Declaración de Prácticas de Certificación

CPS-FEA CertiNet

CertiNet

Versión 2.2

Audiencia

Titulares/Usuarios, Profesionales de áreas de operaciones y tecnologías de Empresas que estén involucrados con la puesta en marcha u operación de la Aplicaciones que reciben objetos electrónicos firmados electrónicamente y público general participante del comercio electrónico, interesados en obtener confianza en la seguridad e interoperabilidad de estos Certificados.

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	
May/2004	V1.4	Adecuación al modelo Bancario definido por el grupo de Bancos	R. Riveros R. Gutiérrez	
Ago/2006	V 1.5	Incorporación de conceptos de Firma Electrónica Avanzada	R. Gutiérrez R. Riveros	
Nov/2010	V1.6	Eliminación de referencias a firma electrónica no avanzada y cambio domicilio de Certinet.	R. Riveros	
Ene/2016	V1.7	Actualiza Algoritmo de Firma de los certificados Sha1 a Sha2	A. Carreño R. Riveros	
Abr/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	

Ago/2021	V1.9	Actualización de contenidos	A. Carreño M. Robles	
Nov/2021	V1.9-1	Introduce Nota aclaratoria al Dto. 24 de 2019, en Capítulos: 3 (Identificación) y 4 (Ciclo de vida de los certificados: Emisión / Revocación / Suspensión / Expiración / Renovación)	A Carreño	
Dic/2021	V1.9-2	Actualiza contenidos, flujo FAR según nuevo modelo de custodia central segura de Certificados FEA, de acuerdo con el Decreto Supremo N°24 de 2019 del MINECON	A. Carreño R. Riveros	
Jul/2022	V2.0	Incorpora elementos de estandarización de ETSI 102.042 y actualizaciones de contenido solicitadas por la Entidad acreditadora. Revisión General por parte del nuevo Oficial de Seguridad	I. Infante M. Robles	
Oct/2022	V2.1	Se agrega Atención de Reclamos por Ley de consumidor y aclaraciones de las suspensión	R. Riveros	
Mayo/2023	V2.2	Se Incorpora descripción Enrolamiento a domicilio y ajustes de redacción	R. Riveros	

1. Introducción

El presente documento de carácter público, contiene las estipulaciones que constituyen las Prácticas de Certificación de Firma Electrónica Avanzada en adelante "CPS-FEA CertiNet" y establece cómo se cumple con las directrices establecidas en su Política de Certificados de Firma Electrónica Avanzada en adelante CP-FEA CertiNet, las que puede encontrar en nuestra página web https://www.certinet.cl/acreditacion.

En términos generales describe los procesos, operaciones y prácticas que CertiNet utiliza para crear, mantener y administrar sus servicios como Prestador de Servicios de Certificación durante el ciclo de vida de dichos certificados, lo anterior dentro de los parámetros regulaciones y estándares, establecidos en la Ley 19.799 sobre firmas y documentos electrónicos, su reglamento y la guía de acreditación de la Subsecretaría de Economía y Empresas de Menor Tamaño, las que puede encontrar en: https://www.entidadacreditadora.gob.cl/ bajo el título "Leyes y Estándares".,

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 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. Y está acreditado como Prestador de Servicio de Certificación de Firma Electrónica Avanzada, en adelante "el o los Certificados", 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.

CertiNet ha establecido una Política de Seguridad y protección de datos acorde con el modelo de confianza requerido para la Certificación de la Firma Electrónica.

1.1 Generalidades

La "CPS-FEA CertiNet" establece en esta declaración, los procedimientos y normas que CertiNet adopta actuando como Autoridad Certificadora en la provisión de Servicios de Certificación y constituyen el contrato entre CertiNet y el Titular/usuario de un Certificado de Firma Electrónica Avanzada.

En esta CPS-FEA CertiNet, se describen también las reglas que deben observar y cumplir los Solicitantes, Titulares/usuarios y Terceras partes que confían en la cadena de confianza de CertiNet, durante el ciclo de vida de los certificados.

1.1.1 Sobre esta Declaración de Prácticas

Estas reglas y procedimientos, regulan la emisión y/o renovación, la suspensión y/o revocación, el uso, almacenamiento y resguardo de dichos certificados. Como también de las claves privadas, contraseñas y factores secundarios asociados a dichos certificados que se generan y permanecen bajo el exclusivo conocimiento y control del Titular/usuario.

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

- Obligaciones del Prestador de Servicios de Certificación Autoridad Certificadora CertiNet (CA), las Autoridades de Registro (RA), Solicitantes, Titulares/usuarios y Terceros que Confían, dentro del ámbito que regula la "CPS-FEA CertiNet".
- Aspectos considerados en el Contrato de Titular/usuario, para el ámbito de aplicación de la "CPS-FEA CertiNet",
- Revisiones de Auditoría, de Seguridad y de cumplimiento de estas Prácticas.
- Métodos usados para confirmar la identidad de los solicitantes y Titulares/usuarios 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 llaves.
- Contenidos de las listas de certificados emitidos, vigentes y revocados
- Administración de este documento, incluyendo métodos de su actualización.

1.1.2 Alcance

Las regulaciones establecidas en esta CPS-FEA CertiNet, deben ser aplicadas por la organización en todo el ciclo de vida de sus Certificados de Firma Electrónica Avanzada y se encuentra disponible para los Titulares/usuarios y terceras partes que decidan operar con dichos certificados.

1.2 Identificación

a) Esta "CPS-FEA CertiNet", se ha desarrollado en conformidad con el documento RFC 3647 "Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Framework*" y la ETSI TS 102 042 V1.1.1 (2002-04) 7.1 Certification practice statement, 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" y la Guía de Evaluación Procedimiento de Acreditación Prestador de Servicios de Certificación Firma Electrónica Avanzada versión 2.0. ubicada en: https://www.entidadacreditadora.gob.cl/guias/

b) El presente documento será individualizado como:

Nombre: CPS-FEA CertiNet.
OID.: 1.3.6.1.4.1.52428.100
Descripción: Declaración de Prácticas de Certificación de CertiNet S.A., para Firma Electrónica Avanzada.
Versión: 2.0
Fecha de emisión: 01 de agosto del 2022
Ubicación: https://www.certinet.cl/acreditacion

CP relacionada: Política de Certificados para Firma Electrónica Avanzada de CertiNet S.A. (CP-FEA CertiNet)
Ubicación: https://www.certinet.cl/acreditacion

c) **Detalle de Contacto:**

Razón Social: CertiNet S.A.
Rut: 99.532.830-5
Representante Legal: Roberto Riveros Durán
Dirección Social: Huérfanos #1052 Piso 12, Santiago.

