital, Firma Electrónica Avanzada e Infraestructura de Clave Pública (PKI).

Se aconseja a los usuarios conocer el funcionamiento de una Infraestructura de Clave Pública (PKI), antes de solicitar un Certificado. Se recomienda, además, leer el documento de *Introducción a la Firma Electrónica* y *Glosario de Términos Certinet*, disponible en **www.certinet.cl**

1.1 Generalidades

La "CPS Certinet" establece (a) la política, los procedimientos y las normas que Certinet adopta actuando como Autoridad Certificadora en la provisión de Servicios de Certificación para este Modelo Bancario y (b) constituyen el contrato entre Certinet y el *Suscriptor* (Titular).

Contienen además las reglas que regulan el uso de las claves y de los certificados asociados por el Suscriptor y de todos aquellos que libremente deciden confiar en un Certificado emitido por Certinet para este Modelo.

La "CPS Certinet", se dictan bajo la VeriSign Trust Network, por lo que éstas CPS acceden y son un complemento de las prácticas de VeriSign vigentes, que se encuentran en

https://www.certisur.com/cps, y el estándar ISO/IEC 9594-8, según el tipo de certificado emitido, todo lo cual se entenderá como parte integrante de este instrumento.

En el presente documento se describen entre otras materias, las siguientes:

- Obligaciones del Prestador de Servicios de Certificación, las Autoridades de Registro, Suscriptores y Usuarios dentro del ámbito que regula la "CPS Certinet".
- Aspectos considerados en el Contrato de Suscriptor para el ámbito de aplicación de la "CPS Certinet",
- Revisiones de Auditoria, de Seguridad y de cumplimiento de las "Prácticas" que están consideradas,
- Métodos usados para confirmar la identidad de los solicitantes de certificados.
- Protección de Datos Personales y Propiedad Intelectual
- Procedimientos operacionales para los servicios asociados al ciclo de vida de los certificados: Solicitud, Emisión, Aceptación, Revocación, Suspensión y Renovación.
- Procedimientos operacionales para registros de auditoría, retención de registros de información, contingencia y recuperación de desastres,
- Prácticas de seguridad física, del personal y del manejo de claves.
- Contenidos de las listas de certificados emitidos, vigentes y revocados
- Administración de este documento, incluyendo métodos de su actualización.

1.2 Identificación

a) El presente documento será individualizado como "Prácticas de Certificación Modelo de Certificación Bancario de Certinet" o "CPS Certinet".

b) La *CPS Certinet* se ha desarrollado en conformidad con el documento "Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Framework*", emitido por el *Internet Engineering Task Force* "IETF", como RFC 2527, según lo dispuesto en el Reglamento de Ley de Firma Electrónica, DS 181 de 2002 del Ministerio de Economía, Fomento y Turismo, en adelante "el Reglamento".

c) El presente documento está disponible de las siguientes formas: i) electrónica en el sitio de dominio electrónico ii) por correo electrónico si se solicita a la persona de Contacto de Certinet.

1.3 Aplicabilidad

La “CPS Certinet” se aplica a todos los certificados de Firma Electrónica Avanzada emitidos por Certinet dentro del Modelo Confianza Bancaria implantado.

El uso de los certificados y su información asociada está restringido a las condiciones de uso específicas descritas en este instrumento llamado “CPS Certinet”, y en particular, no pueden ser usados para certificar a otros individuos u objetos ni relacionarse con certificadoras que no tengan acuerdo de interoperabilidad vigente con Certinet.

Certinet ofrece actualmente certificados que proveen un nivel de funcionalidad y confianza específica:

Tipo	Descripción
Firma Electrónica Avanzada	Este certificado solamente se emite a persona natural que ha sido identificada positivamente en forma equivalente a un cliente de cuenta corriente bancario, para disponer de certificado de Firma Electrónica Avanzada. Específicamente se le solicitan los siguientes antecedentes: • Solicitud firmada que identifica los antecedentes del Suscriptor • Cédula o Carnet de Identidad vigente • Capacidad de acceso a sitio WEB para clientes de alguno de los Bancos que forman parte de este modelo, o acceso a “ClaveUnica” • Foto • Huella digital • Correo electrónico • Teléfono Móvil

1.4 Entidades

Las entidades que participan en el uso y aplicación de certificados son:

1.4.1 *Prestador de Servicios de Certificación (PSC)*

Certinet está constituido como un Prestador de Servicios de Certificación en conformidad con las leyes de la República de Chile, en particular por la “Ley Nº 19.799 sobre Documentos electrónicos, firma electrónica avanzada y servicios de certificación de dicha firma”, en adelante *“Ley de Firma Electrónica” y su Reglamento,* Decreto Supremo 181, del Ministerio de Economía, Fomento y Turismo.

Certinet además, está acreditado como un Prestador de Servicio de Certificación de Firma Electrónica Avanzada, según da cuenta la R.A. Exenta No. 380, de 21 de Julio de 2006, de la Subsecretaría de Economía y Empresas de Menor Tamaño.

Su domicilio es Huérfanos 1052, Piso 12, en Santiago de Chile.

Certinet actúa estableciendo modelos de certificación para comunidades de negocios, dentro de las cuales emite y administra Certificados para Firma Electrónica Avanzada y servicios asociados, constituyéndose en una Autoridad Certificadora para dicha comunidad.

1.4.2 *Autoridades de Registro*

Son aquellas personas jurídicas o entidades que autorizadas por Certinet y actuando en representación de Certinet para una determinada comunidad de negocio, realizan: a) la actividad de identificar y registrar los antecedentes de los solicitantes de Certificados, b) evaluar, aprobar o rechazar las solicitudes de Certificados de acuerdo a las políticas definidas y c) Verificar la identidad de un Suscriptor a través del sistema de ClaveUnica, presencial u otra permitido por ley, d) realizar las funciones de solicitar la suspensión, la revocación, la renovación de certificados de acuerdo a las políticas implantadas por Certinet, además de otras funciones que se le encomienden.

Certinet es, por esencia una Autoridad de Registro y cuando actúa como tal, asume todas y cada una de las obligaciones establecidas en estas “CPS Certinet”; en el evento de delegar dicha función asume también la responsabilidad por el cometido de sus delegados o mandatarios, por cuanto estos actúan por cuenta y riesgo de la primera.

1.4.3 *Solicitante*

Persona natural o jurídica debidamente representada que solicita para sí o para un tercero la emisión de un Certificado.

1.4.4 *Suscriptor*

Aquel en cuyo favor se ha emitido un Certificado.

1.4.5 *Usuarios*

Aquel que voluntaria y libremente decide hacer uso y/o confiar en un Certificado emitido por Certinet.

1.5 Detalles de Contacto

La "CPS Certinet" es administrada por Certinet S.A., que puede ser contactada al e-mail: soporte@certinet.cl

Personal de Contacto:

Soporte Certinet

Fono: 56 2 3221 9400

Mayor información de contacto se encuentra disponible en **www.certinet.cl**.

2. Obligaciones y Responsabilidades

En este capítulo se describen las obligaciones y responsabilidades de los diferentes participantes asociados al ciclo de vida de los certificados. Se establece además las materias relacionadas con la interpretación y cumplimiento de estas prácticas, el límite de uso de los certificados, el esquema tarifario y el proceso de publicación, auditoría, derechos de propiedad intelectual y protección de datos personales.

2.1 Obligaciones

2.1.1 Certinet

Se obliga a:

a) Ofrecer y mantener una estructura adecuada, que permita otorgar los servicios de certificación y Sello de Tiempo.

b) Cumplir y respetar los procedimientos establecidos en la *"*CPS Certinet" y en las Prácticas específicas de Certificados (CP) que se otorguen para la emisión de Certificados.

c) Cumplir con todas las otras obligaciones que establezcan la Ley de Firma Electrónica, y su Reglamento asociado.

d) Aprobar o denegar las solicitudes de Certificados realizadas por los Solicitantes, directamente o a través de las Autoridades de Registro de conformidad con las "CPS Certinet".

e) Emitir los certificados en conformidad al procedimiento establecido en las "CPS Certinet"**.**

f) Proveer mecanismos de custodia de llaves del cliente como eToken, y/o mantener la custodia y la disponibilidad de las llaves que el cliente libremente haya escogido guardar en repositorio seguro central de Certinet de acuerdo con el DS N°24 de 2019 del MINECON, que aprueba la norma técnica para la prestación del servicio de certificación de firma electrónica avanzada, publicación en el Diario Oficial de fecha 9 de abril de 2019.

g) Notificar al Suscriptor de la emisión de su Certificado.

h) Configurar y mantener un Registro Público de Certificados en vigencia, suspendidos y revocados.

i) Revocar o suspender los Certificados, notificando al *Suscriptor* de dichas acciones.

j) Realizar razonables esfuerzos para comunicar a los Suscriptores de cualquier hecho conocido por Certinet, que pudiera afectar la validez del Certificado.

k) Delegar la función de Autoridad de Registro en entidades de su confianza, asumiendo la responsabilidad por su cometido en el desarrollo de dicha función.

l) Mantener un sitio de dominio electrónico de libre acceso con información para el público sobre los servicios prestados.