Esta CPS-FEA CertiNet es administrada por el PSC CertiNet S.A., que puede ser contactada al e-mail: soporte@certinet.cl o bien www.certinet.cl. El servicio de atención a clientes, Titulares/usuarios y Terceros que Confían, atiende mediante el mail indicado, bajo un esquema de "Ticket Jerarquizado de Servicio", por lo que el flujo de atención depende del motivo y urgencia de la consulta.

1.3 Comunidad y Aplicabilidad

La "CPS-FEA CertiNet" regula los procedimientos y protocolos establecidos en su CP-FEA CertiNet, los que se deben observar y cumplir de acuerdo a la normativa vigente a lo largo de todo el ciclo de vida de los certificados desde su emisión hasta su revocación, y se aplica a todos los certificados de Firma Electrónica Avanzada emitidos por CertiNet.

Los Certificados de Firma Electrónica Avanzada emitidos de acuerdo a lo dispuesto en esta CPS-FEA CertiNet, están dirigidos a satisfacer las necesidades de identificación y autenticación establecidas en la Ley 19.799, sobre firmas y documentos electrónicos y los servicios de certificación de estos. Tanto para titulares/usuarios como para las terceras partes que decidan libremente confiar en su cadena de confianza y tecnologías.

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

1.4.2 Autoridad de Certificación (CA)

La Autoridad de Certificación es la entidad de confianza acreditada para prestar servicios de certificación electrónica avanzada responsable de emitir y revocar Certificados de Firma Electrónica Avanzada de acuerdo con los requisitos legales establecidos en la ley 19.799, su reglamento, guías, normas y estándares técnicos contenidos en ellos.

1.4.3 Autoridad de Registro (RA)

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, c) Verificar la identidad de un Titular/usuario a través del sistema de Clave Única con mecanismo complementario y segundo factor, en forma Presencial o Notarial y 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.

1.4.4 Solicitante

CertiNet, reconoce como Solicitante a toda “Persona”, natural o jurídica debidamente representada, que solicita para sí o para un tercero la emisión de un Certificado en conformidad a lo establecido en la CP-FEA CertiNet y los procedimientos que la empresa tiene definidos para el registro de estas solicitudes en esta CPS-FEA CertiNet.

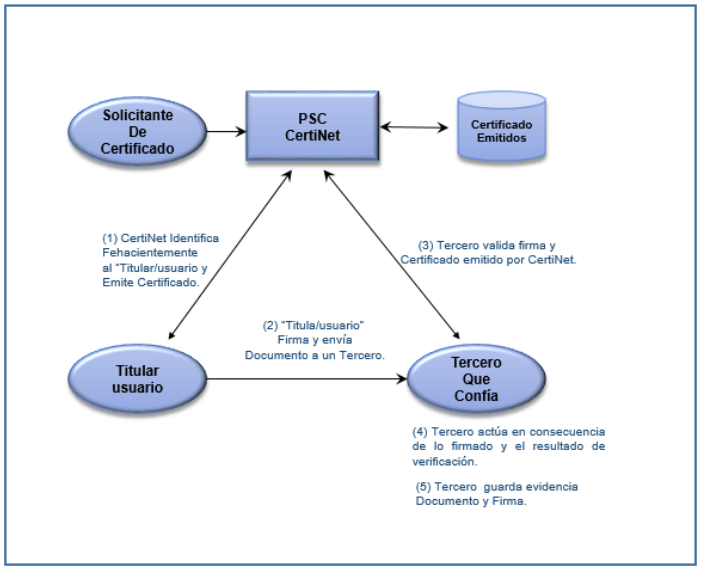
1.4.5 Titular/usuario

Aquel en cuyo favor se ha emitido un Certificado que es una persona natural o jurídica, con cédula de identidad o Rol Único Tributario, según sea el caso, chileno y vigente, que ha sido debidamente autenticada y que cumple con los requisitos legales para solicitar un certificado de firma electrónica avanzada que utiliza bajo su exclusivo control.

1.4.6 Tercero que confía

Toda persona natural o jurídica que voluntaria y libremente al recibir Información firmada a través de una firma electrónica avanzada asociada a un Certificado de Firma Electrónica Avanzada, válidamente emitido por CertiNet decide confiar en la integridad y autenticidad de la información contenida con certeza de la identidad del firmante. El "Tercero que Confía", es responsable de validar el contenido del documento, la firma y el certificado asociado a dicha firma previo a confiar en él.

Esquemáticamente la interacción entre las entidades es:



1.5 Tipos y Usos del Certificado de Firma Electrónica Avanzada:

Según lo definido en el artículo 2 de la Ley 19.799:

Letra b) "*Certificado de firma electrónica: certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica;"*

Y,

Letra g) *"Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría,"*

1.5.1. Tipos de Certificados

CertiNet emite Certificados de Firma Electrónica Avanzada a personas naturales solo después de haber verificado fehacientemente la identidad del solicitante conforme a exigido la Ley 19.799 y su reglamento, y con ello garantizar que el Titular/usuario de un Certificado de Firma Electrónica Avanzada no se pueda "repudiar", la firma de un documento cualquiera.

Estos cumplen con lo establecido en el artículo 15 de la Ley 19.799:

> *"Los certificados de firma electrónica, deberán contener, al menos, las siguientes menciones:*
> *a) Un código de identificación único del certificado;*
> *b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;*
> *c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y*
> *d) Su plazo de vigencia.*
>
> *Los certificados de firma electrónica avanzada podrán ser emitidos por entidades no establecidas en Chile y serán equivalentes a los otorgados por prestadores establecidos en el país, cuando fueren homologados por estos últimos, bajo su responsabilidad, y cumpliendo los requisitos fijados en esta ley y su reglamento, o en virtud de convenio internacional ratificado por Chile y que se encuentre vigente."*

Puede encontrar un mayor grado de detalle sobre este punto en el numeral **7.1 Perfil del Certificado**, de este documento.

CertiNet emite los certificados bajo la plataforma propia de CertiNet, no comercializa sus certificados vía otro nombre de fantasía o empresa.

1.5.2 Usos del Certificado

De acuerdo con lo declarado en el número 1.5, de la CP-FEA CertiNet, el uso de los certificados y su información asociada está restringido a las condiciones de uso específicas descritas en este instrumento y la ley 19.799, su reglamento y las normas y estándares vigentes.

Sin perjuicio de lo anterior, CertiNet reconoce por regla general como:

1.5.2.1: Usos permitidos de los Certificados de firma electrónica avanzada:

Por regla general, CertiNet podrá emitir o acordar emitir certificados de uso específico o con limitaciones de uso. No obstante, por regla general, permite el uso de sus certificados según lo establecido en la Ley 19.799, artículos 3, 4 y 5. Lo que se puede resumir en:

> "Se permite el uso de sus Certificados en actos y contratos otorgados o celebrados, que no sean contrarios a ley o atenten contra la moral u orden público o para realizar actos de naturaleza delictual o que se pueda considerar ilegal. Ya sea por personas naturales o jurídicas.
> Con exención de aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico y aquellos en que la Ley requiera la concurrencia personal, o lo relativos al derecho de familia.

1.5.2.2: Usos no Autorizados:

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 y en particular, no pueden ser usados para certificar a otros individuos u objetos, ni establecer cadenas de confianza a través de ellos para ningún efecto o propósito. En general, CertiNet no asume ninguna responsabilidad por usos de sus servicios para fines que excedan de los límites de uso racional de los mismos.

2. Requerimientos generales

En este capítulo se describen las obligaciones y responsabilidades de los diferentes participantes asociados al ciclo de vida de los certificados. Se establecen 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 derechos de datos personales.

2.1 Obligaciones

CertiNet, declara que en general toda entidad o personas que hagan uso directa o indirectamente de los servicios de nuestra empresa debe observar y cumplir con las obligaciones contenidas en la Ley 19.799, sobre firmas y documentos electrónicos, que se resumen, pero no se limitan a:

2.1.1 Autoridad Certificadora 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 las directrices y procedimientos establecidos en la “CPS-FEA CertiNet” y en la Política de Certificados CP-FEA CertiNet, que se otorguen para la emisión de Certificados.
c) Cumplir con todas las otras obligaciones que establezcan la Ley 19.799 Firmas Electrónicas, 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 la “CPS-FEA CertiNet”.
e) Emitir los certificados en conformidad al procedimiento establecido en las “CPS-FEA CertiNet”**.**
f) Proveer mecanismos de custodia de llaves del cliente como Token, 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 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 Titular/usuario 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 Titular/usuario de dichas acciones.
j) Realizar razonables esfuerzos para comunicar a los Titulares/usuarios 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 fehaciente a los solicitantes de un Certificado de Firma Electrónica Avanzada, de conformidad al procedimiento establecido en las "CPS-FEA CertiNet", y en la Política de Certificado (CP-FEA CertiNet), correspondiente a Certificados de firma electrónica avanzada.
b) Registrar y custodiar los antecedentes requeridos a los solicitantes que permitan una identificación fehaciente de los mismos, de conformidad con los requisitos establecidos en la Política de Certificados CP-FEA CertiNet, correspondiente a los Certificados de Firma Avanzada.
c) Aprobar o denegar las solicitudes de Emisión de Certificados.
d) Entregar al Titular/usuario 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 Titular/usuario.
i) Prestación de otros servicios que CertiNet le solicite.

2.1.3 Obligaciones del Solicitante

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".

2.1.4 Obligaciones del Titular/usuario

Antes de la emisión del certificado el Titular/usuario se obliga a:

a) Seleccionar, el mecanismo digital seguro 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, la contraseña utilizada en el proceso de firma por medios que estén bajo su exclusivo control. En el caso de elegir un dispositivo masivo, según lo establecido en el art. 5 inc. 2° del DS N°24 de 2019 del MINECON, deberá este encontrarse protegido mediante un segundo factor de seguridad, obligándose a mantener el exclusivo control de este segundo factor de seguridad, a fin de controlar el acceso y utilización del dispositivo.

b) 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 acceder su Certificado, teniendo por lo mismo un exclusivo control y acceso a este, según lo señalado previamente en la letra a).

c) Generar, custodiar y no revelar la contraseña de acceso al dispositivo o al servicio de custodia que contiene la llave privada asociada al certificado y/o no revelar el mecanismo de activación de la firma. Ni el segundo factor de seguridad establecido de conformidad con el decreto 24 de 2019.

d) 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.

e) En el caso de las personas naturales, deben ser mayores de edad.

Una vez emitido el certificado el Titular/usuario se obliga a:

f) Aceptar el certificado. Se entiende que un certificado ha sido aceptado por parte del Titular/usuario una vez que: a) 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, b) No se haya formulado un reclamo por error o inexactitud en la emisión, al momento de su recepción c) La instalación en el dispositivo de generación de firma o dejar en custodia para la posterior utilización, de cualquier modo, del Certificado, es considerada la aceptación del Certificado por parte del Titular/usuario.

g) 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.

h) Usar por medio de su contraseña secreta el Certificado para fines legales y autorizados, de conformidad con lo previsto en la Ley de Firma Electrónica, las “CPS CertiNet” y en las Políticas de Certificados “CP-FEA CertiNet”.

i) Utilizar correctamente el Certificado, el que se entrega en depósito por CertiNet o, se mantiene bajo la custodia central de esta.

j) Utilizar el certificado para los fines comerciales que el Titular/usuario libremente aceptó, ya sea para uso “Custodia para uso específico” o con “vigencia limitada” de acuerdo a la CPS CertiNet.

k) Ser un usuario final, y no usar el Certificado para actuar como Prestador de Servicios de Certificación, a su vez.
l) Comunicar inmediatamente a la Autoridad de Registro y/o a CertiNet el compromiso, pérdida, hurto, robo, acceso no autorizado o extravío, falsificación de su contraseña de acceso al certificado o cualquier circunstancia que pudiera ser causal de suspensión o revocación de un Certificado.
m) Comunicar la pérdida o destrucción del dispositivo enrolado para utilización de los certificados, ya sea en dispositivo físico o en custodia.
n) Custodiar la contraseña, tomando precauciones razonables para evitar su pérdida, modificación y uso no autorizado.
o) Solicitar la revocación del Certificado cuando se presente alguna de las causales indicadas para este efecto
p) Abstenerse de usar la llave privada una vez que el Certificado haya expirado o haya sido solicitada la revocación.
q) Destruir la llave privada en caso de que CertiNet así lo exija y haya sido revocado previamente el certificado.