2.1.2 Autoridad de Registro

Son funciones de la Autoridad de Registro

a) Identificar y verificar en forma inequívoca a los solicitantes de un Certificado, de conformidad al procedimiento establecido en las "CPS Certinet"**,** y en las Prácticas Específicas (CP) correspondientes a los Certificados.

b) Registrar y custodiar los antecedentes requeridos a los Solicitantes que permitan una identificación plena de los mismos, de conformidad con los requisitos establecidos en las Prácticas Específicas (CP) correspondientes a los Certificados.

c) Aprobar o denegar las Solicitudes de Emisión de Certificados.

d) Entregar al Suscriptor su Certificado o dar las instrucciones para su retiro y/o de uso, según el mecanismo de custodia que el cliente haya elegido libremente.

e) Recibir las Solicitudes de revocación o suspensión de Certificados, e informarlas a Certinet.

f) Obtener la aceptación de los términos y condiciones del servicio por parte del Solicitante mediante la firma de la Solicitud o Contrato.

g) Conservar en forma segura, la información recibida en el proceso de emisión, suspensión y revocación de un certificado por el período que la Ley de Firma Electrónica y su Reglamento indiquen.

h) Permitir operar solamente certificados que hayan sido aceptados por el Solicitante.

i) Prestación de otros servicios que Certinet le solicite.

Todas las actuaciones indicadas en las letras anteriores, las realiza la Autoridad de Registro en representación y por cuenta y riesgo de Certinet.

2.1.3 Obligaciones del *Suscriptor*

Antes de la emisión del certificado el Suscriptor se obliga a:

a) Establecer una solicitud formal de emisión de certificado, en la que acepta los términos y condiciones descritos en la “CPS Certinet”

b) Cumplir con los requerimientos de información solicitados por Certinet y/o la Autoridad de Registro de conformidad a la presente “CPS Certinet”.

c) Seleccionar, el mecanismo digital o el dispositivo token, custodiando el dispositivo físico para almacenamiento seguro de los datos asociados a la generación de firma ya sea individual o masivo, y generar en él, el par de claves utilizadas en el proceso de firma por medios que estén bajo su exclusivo control. En el caso de elegir un mecanismo complementario digital, según lo establecido en el art. 5 inc. 2° del DS N°24 de 2019 del MINECON, se obliga a mantener el exclusivo control del segundo factor de seguridad.

d) El Usuario puede elegir libremente almacenar las llaves para creación de firma en un dispositivo individual físico o bien, utilizar un dispositivo masivo con el servicio de custodia

central segura, que CERTINET mantiene en alta disponibilidad con acceso remoto y bajo los mismos resguardos establecidos por el PSC en su Política de Seguridad. No obstante se deja especial constancia que el Usuario Titular de un Certificado es el único que puede accesar a su Certificado, teniendo por lo mismo, un exclusivo control y acceso a este, según lo señalado previamente en la letra c).

e) No revelar la clave de acceso al dispositivo que contiene la clave privada asociada al certificado y/o no relevar el mecanismo de activación de la firma, según lo señalado en la letra c).

f) Pagar las tarifas convenidas por concepto de los servicios de certificación y/o custodia que solicite, aun cuando no se acepten o no se ocupen los Certificados emitidos.

g) En el caso de las personas naturales, ser mayor de edad.

Una vez emitido el certificado el Suscriptor se obliga a:

h) Aceptar el certificado. Se entiende que un certificado ha sido aceptado por parte del Suscriptor una vez que: i) este haya sido emitido por Certinet, aun cuando el certificado no haya entrado en vigencia por contener una fecha de inicio de operación posterior a su fecha de emisión, ii) No se haya formulado un reclamo por error o inexactitud en la emisión, al momento de su recepción III) La utilización, por parte del Suscriptor, de una Clave de Confirmación comunicada por Certinet para retirar el Certificado, la instalación en el dispositivo de generación de firma o dejar en custodia para la posterior utilización, de cualquier modo, el Certificado, es considerada la aceptación del Certificado por parte del Suscriptor.

i) Comunicar a Certinet cualquier error o inexactitud en el Certificado que reciba. Si no lo hace al momento de su recepción, todas las declaraciones se tendrán por verdaderas.

j) Usar la clave privada asociada al Certificado y el Certificado para fines legales y autorizados, de conformidad con lo previsto en la Ley de Firma Electrónica, las “CPS Certinet” y en las Prácticas Específicas (CP) de los Certificados.

k) Utilizar correctamente el Certificado, el que se entrega en depósito o se mantiene bajo la custodia central segura de Certinet.

l) Ser un usuario final, y no usar el Certificado para actuar como Prestador de Servicios de Certificación, a su vez.

m) Comunicar inmediatamente a la Autoridad de Registro y/o a Certinet el compromiso, pérdida, hurto, robo, acceso no autorizado o extravío, falsificación de su clave privada o certificado o cualquier circunstancia que pudiera ser causal de suspensión o revocación de un Certificado.

n) Comunicar la pérdida o destrucción del dispositivo enrolado para utilización de los certificados, ya sea en dispositivo físico o en custodia.

o) Custodiar la clave privada, tomando precauciones razonables para evitar su pérdida, modificación y uso no autorizado.

p) Solicitar la suspensión o revocación del Certificado cuando se presente alguna de las causales indicadas para este efecto

q) Abstenerse de usar la clave privada una vez que el Certificado haya expirado o haya sido solicitada la suspensión o revocación.

r) Destruir la clave privada en caso de que Certinet así lo exija y haya sido revocado previamente el certificado.

2.1.4 Obligaciones de los Usuarios

Los Usuarios que decidan en forma libre y espontánea confiar y usar los Certificados emitidos por Certinet, se obligan en forma previa a:

a) verificar la validez del certificado mediante consulta al registro de certificados,

b) verificar la firma del Suscriptor,

c) comprobar las restricciones de uso que figuren en el certificado y las prácticas “CPS Certinet” y,

d) validar el uso de certificado para propósitos autorizados de conformidad con la Legislación vigente.

2.1.5 Obligación General

Los usuarios del servicio de certificación de Certinet, se obligan a conocer y aceptar los términos, condiciones y límites contenidos en estas “CPS Certinet”, y en las Políticas de Certificación específicas de los Certificados (CP) que suscriban, los que en conjunto regulan la prestación de Servicios de Certificación.

2.2 Responsabilidades

En este punto se incluyen en forma unificada los conceptos definidos por el “Internet X.509 Infraestructura de clave pública Política de certificados y marco de prácticas de certificación – RFC 2527”, en particular respecto de los puntos “2.2 *Liability*”, y “2.3 *Financial responsabilities*”.

2.2.1 Certinet

Es responsable de:

a) Emitir el Certificado cumpliendo todas las exigencias materiales requeridas en las presentes “CPS Certinet”, y de conformidad con los datos entregados por el Suscriptor.

b) Que el Certificado no contenga errores de trascripción de los datos recogidos del Suscriptor, y se ha emitido ejerciendo la actividad con diligencia y cuidado razonable.

c) Que la información incluida o incorporada por referencia en el Certificado es exacta.

d) Publicar el Certificado en el directorio correspondiente.

e) La aplicación correcta del procedimiento empleado.

Certinet no será responsable por ningún daño o perjuicio actual o futuro, directo o indirecto, previsto o imprevisto, emergente o lucro cesante, pérdida de datos u otros, debidos, ocasionados o conectados con el uso indebido, no uso, uso tardío de Certificados o Firma Electrónica Avanzada y/o cualquiera otro servicio ofrecido o contemplado por estas Prácticas de Certificación, aun cuando el *Prestador de Servicios de Certificación* hubiera sido advertido de la posibilidad de producción de tales daños.

Certinet no será responsable del uso indebido o incorrecto de los certificados, sus claves sus dispositivos de almacenamiento de llaves o activación.

Certinet quedará exento de toda responsabilidad y liberada del cumplimiento de sus obligaciones, si por razones de caso fortuito o fuerza mayor tales como sismos, cortes de energía eléctrica y/o del servicio telefónico y/o de líneas de transmisión de datos, intervenciones de redes por partes de terceros, no funcionamiento de redes públicas y/o privadas, actos terroristas, huelgas u otros similares, no se pudiere mantener en funcionamiento u operativo el servicio contratado. El Suscriptor renuncia por este medio a cualquier acción en contra de Certinet por pérdidas, perjuicios, gastos o daños actuales o futuros, en relación con su participación en el servicio objeto de la presente “CPS Certinet”.

2.2.2 Limitaciones de Responsabilidad de Certinet.

Por aplicación a la responsabilidad contractual (incluyendo incumplimientos de las garantías acordadas), extracontractual (incluyendo negligencia y/o daños y perjuicios, directos o indirectos, previstos e imprevistos) y a cualquier tipo de reclamo efectuado mediante procedimiento legal comparable, si el Suscriptor inicia cualquier reclamo, acción, demanda, arbitraje o cualquier otro procedimiento legal relacionado con los servicios suministrados bajo las presentes “CPS Certinet” y/o el Contrato de Suscriptor, la responsabilidad total de Certinet por los daños y perjuicios invocados por el Suscriptor y/o cualquier tercero, por cualquier uso o confianza asignados a un certificado específico estarán limitados, en su totalidad, al monto establecido a continuación:

Clase	Tope Máximo de Responsabilidad
Firma Electrónica Avanzada	El equivalente en moneda local a Mil Dólares Estadounidenses (US$) 1.000,00)

Las limitaciones de responsabilidad establecidas en el presente numeral constituyen el tope máximo, independientemente del número de firmas electrónicas avanzadas, transacciones o reclamos relacionados con un certificado específico. Certinet no podrá ser obligado a indemnizar una suma mayor que el tope máximo de responsabilidad estipulado, por cada certificado.

2.2.3 *Autoridad de Registro*

Es responsable de:

a) Realizar la correcta identificación y registro del Suscriptor de un Certificado

b) Realizar con la diligencia y cuidado debido, las funciones que conforme a las “CPS Certinet” le correspondan como Autoridad de Registro o que Certinet le solicite.