2.1.5 Obligaciones de Terceros que Confían

Los Terceros que decidan en forma libre y espontánea confiar en la cadena confianza de 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 Titular/usuario,
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.

2.1.6 Obligación General

Los Titulares/usuarios del servicio de certificación de CertiNet, se obligan a conocer y aceptar los términos, condiciones y límites contenidos en esta “CPS-FEA CertiNet”, y en la Política de Certificación (CP-FEA CertiNet) que suscriban, los que en conjunto regulan la prestación de Servicios de Certificación.

El Prestador de Servicios de Certificación, en cumplimiento con las obligaciones impuestas por el legislador en la ley 21.398 (antigua ley 19.496), dispondrá de un servicio de atención al cliente, por medio del cual se podrán dirigir, por medios remotos (correo soporte@certinet.cl) y/o físicos, cualquier reclamo de los consumidores finales de los servicios prestados en virtud del presente contrato.

2.2 Responsabilidades

En este punto se incluye en forma unificada las responsabilidades establecidas en la ley 19.799 SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA.

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 Titular/usuario.
b) Que el Certificado no contenga errores de transcripción de los datos recogidos del Titular/usuario, y se haya 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 contraseñas, 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 Titular/usuario 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

Por aplicación del estatuto de responsabilidad contractual (incluyendo incumplimientos de las garantías acordadas), extracontractual (incluyendo negligencia y/o daños y perjuicios, directos o indirectos, previstos e imprevistos) y de cualquier tipo normativa que funde un reclamo efectuado mediante procedimiento legal comparable, si el Titular/usuario 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 Titular/usuario, la responsabilidad total de CertiNet por los daños y perjuicios invocados por el Titular/usuario y/o cualquier tercero, por cualquier uso o confianza asignados a un certificado específico están limitados, en su totalidad, al monto establecido a continuación:

"Certinet S.A." como Prestador de Servicios de Certificación acreditado, en su conjunto, no podrá ser obligado a indemnizar una suma mayor a la establecida en la cobertura que provee el seguro de responsabilidad civil obligatorio, según lo dispuesto en el artículo 12 del dto. 181, reglamento de la Ley 19.799".

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.

2.2.3 Responsabilidad de la RA y la CA

Está declaración de prácticas provee las regulaciones que limitan, restringen y condicionan las responsabilidades en el actuar tanto de la Autoridad de Registro delegada (RA) y de la Autoridad Certificadora (CA), las que se subordinan a lo establecido en la Ley 19.799 y su reglamento, las que incluyen:

a) La RA, deberá realizar la correcta identificación y registro del Titular/usuario de un Certificado, ya sea mediante comparecencia personal o a través del sistema Clave Única del Registro Civil de Chile.
b) Realizar con la debida diligencia y cuidado, las funciones que conforme a las "CPS CertiNet" le correspondan como Autoridad de Registro o que CertiNet le solicite.
c) La CA deberá emitir el Certificado de Firma Electrónica Avanzada cumpliendo todas las exigencias técnicas y legales, requeridas en la "CP-FEA Certinet" y la "CPS-FEA CertiNet" de conformidad con los datos entregados por el Titular/usuario y publicar el Certificado de Firma Electrónica Avanzada en el directorio correspondiente.

2.2.4 Titular/usuario

El Titular/usuario 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 su contraseña que da acceso a la llave 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 contraseña antes de la aceptación del certificado. El Titular/usuario es el único responsable de los daños y perjuicios que con su actuación se causen en el evento que use su llave 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 Titular/usuario es responsable y así lo acepta y declara, que cada Firma Electrónica Avanzada creada utilizando su llave privada asociada a la llave pública contenida en el certificado, corresponde a la Firma Electrónica Avanzada del Titular/usuario 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, el Titular/usuario 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 Tercero que Confía

Todo receptor de un documento firmado con un certificado válidamente emitido por CertiNet, que decide confiar en su validez e integridad 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 la Política de Certificados “CP-FEA CertiNet”, 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) Ley de aplicación general (Código de Comercio / Código Civil)
d) Contrato de Titular/usuario
e) CPS-FEA CertiNet vigente
f) CP-FEA CertiNet vigente
g) Otros documentos, relacionados con la prestación de servicios de certificación.

2.4 Tarifas

El Titular/usuario 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 Titular/usuario 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 Titulares/Usuarios 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 de conformidad con la Ley, debe estar disponible para los interesados sin costo alguno.

c) Custodia para uso específico

El Titular/usuario podrá optar libremente por un modelo comercial para usos específicos de su Certificado y llaves en Custodia, según las condiciones contractuales; Por ejemplo para “Empresa en un Día”, “Proveedores Afiliados” y otros que se determinen según el modelo comercial acordado los que estarán sujetos precios diferentes.

En el caso que el Titular/usuario quiera usar un certificado de uso específico fuera del dominio adquirido debe completar el pago de un Certificado de modo que pueda ser considerado para uso universal. En el caso que el Titular/usuario utilice un certificado para uso específico en modalidad universal, será advertido

que debe completar el pago, en el caso que no lo haga según los términos y condiciones de esta modalidad, autoriza expresamente a que CertiNet revoque su certificado por mal uso.

d) Certificados con vigencia limitada

El Titular/usuario podrá optar libremente por un modelo comercial para Certificados y llaves en Custodia, con una vigencia limitada según las condiciones contractuales.

Otros Servicios

Otros servicios tales como suspensión, revocación, 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 https://www.certinet.cl

2.4.2. Política de Devoluciones

En el evento que un Titular/usuario determine devolver un certificado ya sea aceptado o no, este será revocado y la tarifa pagada no será devuelta, salvo el caso de Empresa en un Día que:

- La devolución de montos transferidos desde el botón de pago del sitio web por conceptos de suscripción y/o validación a la Firma Electrónica de CertiNet para empresa en un día se analizará si el cliente no pudo acceder al proceso de enrolamiento y si pudo o no firmar en Empresa en un Día, con estos antecedentes resolverá en un plazo no mayor a 15 días a partir de que se ingresó por los canales correspondientes la solicitud de devolución.
- Si el cliente ya firmó en Empresa en un Día no corresponde la devolución
- Para la solicitud de devolución: Enviar correo electrónico a soporte@certinet.cl su solicitud de devolución indicando su RUT, Fecha de Pago y teléfono de Contacto.
- Las resoluciones de devolución se informarán vía correo electrónico.

2.5 Publicaciones y Repositorio

La CPS CertiNet estará disponible para los Titulares/usuarios, Terceros que Confían 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 https://www.certinet.cl/acreditacion.

Se contempla una publicación material del original, cuya exactitud y veracidad deberá ser refrendada mediante la protocolización correspondiente, y su 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 Titulares/usuarios o terceras partes que confían 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 el sitio web de la PSC https://www.certinet.cl/acreditacion y en los detalles básicos de cada certificado entregado:

Objeto	Ubicación:
Prácticas de Certificación Vigentes	URL CPS en Apartado "*Directivas del Certificado".*
Directorio de Certificados Emitidos	URL OCSP en Apartado "*Acceso a información de autoridad".*
Directorio de Certificados Firma Electrónica Avanzada Revocados y Suspendidos	URL CRL en Apartado *"Puntos de Distribución 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 auditoría al iniciar la operación como Autoridad de Registro. La Auditoría 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 Titulares/usuarios 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 Titulares/usuarios 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, de forma presencial en las oficinas ubicadas 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 Titular/usuario es 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.

2.7.1 Tipos de Información a Proteger

CertiNet está sujeto a la obligación de reserva, de conformidad con la Ley N° 19.628 sobre Protección de la Vida Privada, considerando los principios internacionales de protección de datos, los relativos a Secreto Bancario y los emanados de contratos suscritos para la prestación de servicios con condiciones particulares.

2.7.2 Tipos de Información considerada no confidencial o pública:

- ✓ La contenida en la CP-FEA Certinet y CPS-FEA CertiNet, la contenida en los Certificados emitidos por CertiNet y la del Registro Público de Certificados. La solicitada para fines judiciales, en especial si es destinada a auditorías que tengan por fin garantizar el No Repudio de una firma generada al tenor de las prácticas contenidas en el presente documento.
- ✓ La Información del Certificado: La estructura del Certificado para Firma Electrónica Avanzada cumple con las disposiciones legales, normativas y técnicas vigentes, con el fin de garantizar interoperabilidad del sistema. Y la que sea significativa en función de la finalidad y limitaciones del certificado tales como periodo de validez del certificado, así como la fecha de emisión y caducidad del certificado, número de serie y los diferentes estados (vigente o revocado) del mismo.
- ✓ Las listas de revocación (CRLs)
- ✓ Toda aquella impuesta normativamente.

2.7.3 Entrega de Información en virtud de un Procedimiento Judicial

CertiNet en cumplimiento de la ley vigente, entregará toda la información requerida por vías formales judiciales, en los tiempos y formas que estipula la ley.

2.7.4 Entrega de Información a Petición del Titular

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 por vía electrónica, a la dirección de correo electrónico: soporte@certinet.cl

2.8 Derechos de Propiedad Intelectual

CertiNet es titular de los derechos de Propiedad Intelectual de todas las "CP y CPS CertiNet" que se emitan bajo su modelo de confianza, y de todos los derechos que la Ley N° 17.336 sobre Propiedad Intelectual contempla respecto de los mismos, lo mismo respecto de los derechos contemplados en virtud de la Ley N° 19.039 de Propiedad Industrial.

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 contraseñas, llaves criptográficas 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 Políticas de Certificados (CP).

Lo que a lo menos considera:

- ✓ "En el otorgamiento de Certificados de Firma Electrónica Avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;"; Artículo 12 letra e) Ley 19.799
- ✓ Lo dispuesto en el Decreto N° 24 de 2019 del Ministerio de Economía Fomento y Turismo, que Aprueba Norma Técnica para la Prestación del Servicio de Certificación de Firma Electrónica Avanzada, en especial pero no limitado a lo referido a enrolamiento con Clave Única junto con

mecanismos complementarios y segundo factor, para firma con autorización remota FAR y los que sean requeridos para prestar el servicio de custodia central segura de CertiNet, o Token.

- ✓ Asignación de nombre: Todos los certificados tienen un nombre distintivo (DN o distinguished name) conforme al estándar X.501.
- ✓ Unicidad de nombres: Todos los nombres y datos individuales asignados, relativos a la individualización de los certificados emitidos serán únicos para cada Titular/usuario conforme a la ley vigente.
- ✓ Toda contraseña que proporcione acceso al certificado y las llaves pública y privada del certificado, son generadas en instancia directa por el Titular/usuario y debe permanecer en todo momento bajo su exclusivo control y secreto.
- ✓ La solicitud de Revocación o Renovación de Certificado por parte del Titular/usuario es personal es intransferible y se efectúa según los procedimientos autorizados por CertiNet.

3.1 Registro Inicial

Sin perjuicio de los requisitos particulares que las Prácticas de Certificación (CPS) exijan, previo a la emisión inicial de un "Certificado de Firma Electrónica Avanzada", el solicitante deberá comparecer en forma personal y directa o agendar la visita a la dirección comercial si se trata de una persona natural o, bien por medio de identificación notarial, o debe identificarse mediante el uso de su propia Clave Única, otorgada por el Servicio de Registro Civil e Identificación, junto con los mecanismos complementarios autorizados como es la Transferencia de Fondos de su propio RUT todo esto ante CertiNet o ante la Autoridad de Registro que actuando por cuenta, riesgo y en representación del primero, éste hubiere autorizado.