2.2.4 Suscriptor

El Suscriptor es responsable de:

a) La veracidad de la información entregada a Certinet y/o la Autoridad de Registro al momento de solicitar un certificado.

b) El pago de los servicios solicitados

c) Mantener bajo su custodia y exclusivo control la clave privada y/o el acceso al mecanismo complementario digital de activación de firma, desde el momento de su generación hasta su extinción.

d) Abstenerse de usar la clave privada antes de la aceptación del certificado. El Suscriptor es el único responsable de los daños y perjuicios que con su actuación se causen en el evento que use su clave privada y/o mecanismo complementario digital de creación o autorización de firma mientras no se haya efectuado tanto la aceptación como la entrada en vigencia del certificado.

e) Durante el período de vigencia del certificado, el Suscriptor es responsable y así lo acepta y declara, que cada Firma Electrónica Avanzada creada utilizando su clave privada asociada a la clave pública contenida en el certificado, corresponde a la Firma Electrónica Avanzada del Suscriptor y que el Certificado ha sido aceptado y se encontraba vigente, al momento de la creación de dicha firma.

f) Desde el momento que acepta el Certificado, según lo indicado en el punto 2.1.3, Letra h) el Suscriptor será responsable de indemnizar al Prestador de Servicios de Certificación y/o a la Autoridad de Registro, todo daño o perjuicio proveniente de cualquier acción u omisión negligente, culposa o dolosa de su parte.

g) Ratificar que todas las declaraciones que realizó al momento de solicitar el Certificado son verdaderas.

h) Ratificar que todas las declaraciones contenidas en el Certificado se tienen por verdaderas.

2.2.5 *Usuario*

El Usuario que confía y usa libre y espontáneamente un Certificado asumirá la responsabilidad y riesgos derivados de la aceptación de dicho Certificado, cuando no haya realizado en forma previa los pasos necesarios para la verificación de su validez de acuerdo a las “CPS Certinet”.

2.3 Interpretación y Cumplimiento

2.3.1 Ley Aplicable

El presente documento y las Prácticas de Certificación de Certificados (CP), se regirán por la ley Chilena y se someterán al Tribunal Arbitral que más adelante se expresa.

2.3.2 Procedimiento de Resolución de Conflictos

Cualquier dificultad que se produzca entre las partes con motivo de la validez, nulidad, aplicación, cumplimiento, interpretación o resolución del presente documento, incluso las relativas a la competencia del árbitro, será resuelta por medio de las siguientes instancias:

a) Mediación Técnica, efectuada por un Perito Judicial designado de común acuerdo entre las partes.

b) Arbitraje efectuado por un árbitro arbitrador en contra de cuyo fallo no procederá recurso alguno, incluso casación ni queja.

El árbitro será designado de común acuerdo entre las partes y, a falta de dicho acuerdo, será nombrado por los tribunales de Justicia, debiendo la designación recaer en un abogado que se desempeñe o haya desempeñado como integrante de la Excelentísima Corte Suprema o de la Corte de Apelaciones de Santiago, o como profesor de alguna cátedra universitaria de Derecho Civil, Comercial o Económico de una Universidad estatal o reconocida por el Estado.

2.3.3 Separación o Divisibilidad de Cláusulas

En el evento que alguna disposición contenida en las “CPS Certinet” sea declarada nula, inoponible o cualquier otra causa de ineficacia jurídica, se deja constancia que dicha declaración sólo afecta la norma en particular, dejando vigente en su integridad el resto del documento.

2.3.4 Conflicto de Normas

En caso de producirse un conflicto de normas, se seguirá el siguiente orden de precedencia:

a) Ley de Firma Electrónica
b) Reglamento de Ley de Firma Electrónica
c) Contrato de Suscriptor
d) CPS Certinet vigente
e) CP Certinet vigente
f) Otros documentos, relacionados con la prestación de servicios de certificación.

2.3.5 Limitación de uso de los Certificados

Los Servicios de Certificación de Certinet no fueron diseñados, pensados ni autorizados para su uso o reventa como equipo de control en circunstancias peligrosas, o para usos que requieran un desempeño a prueba de fallas, como por ejemplo la operación de instalaciones nucleares, navegación o sistemas de comunicación de aeronaves, sistemas de control de tráfico aéreo o

sistemas de control de armas, en los cuales una falla podría causar la muerte, un daño personal o severos daños al medio ambiente.

2.4 Tarifas

El Suscriptor se obliga a pagar a Certinet y/o a las Autoridades de Registro que se establezcan, las tarifas establecidas para los Certificados cuya emisión se solicite.

El pago señalado tiene como causa y fundamento exclusivamente la emisión del Certificado y según corresponda, el servicio de custodia central segura, por lo que su no aceptación posterior por una causal distinta a errores o inexactitudes, o por su no uso, no libera al Suscriptor de dicho pago ni lo autoriza para pedir reembolso alguno.

2.4.1. Clases de Tarifas

Certinet cobrará una tarifa diferente por cada uno de los servicios que otorgue. Estos servicios son:

a) Emisión y Renovación de certificados

Los suscriptores se obligan a pagar a Certinet y/o a las Autoridades de Registro que se establezcan, las tarifas establecidas para los Certificados cuya emisión y/o renovación se solicite.

b) Acceso base a información de Certificados

El acceso a la información de estado de los certificados de firma electrónica avanzada emitidos u homologados por Certinet que de conformidad con el Reglamento de Ley debe estar disponible para los usuarios, no tendrá costo alguno.

c) Otros Servicios

Otros servicios tales como suspensión, revocación, sello electrónico, custodia de documentos, acceso en línea información de estado, servicio de custodia central segura y cualquier otro servicio actual o futuro que se incorpore, tendrán tarifas que serán publicadas por Certinet en el sitio www.certinet.cl

2.4.2. Política de Devoluciones

En el evento que un Suscriptor determine devolver un certificado ya sea aceptado o no, este será revocado y la tarifa pagada no será devuelta.

2.5 Publicaciones y Repositorio

La CPS Certinet estará disponible para los Suscriptores, Usuarios y público en general a título de información vía electrónica en una página Web contenida en el repositorio de documentos de Certinet en el sitio Web www.certinet.cl.

Se contempla una publicación material del original, cuya exactitud y veracidad deberá ser refrendada mediante la protocolización correspondiente, y el depósito ante el Ente Acreditador cuando corresponda.

Cualquier cambio o modificación en la CPS Certinet generará una nueva versión, debiendo publicarse dicho cambio, además de guardar y custodiar la versión anterior, toda vez que al amparo de esta última pudiesen haberse originado derechos y obligaciones para los Suscriptores y Usuarios de las mismas.

Todas aquellas situaciones de vigencia de Certificados y de obligaciones contraídas, se resolverán de acuerdo a la “CPS Certinet” vigente al momento de la emisión del Certificado en cuestión.

Los respectivos elementos de información de Certinet serán publicados en las siguientes direcciones electrónicas (URL):

Objeto	Dirección
Prácticas de Certificación Vigentes	http://www.certinet.cl/2c_PracticasCertificacion.asp
Directorio de Certificados Emitidos	En www.certinet.cl en Atención al Cliente, opción Directorio de Certificados emitidos
Directorio de Certificados Firma Electrónica Avanzada Revocados y Suspendidos	http://onsitecrl.verisign.com/CertiNetSAFirmaElectronica/LatestCRL.crl

2.6 Auditorías

Certinet considera efectuar auditorías a sus instalaciones por parte de una empresa externa, comprometiéndose a corregir dentro de un plazo razonable, las eventuales deficiencias que se puedan encontrar.

Adicionalmente, Certinet auditará a las Autoridades de Registro asociadas cuando lo estime conveniente, incluyéndose al menos, una auditoria al iniciar la operación como Autoridad de Registro. La Auditoria en este caso podrá ser desarrollada por personal de Certinet o por empresas externas de prestigio y conocimiento del proceso de certificación.

2.7 Privacidad y Confidencialidad

El contenido de los Certificados emitidos por Certinet y el Registro Público de Certificados es información de público conocimiento, y puede contener datos personales de los Suscriptores que sean necesarios para dicho efecto de conformidad con el artículo 12 letra b) de la Ley de Firma Electrónica.

No obstante lo anterior, Certinet quedará sujeto a la obligación de reserva, de conformidad con la Ley N° 19.628 sobre Protección de la Vida Privada, respecto de los atributos, datos personales y antecedentes que reciba de los Suscriptores para la solicitud de Certificados, y respecto de las operaciones o información a que eventualmente pudiese acceder como consecuencia de los servicios que presta.

Certinet, en cumplimiento de lo dispuesto en la Ley N° 19.628, sobre Protección de la Vida Privada, y considerando los principios internacionales de protección de datos, informa a usted que los datos que le son solicitados en este acto serán utilizados, únicamente, con la finalidad para la cual se han recabado. Al titular de los datos personales se le informa que podrá ejercer respecto de aquéllos, los derechos de acceso, rectificación o modificación, cancelación o eliminación y bloqueo, en forma independiente y gratuita ante Certinet. Para ello deberá efectuar una solicitud por escrito en Huérfanos 1052, Piso 12, en Santiago de Chile, cuyo horario de atención es de 9 a 17 horas y, en caso de contar con mecanismos para acreditar su identidad, como la firma electrónica avanzada u otro medio, también, podrá hacerlo por vía electrónica, a la dirección de correo electrónico: soporte@certinet.cl

Igual obligación recaerá en las Autoridades de Registro que actúan por cuenta de Certinet.

La prohibición anterior no regirá si media alguna disposición legal o resolución judicial que obligue a Certinet a someter materias sujetas a secreto, reserva o confidencialidad al conocimiento de los Tribunales de Justicia, instituciones o entidades facultadas por ley y que actúen dentro de sus atribuciones.

Certinet se obliga a utilizar los datos obtenidos sólo para funciones asociadas al ciclo de vida de los Certificados, y respetar los derechos de los Suscriptores en los términos de la Ley N° 19.628 sobre Protección de la Vida Privada y 19.496 sobre Protección a los Derechos de los Consumidores. 2.8 Propiedad Intelectual

En consecuencia, queda prohibida su reproducción total o parcial, por cualquier medio y de cualquier forma sin expresa autorización previa de Certinet.

Adicionalmente, Certinet es dueño de la propiedad intelectual y de los derechos de la información de certificados que se mantienen en forma pública, por lo que esta información no puede ser extraída ni copiada sin previo acuerdo con Certinet.

3. Identificación y Autentificación

En este capítulo se describe el proceso general para la solicitud de certificados, la entrega de la información requerida y los mecanismos de generación de claves o datos de creación de firma.

Se analiza además, cada una de las etapas del ciclo de vida de un Certificado que va desde que son emitidos hasta que caducan. Los procedimientos específicos se describen en las Prácticas específicas de Certificados (CP).

3.1 Registro Inicial

Sin perjuicio de los requisitos particulares que las Prácticas de los Certificados (CP) exijan, previo a la emisión inicial de un “Certificado de Firma Electrónica Avanzada”, el solicitante deberá ya sea:

a) Comparecer en forma personal y directa si se trata de una persona natural, ante Certinet o ante la Autoridad de Registro que actuando por cuenta, riesgo y en representación del primero, éste hubiere autorizado.
b) Comparecer frente a un Notario para la identificación, el modelo de registro notarial como indica la ley de firma electrónica.
c) Comparecer usando la autenticación de la clave única según lo establecido en el Decreto N° 24 de MINECON de 2019.

Todas las Autoridades de Registro Autorizadas por Certinet para operar en el Modelo Bancario, realizarán un procedimiento para identificar y registrar a un Suscriptor de certificados, de modo tal de ofrecer un grado de confianza equivalente para cualquier Suscriptor de un certificado emitido por Certinet para este modelo, independiente de la Autoridad de Registro Autorizada que haya efectuado dicho proceso.

3.1.1. Presentación de Antecedentes.

Toda persona que desee obtener un Certificado emitido por Certinet, debe presentar a la Autoridad de Registro correspondiente, los siguientes antecedentes:

Tipo de Certificado	Antecedentes Requeridos
Firma Electrónica Avanzada	Comparecer en forma personal o notarial o con clave única ante una Autoridad de Registro Autorizada por Certinet proveyendo: • Solicitud con sus antecedentes personal debidamente firmada • Cédula nacional de identidad vigente • Acceso a servicios de cliente en alguno de los Bancos incluidos en el Modelo o acceso al sistema denominado “ClaveUnica” • Foto y Huella digital (según el modelo utilizado) • Correo electrónico • Teléfono móvil para activación y/o para segundo factor

3.1.2. Existencia de antecedentes previos

No serán requeridos aquellos antecedentes necesarios para la emisión de certificados, cuando estos ya constaran fehacientemente en poder de Certinet, de una Autoridad de Registro Autorizada o que sea acreditada la identidad mediante el sistema denominado “ClaveUnica”.

Tampoco será necesario acompañar dichos antecedentes si la solicitud de emisión de un certificado se firma con Firma Electrónica Avanzada, adjuntando otro certificado vigente emitido por Certinet que cumpla con estas características.

No obstante lo anterior, los antecedentes necesarios deberán custodiarse en los términos señalados por la Ley de Firma Electrónica y su Reglamento.

3.1.3. Asignación de nombres.

Para los efectos de asignar los nombres a ser incluidos en el certificado, se utilizará el siguiente criterio:

- Certificado Firma Electrónica Avanzada: Se incluirán los mismos nombres que señala la cédula nacional de identidad u otro documento similar, con uno, dos, tres nombres y dos apellidos o los nombres que consten en el Sistema ClaveUnica.

3.1.4. Generación de claves

El Suscriptor de Certificado de Firma Electrónica Avanzada, debe ser capaz de generar sus datos de creación de firma o clave privada y su correspondiente clave pública, en forma segura y bajo su exclusivo control; para esto deberá utilizar los dispositivos de almacenamiento seguro que hayan sido validados por Certinet respecto del cumplimiento de los estándares de seguridad u optar por el servicio de custodia central seguro provisto por Certinet. Este es un requisito esencial para obtener un certificado de este tipo.

3.1.5 Protección de claves

El Suscriptor es el único responsable de la protección de sus datos de creación de firma o clave privada cuando disponga del dispositivo o del mecanismo complementario de activación, para lo cual deberá tomar los resguardos y mecanismos que estime suficiente para prevenir la pérdida, compromiso, revelación, mal uso o uso no autorizado de la misma.

Certinet y/o las Autoridades de Registro, no generan, ni mantienen ni protegen datos de creación de firmas o claves privadas para los Suscriptores de certificados de Firma Electrónica Avanzada, excepto para los clientes que optan por usar el servicio de custodia central seguro de Certinet.

Con el objeto de dar cumplimiento a lo establecido en el artículo 5° del Decreto N° 24 de 2019 del Ministerio de Economía Fomento y Turismo, conocido como "Norma Técnica de Seguridad", en el caso que se emitan certificados utilizando el medio de comprobación digital se informa que Certinet opera un Servicio de Custodia Segura, el cual se trata de un servicio central protegido y que permite al titular tener el control exclusivo del acceso y utilización de su certificado. De acuerdo a la norma citada se hace una mención específica respecto la fiabilidad que estos tienen:

El servicio se basa en la reciente certificación del producto clase mundial Ascertia para que sus sistemas puedan operan con Firma Remota de acuerdo con la norma eIDas (Electronic Identification and Signature), que es un Reglamento de la Comunidad Economica de Europa que regula la identificación electrónica y establece las pautas para los servicios de confianza relativos a las transacciones electrónicas. La normativa entró en vigor el 1 de julio de 2016 como Reglamento (UE) nº 910/2014.

La norma europea permite que el Cliente logre el control exclusivo de acceso y utilización, equivalente al Token.

En lo específico, este Servicio de Custodia Segura, fue acreditado con las siguientes normas:

- ISO/IEC 15408 (Common Criteria) versión 3.1 logrando la evaluación EAL4+ (nivel 4+).
- CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1 para poder operar como Qualified Certificate Service Providers (CSPs).

- FIPS 201 con GSA EPL #1411.
- FIPS 140-2

3.1.6 Uso de claves

En el evento que el Suscriptor autorice el uso de sus datos de creación de firma o clave privada por parte de terceros, los actos celebrados con ellos serán de su exclusiva responsabilidad, puesto que el titular sigue siendo el responsable por el uso que de ella se haga. Lo cual no obsta a que Certinet haga expresa reserva de las acciones legales que procedieren contra terceros en sede civil, administrativa o penal.

3.2 Identificación frente a otras solicitudes

3.2.1 Solicitud de Suspensión

Frente a una solicitud de suspensión se requiere efectuar un proceso de identificación similar al utilizado para emitir un certificado, es decir, se requiere confirmar que la persona que solicita la suspensión sea efectivamente el Suscriptor; esto se hace por medio de las siguientes alternativas:

- Comunicación con la Autoridad de Registro por medios electrónicos para efectuar un procedimiento de identificación que permita identificar fehacientemente al Suscriptor, posteriormente deberá ratificar por Correo electrónico firmado digitalmente a Certinet esta Solicitud.

- Notificación enviada por el Suscriptor a la Autoridad de Registro o a Certinet utilizando Firma Electrónica Avanzada, según corresponda.

- Por comparecencia personal ante la Autoridad de Registro o ante Certinet.

- Por comprobación mediante el sistema denominado ClaveUnica, según lo establecido en el Decreto N° 24 de MINECON de 2019.

3.2.2 Solicitud de Revocación

Frente a una solicitud de Revocación iniciada por el Suscriptor, se requiere efectuar un proceso de identificación similar al utilizado para emitir un certificado, es decir, se requiere confirmar que la persona que solicita la revocación sea efectivamente el Suscriptor; esto se hace a través de:

- Notificación enviada por el Suscriptor a la Autoridad de Registro o a Certinet utilizando Firma Electrónica Avanzada vigente.
- Por comparecencia personal ante la Autoridad de Registro o ante Certinet

Por comprobación mediante el sistema denominado ClaveUnica, según lo establecido en el Decreto N° 24 de MINECON de 2019.

3.2.3 Solicitud de Renovación

Frente a una solicitud de renovación, existen dos formas de proceder dependiendo si el Suscriptor dispone o no de una Firma Electrónica Avanzada vigente, según corresponda,

A) Sin Firma Electrónica Avanzada Vigente

En este caso se requiere efectuar un proceso de identificación con comparecencia personal idéntico al procedimiento usado para obtener el primer certificado de Firma Electrónica Avanzada.

O bien cumplir con lo establecido para la comprobación de identidad en el sistema denominado ClaveUnica, según lo establecido en el Decreto N° 24 de MINECON de 2019.

B) Con Firma Electrónica Avanzada Vigente

En el caso de disponer de Firma Electrónica Avanzada, basta completar y firmar los antecedentes que solicita la Autoridad de Registro al momento de generar la solicitud de renovación. La firma deberá ser generada utilizando la Firma Electrónica Avanzada vigente del mismo suscriptor.

4. Requerimientos Operacionales

En este capítulo se describen los procedimientos específicos asociados al ciclo de vida de los certificados que emite Certinet.

4.1. Emisión de Certificados

4.1.1 Presentación Solicitud de Certificados

Toda persona que desee obtener un Certificado de Firma Electrónica Avanzada emitido por Certinet, debe completar el formulario de solicitud de Certificado, indicando el mecanismo de custodia de su certificado según las opciones provistas por CERTINET y presentarse a la Autoridad de Registro correspondiente, cumpliendo los requisitos establecidos en la normativa vigente o adjuntando la información que se indicó en el capítulo anterior.