Todas las Autoridades de Registro Autorizadas por CertiNet para operar como tales, realizarán el mismo procedimiento para identificar y registrar a un Titular/usuario de certificados, de modo tal de ofrecer un grado de confianza equivalente a todos nuestros clientes.

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 antecedentes necesarios para que su identidad sea verificada fehacientemente. Los factores de identificación a utilizar son:

Modalidad 1: Por comparecencia personal ante CertiNet o Notario Público.

Tipo de Certificado	Antecedentes Requeridos: Comparecencia ante CertiNet o Notario Público
Firma Electrónica Avanzada	• Comparecer de forma presencial ante CertiNet o Notario Público. • Cédula o Carnet de Identidad vigente • Correo electrónico • Teléfono de contacto • Fotografía el caso de comparecencia personal ante un oficial de registro autorizado por CertiNet • Disponibilidad para Configurar Computador y Dispositivo Token con asistencia de ejecutivos CertiNet.

En caso que se haga la validación de acto presencial ante notario como parte del proceso de solicitud de Certificado de Firma Electrónica Avanzada de la PSC CertiNet S.A., acogido a lo estipulado en el Artículo 12 letra (e) de la ley 19.799, CertiNet entrega formulario que debe ser completado y firmado ante el notario, una vez recepcionado dicho formulario, CertiNet lo valida, envía el token previo a transferencia del cliente y coordina la atención para otra validación de identidad al momento del enrolamiento final con los datos provistos en la notaría.

Modalidad 2: Por comparecencia personal en el domicilio comercial

Tipo de Certificado	Antecedentes Requeridos: Domicilio Comercial
Firma Electrónica Avanzada	• Enviar previamente copia de Cédula o Carnet de Identidad vigente • Indicar el Correo electrónico que se usará para el Certificado • Teléfono de contacto • Pagar la tarifa de Certificado, enrolamiento y token. • Agendar con CertiNet la visita del Oficial de Enrolamiento de CertiNet al domicilio comercial. • Recibir y Comparecer de forma presencial ante el oficial de CertiNet • Fotografía de la comparecencia personal ante un oficial de registro autorizado por CertiNet • Disponibilidad para Configurar Computador y Dispositivo Token con asistencia de ejecutivos CertiNet.

La autorización de la emisión se hace por medio de control dual, de modo que el acto presencial es la corroboración de la identidad como indica la ley, el control dual se hace por medio de Oficial de Enrolamiento en el Domicilio junto con el Supervisor de Enrolamiento quien dispone de los elementos previos que al revisar las piezas de identificación del solicitante enviadas en el proceso, autoriza la generación del certificado.

Modalidad 3 - Enrolamiento FAR CertiNet: Firma Electrónica Avanzada con Autorización Remota FAR es un servicio de custodia centralizada segura en CertiNet basado en un HSM "Hardware Security Module", en la nube.

Tipo de Certificado	Antecedentes Requeridos
Firma Electrónica Avanzada	• Capacidad de acceso a sitio WEB vía internet. • Identificarse a través del sistema "Clave Única", proporcionada por el Registro Civil de Chile. • Identificarse con un mecanismo complementario como es pago del servicio con transferencia electrónica o con pago en línea desde una cuenta asociada al RUT del solicitante, transferencia • Correo electrónico, para activación segundo factor de seguridad. • Teléfono Móvil para activación de segundo factor de seguridad.

3.1.2. Existencia de antecedentes previos

No serán requeridos aquellos antecedentes necesarios para la emisión de certificados, cuando estos ya constan fehacientemente en poder de CertiNet, de una Autoridad de Registro Autorizada.

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 o pasaporte, con uno, dos, tres nombres y dos apellidos o los nombres que consten en el Sistema Clave Única.

3.1.4. Generación de llaves

El Titular/usuario de Certificado de Firma Electrónica Avanzada, debe ser capaz de generar sus datos de creación de firma o llave privada y su correspondiente llave pública, tanto para su certificado como para el dispositivo móvil para autorizar la firma cuando se usa el modelo de custodia central segura, la generación de llaves debe hacerse 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. Todo dispositivo usado para firmar debe disponer de una clave personal del Titular/usuario. Este es un requisito esencial para obtener un certificado de este tipo.

3.1.5 Protección de llaves

El Titular/usuario es el único responsable de la protección de sus datos de creación de firma o llave 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, por medio de usar su clave personal.

CertiNet y/o las Autoridades de Registro, no generan, ni mantienen ni protegen datos de creación de firmas o llaves privadas para los Titulares/usuarios de Certificados de Firma Electrónica Avanzada, salvo para los clientes que opten libremente por usar el servicio de custodia central seguro de CertiNet, en cuyo caso se declara explícitamente que CertiNet no tiene ni mantiene métodos para acceder directa o indirectamente a estos datos, ni mantiene acceso a la contraseña que es de exclusivo control del cliente.

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, en el caso que se emitan certificados utilizando el medio de comprobación digital se informa claramente que existe 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 certificación del producto clase mundial Ascertia para que sus sistemas puedan operar con Firma con Autorización Remota.
- La norma ISO/IEC 15408 versión 3.1 permite que logre el control exclusivo del cliente, equivalente al Token.
- La Aprobación por parte de la Entidad Acreditadora de *"flujo entregado para el proceso de emisión de Firmas Electrónicas Avanzadas llamado -Flujo Certinet FAR EEUD-, podemos señalar que este cumple con lo requerido en el Decreto N°24 de la Ley 19.799 y está apto para que pueda ser implementado y de esta forma los ciudadanos puedan adquirir certificados mediante esta metodología a partir del lunes 6 de Diciembre de 2021"*
- La Aprobación por parte de la Entidad Acreditadora de *"flujo entregado para el proceso de emisión de Firmas Electrónicas Avanzadas llamado -Flujo Certinet MDS- está en proceso de Aprobación respecto del cumplir con lo requerido en el Decreto N°24 de MINECON de 2019. "*

En lo específico el servicio en cuestión 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 llaves

En el evento que el Titular/usuario autorice el uso de sus datos de creación de firma o contraseña Personal por parte de terceros, los actos celebrados con ellos serán de su exclusiva responsabilidad, puesto que el titular tiene el exclusivo control de estos y por tanto sigue siendo el único 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

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 Titular/usuario; 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 Titular/usuario, en la página de CertiNet para completar esta Solicitud.
- Notificación enviada por el Titular/usuario a la Autoridad de Registro o a CertiNet utilizando Firma Electrónica Avanzada, según corresponda.
- Por comparecencia presencial ante la Autoridad de Registro o ante CertiNet.
- Por comprobación mediante el sistema denominado Clave Única, 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 Titular/usuario, 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 Titular/usuario; esto se hace a través de:

- Notificación enviada por el Titular/usuario a la Autoridad de Registro o a CertiNet utilizando Firma Electrónica Avanzada vigente.
- Por comparecencia presencial ante la Autoridad de Registro o ante CertiNet.