4.1.2 Comprobación de Solicitudes

Las Autoridades de Registro deberán comprobar y validar los elementos que son requeridos de conformidad con el numeral 3.1.1.

Para estos efectos el solicitante autoriza y faculta expresamente a Certinet y/o a la Autoridad de Registro para verificar los antecedentes entregados con otras bases de datos públicas o privadas.

Certinet y/o la Autoridad de Registro, deberá mantener un archivo con la información que respalde cada solicitud que remita para emisión de Certificados, por el período que determina la Ley de Firma Electrónica y su Reglamento.

Este nivel de verificación de identidad permite a Certinet ofrecer la seguridad y confianza del Sistema a todo Suscriptor y Usuario de certificados de Firma Electrónica Avanzada respecto de

la identidad y autenticidad del certificado emitido, en la medida que siga las prácticas que estén vigentes.

4.1.3 Aceptación de la Solicitud

Si el proceso de validación y comprobación de antecedentes resultó exitoso, la Autoridad de Registro, aceptará la solicitud de emisión de certificado.

4.1.4 Rechazo de la Solicitud

Aquellos solicitantes que no dispongan de la adecuada información, que no acrediten mediante el sistema de ClaveUnica o que los antecedentes que presenta no sean concordantes, se les rechazará la solicitud sin expresión de causa.

El Solicitante podrá con posterioridad iniciar nuevamente el proceso de solicitud de Certificado.

4.2 Emisión de Certificados

En el caso de el enrolamiento presencial, una vez que Certinet y/o la Autoridad de Registro aprueba la solicitud, ésta debe ser enviada a Certinet en un formulario el cual contiene solamente los antecedentes requeridos para la emisión del certificado. En el caso de la Autoridad de Registro distinta a Certinet, ésta será firmada electrónicamente.

Para los certificados que se enrolen por medio del sistema ClaveUnica, sólo Certinet aprobará la solicitud.

Certinet solamente emitirá certificados con el consentimiento del Suscriptor: Se entiende que existe consentimiento para la emisión por el sólo hecho de que se presente una solicitud de emisión de certificado.

El Certificado y su contenido son de propiedad exclusiva de Certinet y se emitirá con carácter personal e intransferible a nombre del Suscriptor.

4.3 Aceptación del Certificado por parte del *Suscriptor*

Se entiende que un certificado ha sido aceptado por parte del Suscriptor una vez que: i) este haya sido emitido por Certinet, aun cuando el certificado no haya entrado en vigencia por contener una fecha de inicio de operación posterior a su fecha de emisión, ii) No se haya formulado un reclamo por error o inexactitud en la emisión, al momento de su recepción, iii) La utilización, por parte del "Suscriptor", de una Clave de Confirmación comunicada por Certinet para retirar el Certificado o la instalación o utilización de cualquier modo del Certificado, es considerada como la aceptación del Certificado por parte del "Suscriptor".

Aceptando el Certificado, el Suscriptor confirma y acepta lo siguiente:

a) que cada firma electrónica avanzada creada utilizando sus datos de creación de firma o clave privada es la firma del Suscriptor
b) la exactitud del contenido del mismo y la veracidad de la información entregada a Certinet o a la Autoridad de Registro,
c) que no divulgará sus datos de creación de firma o clave privada
d) que asume las obligaciones con Certinet y con cualquier usuario que confíe en la información del certificado y
e) que acepta en forma expresa los términos y condiciones de las "CPS Certinet" y las Prácticas específicas para cada tipo de Certificado.

4.4 Vigencia del Certificado

Los certificados emitidos por Certinet tendrán la siguiente vigencia:

Tipo	Duración
Firma Electrónica Avanzada Estándar de seguridad: SHA2:	1 año, o menos según solicitud del Suscriptor.

Todos los certificados se consideran vigentes desde el momento de su emisión y hasta la fecha de expiración o revocación, salvo que el propio certificado indique una fecha de entrada en vigencia posterior a la fecha de emisión, en cuyo caso el certificado entra en vigencia en la fecha que se indique.

4.5 Uso de los certificados.

Solamente se podrán utilizar certificados durante su período de vigencia.

4.5.1 Verificación de Firma

La verificación de la Firma Electrónica Avanzada de un documento o mensaje se efectúa para determinar que:

(1) La Firma Electrónica Avanzada fue creada por los datos de creación de firma o la clave privada se corresponde con la clave pública contenida en el Certificado del Suscriptor que firma y, que

(2) el mensaje o documento no ha sido alterado desde que la Firma Electrónica Avanzada ha sido creada.

Esta verificación debe hacerse en forma consistente con esta “CPS Certinet” de la siguiente manera:

- Establecer la cadena de Certificación del Certificado (emisor y sus respaldos) y verificar que sea un Certificado emitido por o en relación de confianza directa con Certinet.
- Verificar el Registro Público de Certificado de Certinet para determinar si el certificado no ha sido suspendido ni revocado. En el caso de certificados encadenados previos al de Certinet, se debe verificar esto para todos ellos.
- Delimitar la información que haya sido firmada. Para esto los mensajes o documentos firmados deben seguir los estándares PKCS, XMLDSIG, ETSI vigentes.
- Establecer el propósito que intenta el Suscriptor con esta firma. Para lo anterior, debe verificar que los atributos del certificado del Suscriptor sean los adecuados para firmar dicho mensaje o documento.

4.5.2 Efecto de validar al *Suscriptor*

Una Firma Electrónica Avanzada genera efectos legales para el que la produce, a través de sus datos de creación de firma o clave privada si:

(1) fue creada durante el período de vigencia de un certificado de Firma Electrónica Avanzada válidamente emitido de acuerdo a la “CPS Certinet”,

(2) dicha Firma Electrónica Avanzada puede ser verificada por medio de la cadena de verificación

(3) el tercero que confía no tiene conocimiento o información del incumplimiento de esta "CPS Certinet" por parte del Suscriptor y,

(4) el tercero que confía ha cumplido con todos los requisitos de esta "CPS Certinet".

4.5.3 Responsabilidad ante la no Verificación de una firma Electrónica

Un usuario que confía en una Firma Electrónica Avanzada que no ha sido verificada en forma total, por cualquier razón, asume todos los riesgos y no puede hacer ninguna presunción de que la firma es válida bajo los términos de esta "CPS Certinet".

4.5.4 Confianza en la Firma Electrónica

El usuario que confía en un mensaje o documento firmado electrónicamente por un Suscriptor puede confiar en la Firma Electrónica Avanzada acorde a esta "*CPS Certinet",* si:

(1) La Firma Electrónica Avanzada fue creada en el período de vigencia de un certificado de Firma Electrónica Avanzada, lo cual puede ser verificado siguiendo la cadena de certificación y,

(2) dicha confianza es razonable de acuerdo a las circunstancias. Si las circunstancias indican que se deben tomar medidas de confirmación adicionales, tales como recibos digitales, consultas en línea u otros, el usuario que confía debe tomar dichas medidas adicionales de modo que la confianza resulte razonable.

La decisión de confiar o no en una determinada Firma Electrónica Avanzada la toma en forma libre y exclusiva quien realiza la verificación.

4.5.5 Efectos

a) El mensaje o documento electrónico que contenga una Firma Electrónica Avanzada válidamente emitida será válido y producirá los mismos efectos que un mensaje escrito y soportado en papel. Su valor probatorio se encuentra establecido en el artículo 5º números 1 y 2 de la Ley Nº 19.799, "Ley de Firma Electrónica" y su Reglamento asociado, y sus modificaciones posteriores.

b) Cuando la ley requiera una firma para dar validez a un acto o prevea ciertas consecuencias por su ausencia, este requisito se entenderá satisfecho respecto de un mensaje electrónico cuando el Suscriptor de un certificado cree una Firma Electrónica Avanzada, con la intención de firmar dicho mensaje.

4.6 Suspensión y Revocación de Certificados

4.6.1. Suspensión de los Certificados

Certinet podrá suspender la vigencia de un Certificado cuando se constate o verifique alguna de las siguientes circunstancias:

a) Solicitud del Suscriptor de un Certificado
b) Decisión unilateral de Certinet en el caso que constate razones técnicas que así lo justifiquen. Se entenderá por razones técnicas entre otras, las irregularidades en el Sistema, las situaciones de compromiso de seguridad, las fundadas sospechas de que la clave privada del Suscriptor ha sido comprometida, etc.

Para los efectos señalados en la letra a) el Suscriptor deberá realizar una de las siguientes acciones:

- Comunicación con Certinet o la Autoridad de Registro por medios electrónicos que permitan efectuar un procedimiento de identificación que involucre el conocimiento de secretos compartidos que permitan identificar positivamente al Suscriptor, o por la verificación en el sistema de ClaveUnica.
- Notificación enviada por el Suscriptor a la Autoridad de Registro o a Certinet utilizando Firma Electrónica Avanzada, según corresponda.
- Por comparecencia personal ante la Autoridad de Registro o Certinet a la cual solicitó el Certificado

4.6.2 Efectos de la Suspensión

La suspensión tiene como principal efecto el cese temporal del período de vigencia del Certificado.

Los terceros que confíen en certificados emitidos por Certinet deberán verificar si tienen indicado el estado de Suspensión usando los sistemas de validación en línea de certificados (OCSP), si este fuera el caso, deberán abstenerse de operar con ellos.

Los Suscriptores deberán cuidar con igual diligencia que para un certificado vigente, la clave privada correspondiente a todo el período de un certificado suspendido, hasta la destrucción de las claves.

4.6.3 Término de la Suspensión

La suspensión de un Certificado terminará por:

a) Decisión de Certinet de revocar el Certificado, una vez comprobado alguna de las causales establecidas en el Numeral 4.6.1.

b) Decisión de Certinet de levantar la suspensión una vez que las cesen las causas que lo originaron.

c) Por solicitud del Suscriptor cuando la suspensión haya sido solicitada por este.

4.6.4 Revocación

La Revocación es la cancelación anticipada del período operativo de un Certificado válidamente emitido.

Certinet procederá a revocar un Certificado válidamente emitido en las siguientes circunstancias:

a) A solicitud del titular del Certificado.

b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso.

c) Por incapacidad sobreviniente del titular, quiebra o notoria insolvencia.

d) Por resolución judicial ejecutoriada.

e) Por declaraciones inexactas o incompletas en los datos aportados por el Solicitante para la obtención de un Certificado.

f) Por compromiso de la clave del Suscriptor o de Certinet.

g) Por cese de la actividad de Certinet, a menos que los Certificados sean transferidos a otro Prestador.

h) Por incumplimiento de parte del Suscriptor de las obligaciones establecidas en estas "CPS Certinet".

Los certificados que son revocados serán publicados tanto en las CRL de Certinet como en los sistemas de consulta en línea (OCSP), que corresponden a listas de certificados que no son válidos.

Estas listas contienen los números de serie de los certificados revocados y están firmados electrónicamente por Certinet.

4.6.5 Efectos de la Revocación

La revocación tiene como principal efecto la terminación inmediata del período de vigencia del Certificado y, como consecuencia de lo anterior, se impide su uso para los fines con que fue solicitado.

4.6.6 Fecha de Inicio de Efectos de la Suspensión o Revocación

La Revocación o la Suspensión, en su caso, operarán desde el momento en que efectivamente sean verificadas por Certinet y sean publicadas en la CRL. La publicación en la CRL no podrá ser en un plazo superior a las 24 horas.

En ningún caso la Revocación o Suspensión afectarán el valor de los Certificados y los derechos y obligaciones constituidos bajo su vigencia, en un momento anterior a dicha verificación.

El término de la Suspensión por levantamiento de la misma deja vigente el Certificado por todo el tiempo que resta hasta su fecha de término de vigencia original.

4.6.7 Procedimientos para Suspender o Revocar un Certificado

La revocación se efectuará una vez que se confirme que la persona que solicita la revocación sea efectivamente el Suscriptor, mediante:

- Notificación enviada por este último y además su comparecencia personal ante Certinet o ante la Autoridad de Registro correspondiente, a fin de ratificar la información enviada.
- Notificación usando ClaveUnica
- Utilizando una Firma Electrónica Avanzada vigente certificada por Certinet

4.7 Renovación de Certificados

La renovación se produce cuando el Certificado va a expirar y el Suscriptor desea continuar usando un Certificado. Para esto el Suscriptor deberá presentar una solicitud de Renovación en los términos que Certinet haya definido y realizar el mismo proceso utilizado para solicitar un certificado, excepto que no será necesario acompañar los antecedentes que ya se encuentran en poder de Certinet o la Autoridad de Registro, salvo que existan nuevas informaciones o cambios no informados.

Sin perjuicio de lo anterior, Certinet o la Autoridad de Registro correspondiente, realizará razonables esfuerzos para notificar la pronta expiración del certificado, a través de un correo electrónico a la dirección de e-mail registrado del Suscriptor. Este aviso se enviará con la antelación necesaria para que el Suscriptor pueda iniciar el proceso de Renovación correspondiente.

Esta notificación está establecida sólo en beneficio del Suscriptor, para facilitarle el proceso de Renovación antes indicado, por lo que Certinet ni la Autoridad de Registro asumen obligación alguna en este sentido.

4.8 Procedimientos de Auditoría de Seguridad

Certinet podrá ser Inspeccionado y/o Auditado en los términos y condiciones establecidas en la Ley de Firma Electrónica y el Decreto Supremo N°181 de 2002 del MINECON.

Por su parte, Certinet efectuará en forma periódica Auditorias de Seguridad a los procedimientos de registro delegados a las Autoridades de Registro. En el Sitio Web de la Certificadora se indicará la fecha de la última auditoria efectuada a cada Autoridad de Registro

4.9 Archivo de Registros

Certinet dispondrá de registros históricos, acorde a sus prácticas, en los cuales mantendrá la información del proceso de registro y estado del certificado durante todo el período de vida de los documentos involucrados. Esta información específicamente es:

- Archivos de antecedentes utilizados para el Registro
- El contenido del Certificado emitido.
- Información del Estado del Certificado: Emisión, Suspensión, Revocación, Renovación.

Esta información será mantenida desde la fecha de emisión del certificado incluyendo los datos de la solicitud al menos por seis años.

La información anterior se mantendrá accesible por medios electrónicos hasta un año después de su revocación o expiración del certificado; posteriormente se mantendrá accesible en forma expedita frente a solicitudes específicas.

En el caso que se trate de información almacenada asociada a los servicios adicionales prestados, tales como: Time Stamp, Custodia y Verificación de Documentos, Consultas en Línea de estado de Certificado, su duración y condiciones de Almacenamiento serán definidas en función del Servicio mismo, cuando este sea ofrecido.

4.10 Cesación de Actividad de Certinet.

En el evento que Certinet cesara voluntariamente de realizar su actividad, se obliga a:

a) Comunicar el cese de la actividad a cada uno de los Suscriptores con Certificados vigentes, por medio de correo electrónico, con una antelación mínima de dos meses a la fecha de término.

b) Transferir con consentimiento previo del Suscriptor, los datos del Certificado a otro Prestador de Servicio de Certificación activo. Se entenderá que existe consentimiento del Suscriptor si una vez recibida la comunicación señalada en la letra a), el Suscriptor no manifiesta su oposición dentro los quince días hábiles siguientes.

c) Existiendo oposición del Suscriptor, el Prestador de Servicios de Certificación deberá dejar sin efecto los Certificados correspondientes.

d) Hacer esfuerzos razonables para que el término de sus servicios cause los mínimos inconvenientes a sus Suscriptores y quienes necesiten verificar firma electrónica y/o firma electrónica avanzada cuando corresponda.

e) Pagar una restitución razonable que no excederá el costo de los certificados a los Suscriptores activos que no consientan el traspaso indicado en la letra b) y soliciten la restitución del dinero pagado. Se deducirá de esta restitución el costo proporcional del certificado que medie entre su fecha de emisión y su fecha de revocación, correspondiente al tiempo efectivamente activo.

5. Control Físico, Procedimientos y Personal

5.1 Control Físico

La ubicación física de la unidad que otorgue los servicios de certificación no será publicada en las "CPS Certinet" por razones de seguridad; no obstante su dirección legal para todos los efectos que sean requeridos será la dirección de la sociedad ubicada en Huérfanos 1052, piso 13, Santiago, Chile. El acceso físico a la sociedad dispone de un esquema de control de acceso.

El acceso físico a la unidad que otorga los servicios de certificación será bajo estrictas normas de seguridad y monitoreo incluyendo esquemas electrónicos de identificación y control, adicionalmente, este lugar dispone de elementos adecuados para la operación tales como aire

acondicionado, sistema de detección y prevención de incendios, almacenamiento seguro de material confidencial, esquema seguro de respaldos externos para eventuales catástrofes.

5.2 Procedimientos de Control

El control de las funciones se efectuará por medio de disponer de:

- Adecuada segregación de funciones
- Control dual de las funciones críticas
- Identificación y autenticación de cada rol

5.3 Compromisos de Seguridad y Recuperación de Desastres

Las Prácticas de Certificación no establecen como parte de su contenido un Plan de Contingencia en el caso de presentarse problemas en el desarrollo de sus operaciones. Sin embargo, se describe a continuación en forma somera la seguridad que disponen las aplicaciones de Certinet.

Dentro de los procedimientos y planes que dispone Certinet, se incluye el Plan de Contingencia específico.

Un Prestador de Servicios de Certificación es un servicio de disponibilidad 24x7 por lo cual la solución tecnológica utilizada considera las medidas necesarias de recuperación en caso de contingencia o desastre, ya sea tecnológico, operacional o incluso de confianza producto de aspectos de seguridad comprometidos.

Certinet estará preparada para atender dos tipos de contingencias:

- Falla de una o más componentes del Servicio
- Desastre que involucre el Sitio de Procesamiento

A continuación se describe cada una de ellas:

5.3.1 Alta Disponibilidad

En el eventual escenario de no disponibilidad por la falla de una o más componentes, se evitarán las consecuencias negativas en el servicio mediante una configuración de alta disponibilidad, por medio de la duplicación de los servicios y equipos necesarios para otorgar los Servicios críticos asociados a la Certificación, tales como consulta en línea del estado de los certificados, de modo que puedan restablecerlos en un plazo que no afecte la calidad del servicio.

Dentro de los elementos duplicados para los sistemas críticos se incluyen servidores, conexiones de red, *switches* y *routers*. Adicionalmente, se consideran conexiones a diferentes proveedores de servicios Internet que utilicen diferentes *Backbones* de modo de asegurar el acceso expedito desde diferentes proveedores de conexión Internet.

Desde el punto de vista de las componentes principales que conforman un Prestador de Servicios de Certificación (Certificadora, Autoridad de Registro, acceso al sistema ClaveUnica, OSCP y CRL) y los servicios que sustentan, se da un mayor énfasis a los servicios de certificación que se encuentran en el servidor que contiene la componentes de consulta en línea del estado del Certificado (OSCP), los servicios para revocación en línea y el acceso a la CRL para la validación de certificados que se encuentran en uso.

5.3.2 Soporte de Desastres

Tratándose de un caso de desastre, para los sistemas críticos se dispone de un sitio alternativo remoto de procesamiento, para asumir las funciones, con indicación de los niveles de servicio y tiempo de recuperación comprometidos para continuar con los servicios de Certinet.