- Identificación mediante el sistema denominado Clave Única, según lo establecido en el Decreto N° 24 de MINECON de 2019.

3.2.3 Solicitud de Renovación

Frente a una solicitud de renovación, el Titular/usuario dispone debe disponer de Firma Electrónica Avanzada vigente de CertiNet, para eso debe 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 Titular/usuario.

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. Identificándose mediante el sistema Clave Única del Servicios de Registro Civil de Chile, conforme a lo dispuesto en el Decreto N° 24 de MINECON de 2019 y siguiendo el procedimiento indicado para este caso por CertiNet.

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 Titular/usuario 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 identidad mediante los métodos indicados en 3.1.1 o que los antecedentes que presenta no sean concordantes a lo solicitado, se les rechazará la solicitud dado que no cumplen lo solicitado.

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

4.2 Emisión de Certificado: Esquema general de enrolamiento

Una vez que CertiNet y/o la Autoridad de Registro aprueba la solicitud, esta debe ser enviada a CertiNet en un formulario el cual contiene solamente los antecedentes requeridos para la emisión del certificado. La Autoridad de Registro delegada, el formulario deberá ser firmado electrónicamente.

Los certificados que se enrolen por medio del sistema Clave Única, CertiNet aprobará la solicitud en la medida que de cumplimiento con Decreto N° 24 de MINECON de 2019 autorizada por la Entidad Acreditadora

CertiNet solo emitirá certificados previo consentimiento del Titular/usuario: A mayor claridad, 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 del Titular y se emitirá con carácter personal e intransferible a nombre del Titular/usuario.

A continuación se presenta un esquema general para los enrolamientos de acuerdo al sistema de almacenamiento seguro que el Titular/usuario haya solicitado libremente:

4.2.1 Modalidad Comparecencia personal ante CertiNet o Notario Público.

En caso que el titular opte por el servicio de Firma Electrónica Avanzada con almacenamiento de llaves en dispositivo Token, se aplica un proceso de enrolamiento que consta, en general, de las siguientes actividades.

- Solicitud de antecedentes de emisión de Firma Avanzada de acuerdo a lo establecido en el punto 3.1 Registro Inicial.
    - El titular levanta el requerimiento formal de un certificado de Firma Electrónica Avanzada
    - Se obtienen los datos para establecer contacto
    - Se obtienen los datos preliminares del titular.
- Validación de Identidad del titular Presencial:

- Verificación de documento de identidad. Se verifica vigencia y pertinencia del documento. Se utiliza la verificación en línea del Registro Civil.
- Comprobación presencial observando el documento de identidad validado. Se obtiene evidencia fotográfica del titular, esto se puede hacer tanto las oficinas físicas de la RA o por Notaría.

- Aprobación de la emisión
  - El oficial de Registro entregará evidencias de las piezas de identificación de Solicitante que quedarán los repositorios de CertiNet
  - El supervisor frente a las evidencias y los antecedentes previos validados autoriza la emisión del Certificado al Token específico.
  - Con esos elementos el sistema genera los códigos de validación, los que son enviados al correo del solicitante, y el código de autorización para el enrolador, con ambos códigos se puede continuar con el proceso. El código de autorización permite que el enrolador firme el acto presencial frente al solicitante.
- Validación Técnica:
  - Apoyo en la configuración de Drivers
- Configuración del dispositivo criptográfico Token.
  - Se le entregan las recomendaciones de seguridad básicas para la creación de la contraseña con la que el Titular/usuario debe proteger el dispositivo.
  - Se entrega la información referente al cuidado del dispositivo Token y a la contraseña que da acceso al Certificado.
- El Solicitante Descarga de Certificado con las clave antes enviada al correo junto con clave del enrolador:
  - Acceso a la interfaz web de CertiNet para validar la Solicitud de emisión de certificado de firma avanzada.
  - El Titular/usuario ingresa los códigos de validación de la solicitud para confirmar su correo electrónico y los datos con los cuales será creado el certificado.
  - El Titular/usuario autoriza la generación del certificado e ingresa la Clave Personal con la que protege el dispositivo de almacenamiento.
- Evidencias de emisión de Certificado y cierre de enrolamiento
  - Se induce al Titular/usuario para que realice pruebas de funcionamiento en el sitio web que CertiNet dispone para ello. Se obtiene evidencia de esta validación.
  - Se entrega información general sobre el Certificado de Firma Electrónica Avanzada, ley que la regula, vigencia del certificado, aviso de vencimiento.
  - Se procede a firmar el Contrato como Titular/usuario de su certificado.
  - Ejecutivo de enrolamiento adjunto las evidencias de enrolamiento en las instancias definidas por CertiNet para el resguardo.
  - CertiNet mantiene Log de información del proceso.

4.2.2 Modalidad Comparecencia personal en el domicilio comercial.

En caso que el titular opte por el servicio de Firma Electrónica Avanzada con almacenamiento de llaves en dispositivo Token, se aplica un proceso de enrolamiento que consta, en general, de las siguientes actividades.