Para los servicios no críticos en cuanto a disponibilidad se dispone de un Plan de Contingencia probado que permite restablecer dichos servicios en un plazo adecuado a los tiempos involucrados con la emisión de Certificados.

Complementario a la solución de alta disponibilidad, se mantiene un sistema de respaldo de toda la información y sistemas. Por la criticidad de los datos involucrados en un Prestador de Servicios de Certificación y en este caso específico para la industria bancaria, es imprescindible que de estos se almacenen copias en un sitio geográfico diferente o a través de servicios en la nube.

Para asegurar la adecuada reposición de los servicios, en caso de fallas, se mantienen documentados y publicados los procedimientos necesarios, contemplando el máximo de casos posibles y definiendo los responsables de cada tarea involucrada, para lo cual se dispone de un Plan de Contingencia auditable, administrado por una función del negocio del Prestador de Servicios.

5.4 Control del Personal

Las personas que cumplen roles dentro de los servicios de certificación son incorporados por medio de estrictos procedimientos de contratación que aseguren su alta confiabilidad para trabajar en este tipo de empresa.

Adicionalmente, se dispone de una clara definición de funciones para cada empleado de la empresa, lo cual podrá ser auditado por los organismos correspondientes cuando sea requerido.

Dentro de los elementos que se consideran es el disponer de un procedimiento claro, auditable y no discriminatorio para la postulación, selección y contratación del personal.

6. Controles de Seguridad Técnica

6.1 Generación del Par de Claves e Instalación

Modelo de Certificación Bancario para Firma Electrónica Avanzada las claves serán generadas por un mecanismo el que estará siempre bajo el control exclusivo del Suscriptor. Las claves podrán ser creadas y almacenadas, en los siguientes contenedores:

6.1.1 *Token*

Un Token es un dispositivo con capacidad de almacenamiento y procesamiento que se conecta al PC por medio de una puerta USB dentro del cual se pueden generar, guardar y efectuar procesamientos con las claves al interior del mismo dispositivo, efectuándose así todas las funciones de seguridad y criptográficas en forma segura.

Los Tokens que han sido validados y por lo tanto están autorizados para ser usados en el Modelo Bancario Certinet están descritos en el Sitio Web de Certinet. Al utilizar un *Token* autorizado por Certinet, lea cuidadosamente las indicaciones de generación de claves y almacenamiento de clave privada.

6.1.2 Custodia Central

En caso que el cliente opte por el Servicio de Custodia Central, el cliente deberá utilizar un teléfono móvil que disponga un elemento seguro que permita, sea través de clave, o de biometría, activar sus llaves que quedaran en custodia en un dispositivo de alta seguridad con modulo criptográfico HSM, que al igual que los token permite realizar las funciones criptográficas en forma segura.

El HSM (Hardware Security Module) se trata de un dispositivo criptográfico basado en hardware que genera, almacena y protege múltiples claves criptográficas (en especial la firma electrónica avanzada) y que permite firmar una serie de documentos electrónicos. Por lo tanto, este Hardware está diseñado y certificado para almacenar y proteger los certificados (claves privadas) de los Suscriptores frente al acceso no autorizado de terceras personas a tales dispositivos criptográficos y permite un mayor rendimiento en la emisión de documentos electrónicos firmados con una firma electrónica avanzada. Una vez emitido el certificado éste será almacenado en un Repositorio o Banco de Firmas Electrónicas (HSM) el cual lo mantendrá de manera segura y entregará exclusivo control a su titular, quien, además, podrá revocar dicho certificado cuando lo estime conveniente, según lo prescrito en el presente instrumento.

El servicio implementado por Certinet de Custodia Central (HSM), se basa en sistema que fue acreditado según la regulación eIDAS (910/2014) reconoce la “firma remota” que en el caso de Europa permite la creación de tanto la Firma Avanzada y Cualificada según su modelo. Los HSM que han sido validados y por lo tanto están autorizados para ser usados en el Modelo Certinet esta tecnología permite dar cabal cumplimiento a la “Norma Técnica de Seguridad” contenida en el Decreto Supremo N° 24 del MINECOM, publicada el 9 de abril del 2019 en el Diario Oficial.

6.2 Protección de la Clave Privada

Respecto de la protección de la Clave Privada se debe considerar:

a) Protección del Solicitante y Suscriptor: La clave privada debe ser protegida permanentemente por el Solicitante y/o Suscriptor, incluso cuando el certificado esté en calidad de suspendido.

b) Certinet, y/o La Autoridad de Registro bajo ninguna circunstancia mantienen, custodian, protegen o accesan las claves privadas pertenecientes a Solicitantes o Suscriptores, cuando usan dispositivos seguros como Token.

c) En el caso que del mecanismo escogido libremente el suscriptor sea el Servicio de Custodia Central Segura de Certinet, la activación de la clave privada será solo autorizada por el dispositivo móvil del Suscriptor usando se aplican los más altos estándares de seguridad y protección, como es el Reglamento (UE) eIDas.

Dependiendo del tipo de contenedor de la clave, deben tenerse en cuenta al menos las siguientes precauciones:

6.2.1 Claves en *Token* USB

Certinet publicará la lista de los *tokens* autorizados los que deberán cumplir con los requisitos de seguridad de Certinet, indicando específicamente las opciones de claves que se requiere manejar.

6.2.2 Claves en Servicio de Custodia Central Segura Certinet

Certinet por tratarse de información confidencial, informará de manera privada a los organismos reguladores del Servicio de Custodia Central Segura. Se puede indicar respecto a su fiabilidad que cumplen con las siguientes norma internacionales:

- ISO/IEC 15408 (Common Criteria) versión 3.1 logrando la evaluación EAL4+ (nivel 4+).
- CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1 para poder operar como Qualified Certificate Service Providers (CSPs).
- FIPS 201 con GSA EPL #1411.
- FIPS 140-2

6.3 Otros aspectos de Manejo de Claves

El cuidado de la clave privada debe ser una prioridad por parte del Suscriptor, por lo que debe prevenir tanto que la clave no sea vista al momento de ingresarla, ni copiarla del contenedor, ni adulterarla, para lo cual el Suscriptor debe tener a lo menos las siguientes precauciones:

- Mantener la clave privada protegida bajo *password* considerada segura, esto es de mínimo 8 caracteres que idealmente no sea pronunciable, que contenga letras, números y símbolos especiales, evitando usar un domicilio asociable al Suscriptor.
- Mantener solamente registrada en la memoria la *password* utilizada para proteger la clave privada
- No copiar la clave a papel u otro medio fácilmente legible
- Mantener un respaldo de la información de certificados en un lugar seguro, protegido también bajo clave (caja de fondos, u otro dispositivo de protección)

6.4 Controles de Seguridad Computacional

La seguridad en Certinet comprende soluciones tecnológicas de seguridad en las áreas de red, aplicaciones y sistemas. Dentro del área de aplicaciones, es esencial para la integridad de un Prestador de Servicios de Certificación, su Clave raíz (llave privada), la que se utiliza para firmar todos los certificados emitidos por dicho Prestador, por lo que corresponde a la raíz de confianza de la Autoridad Certificadora.

Tanto la llave raíz como los repositorios críticos en términos de seguridad se encuentran en las instalaciones seguras de VeriSign o de Certinet, ambas empresas líderes en prestación de servicios de certificación a nivel mundial o de acuerdo a los más altos estándares aceptados por la industria internacional.

Los servicios de administración de Certinet y de validación para la emisión de certificados se encuentran en las instalaciones de Certinet

Los aspectos relevantes para considerar respecto de la seguridad en este caso están cubiertos en una parte de los Servicios por VeriSign y en otra por Certinet, estos aspectos se representan en el siguiente esquema:

6.4.1 Seguridad de Redes

La implantación de la Certificadora tanto de VeriSign como de Certinet incluye un perímetro de seguridad que permitan disponer de diferentes niveles de defensa frente a la comunidad, incluidos los *hackers*. El perímetro comienza por la conexión a un ISP confiable (aquellos que desarrollan adecuadamente el tema de seguridad), luego establece *firewalls* en diferentes zonas hasta llegar al núcleo de seguridad del Prestador de Servicios de Certificación.

Tanto en VeriSign como en Certinet, el segmento de LAN donde se instala las aplicaciones de la Certificadora y los repositorios, están ubicados en un segmento de red protegido por *firewall* dedicado, incluyendo el registro de todos los eventos de seguridad, adicionalmente en caso de requerirse se tendrá software para la detección de intrusos en ejecución permanente y software equivalente para servidores donde corresponda. Además ambas empresas cuentan con niveles adecuados de monitoreo de redes.

6.4.2 Seguridad Tecnológica

La seguridad tecnológica de la autoridad certificadora es la base que sustenta el modelo de seguridad y está compuesta por:

- **Seguridad Física**: La Certificadora y Repositorio (Directorio de Certificados y CRL) están en un ambiente físicamente seguro, en una habitación con acceso controlado, alarma y accesible sólo por personal del Centro de Procesamiento. En cuanto a la Autoridad de Registro, estas residirán en un ambiente de seguridad estándar Bancario.

- **Seguridad Computacional**: La Certificadora y Repositorio opera en equipos robustos en cuanto a la seguridad, en el cual todos los servicios no necesarios están deshabilitados y todas las actualizaciones de seguridad son aplicadas. Se verifica en forma periódica con herramientas de seguridad que el sistema es seguro frente a intrusiones de externos. Además se dispone de políticas adecuadas para el manejo y cambio de claves. Certinet puede verificar en cualquier momento que estos aspectos sean cumplidos por los diferentes prestadores de servicios involucrados.
- **Seguridad del HSM y el Mecanismo de activación de la Firma:** Estos elementos tanto a nivel seguridad física y computacional, se encuentran en el servicio de seguridad de Azure, incluyendo las mejores técnicas de protección del HSM y las maquinas. Adicionalmente el sistema que administra el servicio fue acreditado para operar usando el Modelo eIDas, cumpliendo los estándares:
    - ISO/IEC 15408 (Common Criteria) versión 3.1 logrando la evaluación EAL4+.
    - CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
    - FIPS 201 con GSA EPL #1411.
    - FIPS 140-2

- **Disponibilidad**: Se dispone de una configuración de alta disponibilidad para los servicios críticos, que permite operar los servicios de certificados en forma permanente, producto que en general son servicios que operan sin restricciones de horario.
- **Seguridad Operacional**: El personal con acceso de administrador al software de la Certificadora y Repositorio tienen un alto nivel de acreditación de seguridad de la organización de tecnología. El acceso a funciones administrativas se efectúa sólo desde consolas conectadas en forma segura.
- **Seguridad de Respaldos**: Copias de los dispositivos de autenticación, respaldos y cualquier otro ítem relacionado, se guardan con un sistema de seguridad que no permite el acceso a personas no autorizadas.

Respecto de los procedimientos de administración de las llaves estos están documentados. En la documentación se incluyen los procedimientos propiamente tal y objetivos de control para asegurar la integridad de las llaves privadas. Entre otros, se debe incluir:

- Material
- Almacenamiento
- Robustecimiento de la Certificadora
- Requerimientos anuales de auditoria
- Auditoria de la generación de la Clave raíz
- Seguridad física
- Seguridad de la red
- Controles lógicos
- Procedimientos de operación

Respecto de la Autoridad de Registro, ellas tienen un esquema de seguridad requerido para las operaciones Bancarias que es compatible con el tipo de operación de un Prestador de Servicios de Certificación.

6.4.3 Protección de la Clave Raíz

El compromiso de la clave raíz es una de las brechas de seguridad más serias que puede sufrir un PCS. Por lo anterior, se han tomado todas las medidas posibles para protegerla junto con el ambiente donde reside.

En el caso de los Certificados provistos por VeriSign (actualmente Digicert), la Clave es protegida por VeriSign en sus instalaciones contra destrucción, modificación o copia por: Fallas del sistema como caídas y virus, Hackers y otros intrusos externos, errores inadvertidos y empleados maliciosos de la organización, entre otras amenazas.

La Clave Raíz es protegida por VeriSign con las mejores tecnologías y prácticas. La utilización de software o una combinación de software y barreras físicas es considerada insuficiente para protegerla. La única manera considerada adecuada para proveer protección a la Clave raíz es guardándola en un dispositivo de hardware donde se puede controlar su vulnerabilidad frente a intrusos, virus, eliminación inadvertida y complicaciones por falla del sistema.

Si bien la Clave privada de la Certificadora (clave raíz) es lo más importante, este tipo de consideraciones se toman con una debida gradualidad para la administración de todas las Claves privadas.

Desde el punto de vista de los procedimientos, se utilizó una ceremonia formal grabada para la generación de la Clave raíz por parte de VeriSign, de manera de asegurar que la integridad no sea refutable, tanto de los pares de claves como las claves privadas de la Certificadora. Testigos del proceso y la grabación proveen la base para la confianza en la integridad, confidencialidad y disponibilidad de todas las claves privadas, de datos, *token, HSM* y *password* utilizadas en el establecimiento de los servicios de una Certificadora.

En el caso de la nueva CA Raíz y TSA de Certinet, se realizó una ceremonia de llaves formal con la presencia en calidad de testigo de dicha ceremonia y la consiguiente aprobación de la Entidad Acreditadora dependiente del Ministerio de Economía, que es el órgano regulador en Chile. La aprobación de la ceremonia consta en el documento Acta de Ceremonia de llaves, el que está debidamente firmado por las partes.

La Clave Raíz tanto de la CA Raíz como de la TSA, son protegidas por Certinet con tecnologías y prácticas reconocidas a nivel internacional. Debido a que la sola utilización de software o una combinación de software y barreras físicas es considerada insuficiente para protegerla. Certinet, adicionalmente con el fin de proveer una adecuada protección de estas, las ha almacenado en un dispositivo de hardware seguro, donde se puede controlar su vulnerabilidad frente a intrusos, virus, eliminación inadvertida y complicaciones por falla del sistema. Este dispositivo está debidamente custodiado y salvaguardado por el PSC.

7. Perfiles de Certificados y CRL

7.1 Perfil del Certificado

7.1.1 Clases de Certificados

Certinet bajo el Modelo de Certificación Bancario para Firma Electrónica Avanzada sólo emite los Certificados estableciendo los parámetros de usos y aplicabilidad de acuerdo a sus políticas, normas y procedimientos definidos para el modelo. En consecuencia, no representan imposición ni recomendación alguna a los Solicitantes, Suscriptores o Usuarios, quienes deberán en forma individual establecer el uso que le darán.

En el futuro se podrán implementar otras clases de Certificados, que se incorporarán a las presentes prácticas o establecer otros modelos que tendrán sus prácticas específicas.

7.1.2 Contenido de los Certificados

Sin perjuicio de lo dispuesto en las Prácticas de Certificación específicas, un Certificado emitido por Certinet contendrá al menos lo siguiente:

a) Identificación del Prestador de Servicios de Certificación y su clave pública.
b) Código de Identificación del Certificado.
c) Identificación del Suscriptor del Certificado.
d) Clave pública del Suscriptor o bien un elemento de verificación de firma que corresponda a un elemento de creación de firma.
e) Algoritmo de firma del Suscriptor y del Prestador de Servicios de Certificación.
f) Período de Validez del Certificado.
g) Referencia a la “CPS Certinet”

Los certificados de firma electrónica avanzada a ser emitidos por Certinet tendrán las siguientes características:

- Formato X.509 v.3 (ITC Standard)
- Encriptación simétrica (256-bit) SHA2, encriptación asimétrica con largo de llaves de 2048 bits.

- Certificados para uso en Firma y Encriptación para las personas
- Tipo de Certificados: Firma Electrónica Avanzada (Identifica Individuos) Recomendaciones de interoperabilidad tecnológica:

Característica	Recomendación
Formato del Certificado	• X.509 V3 • RFC 2459
Petición de Firma de Certificado a Certificadora Raíz	• PKCS# 10 V.1.5 • RFC 2314
Respuesta de Firma de Certificado desde Raíz	• PKCS# 7 V.1.5 • RFC 2315
Algoritmo de Firma	RSA con SHA2
Largo de Llaves: Raíz otras Certificadoras	• 2.048 bit RSA
Verificación de Certificados	OCSP
Almacenamiento de Certificados	Firma Electrónica Avanzada a libre elección del suscriptor: Token Servicio de Custodia Central Segura Certinet
Hardware de Seguridad	Firma Electrónica Avanzada ▪ Generación de llaves RSA de 1024 y 2048 bits FIPS 140-2

7.1.3 Vigencia de los Certificados

Todos los Certificados emitidos por Certinet tendrán una vigencia de un año, contados desde la fecha de su emisión.

7.1.4 Caducidad

Los certificados caducarán por el transcurso de su período operacional o vigencia.

La caducidad de un Certificado produce también el término de la relación contractual entre el Suscriptor y Certinet.

7.2 Perfil de CRL

Certinet se obliga a mantener un Registro Público de Certificados, donde publicará el estado de los Certificados que se encuentren Vigentes, Suspendidos y/o Revocados.

A este Registro Público de Certificados se podrá acceder inmediata y electrónicamente mediante la visita a la página web correspondiente.

El certificado una vez aceptado será publicado en el repositorio de datos en el cual se almacenan los certificados, el que estará accesible en forma permanente para los diversos tipos de aplicaciones.

La tecnología a utilizar en Certinet para los directorios es la que considera el protocolo LDAP (Lightweight Directory Access Protocol) que corresponde a una versión simplificada de acceso a los directorios basados en el estándar X.500. Este protocolo define un esquema estándar de acceso a los certificados y es fundamental al momento de querer operar en ambientes abiertos o de interrelación con otras Certificadoras.

8. Administración de la CPS

8.1 Procedimientos de Modificación de la CPS

Como resultado del proceso tecnológico al cual acceden, la *"*CPS Certinet" *es* esencialmente dinámica, por lo que están expuestas a variación en el tiempo.

Las presentes *"CPS Certinet"* podrán ser modificadas por Certinet y publicadas con una fecha de entrada en vigencia no inferior a los 30 días de la fecha que queda disponible en el sitio Web de Certinet.

8.2 Políticas de Publicación y Notificación

Dicha modificación será notificada al Suscriptor y/o Solicitante mediante correo electrónico, a la casilla electrónica indicada por el Suscriptor o Solicitante con una anticipación de 30 días a la fecha de aplicación de los cambios efectuados.

El Suscriptor tendrá el plazo indicado para objetar la modificación, en cuyo caso los contratos firmados se entenderán resueltos.

Transcurrido dicho plazo sin que medie comunicación se entenderá que el Suscriptor y/o Solicitante acepta los cambios propuestos.

8.3 Procedimientos de Aprobación de las CPS

Una nueva versión de una CPS Certinet estará sujeta a un procedimiento de aprobación que considera:

- Desarrollo y aprobación interna de la nueva práctica
- Presentación de las prácticas a los organismos competentes para su aprobación
- Presentación de las Prácticas al Directorio de Certinet

Una vez pasada las aprobaciones anteriores, se publicarán las nuevas prácticas indicando el período de entrada en vigencia de ellas.

9. Control Documental

Cabe destacar, que dado el dinamismo que tienen los procedimientos asociados a la certificación bancaria, el presente documento será actualizado periódicamente a fin de adecuarlo a las características de uso del momento.