- Solicitud de antecedentes de emisión de Firma Avanzada de acuerdo a lo establecido en el punto 3.1 Registro Inicial.
    - El titular levanta el requerimiento formal de un certificado de Firma Electrónica Avanzada
    - Se obtienen los datos para establecer contacto
    - Se obtienen los datos preliminares del titular.
    - El Titular debe agendar Hora para el proceso de Enrolamiento
- Validación de Identidad del titular Presencia a Domicilio:
    - El oficial de Registro comparece en la dirección agendada para la visita.
    - Verificación de documento de identidad. Se verifica vigencia y pertinencia del documento. Se utiliza la verificación en línea del Registro Civil.
    - Comprobación presencial observando el documento de identidad validado. Se obtiene evidencia fotográfica del titular, esto se hace en el domicilio comercial del cliente, mediante el uso de los mecanismos de seguridad transportables que CertiNet dispone para ésta opción:
        - Computador asignado por Certinet securitizado y protegido con password.
        - Acceso privado a la AR Certinet, con validación de FEA del oficial de Registro.
        - Autenticación a la AR se realiza mediante autenticación con FEA del oficial de Registro.
- Configuración del dispositivo criptográfico Token.
    - Se le hace entrega del Token.
    - Se entrega la información referente al cuidado del dispositivo Token y a la contraseña que da acceso al Certificado.
    - Se le entregan las recomendaciones de seguridad básicas para la creación de la contraseña con la que el Titular/usuario debe proteger el dispositivo.
    - Se le solicita al usuario que formatee e inicialice el Token con su propia contraseña.
    - El Titular, en su Propio Computador, descarga los Drivers para el Token.

- Aprobación de la emisión
    - El oficial de Registro entregará evidencias de las piezas de identificación de Solicitante que quedarán los repositorios de CertiNet
    - El supervisor frente a las evidencias y los antecedentes previos validados autoriza la emisión del Certificado al Token específico.
    - Con esos elementos el sistema genera los códigos de validación, los que son enviados al correo del solicitante, y el código de autorización para el enrolador, con ambos códigos se puede continuar con el proceso.

- Validación Técnica:

- Apoyo en la configuración de Drivers

- El Solicitante Descarga de Certificado con las Códigos enviado al correo junto con Código del enrolador:
  - Acceso a la interfaz web de CertiNet por medio de una sesión segura encriptada para validar la Solicitud de emisión de certificado de firma avanzada.
  - El Titular/usuario ingresa los códigos de validación de la solicitud para confirmar su correo electrónico y el acto presencial.
  - Si el Sistema de Gestión de CertiNet, verifica los Códigos y si son válidos, entonces usando los protocolos PKI solicita que Token inicie el proceso de descargar el Certificado.
  - El Titular/usuario autoriza la generación del certificado e ingresa la Clave Personal con la que protege el dispositivo de almacenamiento.
  - Entre el Token y la interfaz web de CertiNet manteniendo la conexión segura, se descarga el Certificado en el token.
- Evidencias de emisión de Certificado y cierre de enrolamiento
  - Se induce al Titular/usuario para que realice pruebas de funcionamiento en el sitio web que CertiNet dispone para ello. Se obtiene evidencia de esta validación.
  - Se entrega información general sobre el Certificado de Firma Electrónica Avanzada, ley que la regula, vigencia del certificado, aviso de vencimiento.
  - Se procede a firmar el Contrato como Titular/usuario de su certificado.
  - Ejecutivo de enrolamiento adjunto las evidencias de enrolamiento en las instancias definidas por CertiNet para el resguardo.
  - CertiNet mantiene Log de información del proceso.

4.2.3 Esquema general de enrolamiento FAR.

Modelo de negocio de Firma con Autorización Remota en el servicio de custodia central Segura de CertiNet, acreditado según consta en Oficio Folio OFIC202200037 de fecha 05-01-2022, de la Subsecretaría de Economía y Empresas de Menor Tamaño.

En caso que el titular opte por el servicio de custodia central, deberá utilizar un teléfono móvil o dispositivo inteligente para asociarlo al uso exclusivo del certificado de firma electrónica avanzada que se emita en el proceso de enrolamiento:

- Solicitud de antecedentes de emisión de Firma Avanzada de acuerdo a lo establecido en el punto 3.1 Registro Inicial.
- Sitio web de CertiNet:
  - Informa sobre características del servicio, valores, facturación, necesidad de validar clave única y de pagar con transferencia con cuenta asociada al RUT del solicitante, que corresponde al mecanismo complementario.
- Titular Solicitante: Acepta las condiciones del servicio
- Validación de identidad del Titular:

- Inicia proceso con validación fehaciente de Identidad con Clave Única más mecanismo complementario, que es Transferencia de Fondos del mismo RUT del Titular.
- Se solicita validar Identidad con Clave Única.
- Si la respuesta de validación de la clave única es exitosa, se solicita Pago.
- Solicita pago con transferencia con cuenta asociada al RUT del solicitante
- Inicia proceso de pago online.
- Recepción del pago y validación del RUT del solicitante.
- La autoridad de Registro verifica que el RUT del solicitante corresponda al entregado en con la Clave Única.
- Envío de comprobante de pago a cliente.
- Registro interno de datos para identificar el propietario del pago.
- Botón “Actualizar” para que cliente compruebe el registro de su pago.

- Proceso de Creación del Certificado: Crea Certificado y Solicita datos de registro del dispositivo.
  - Con el pago verificado y datos recolectados, se crea el Certificado de Firma Electrónica Avanzada, que es almacenado en el repositorio seguro de CertiNet.
  - Solicita Crear Contraseña para la autorización del Certificado (ídem Token) para la aplicación FAR CertiNet, además se solicita Correo donde se enviará Código Validación, y Número Teléfono Móvil donde se enviará OTP.
  - Informa pasos a seguir descargar app de firma.
  - Muestra códigos QR para la descarga de la APP (uso opcional).
  - Se envía correo electrónico al registrado con la información para descargar la APP.
- Registro del teléfono móvil que autorizará firma:
  - Teléfono Móvil para activación de segundo factor de seguridad.
  - Inicio de sesión en el Dispositivo con la aplicación FAR de CertiNet con RUT del titular y contraseña del Certificado (de autorización) que está en el HSM de CertiNet (ídem Token).
  - Registro del teléfono móvil ingresando códigos de validación recepcionados, uno por Correo y el otro por SMS al teléfono móvil (dos canales).
  - Uso de Método de Desbloqueo, que es obligatorio para asegurar el control del teléfono móvil.
  - Si el Titular/usuario asegura tener el control del teléfono móvil, entonces completa el registro del teléfono móvil de firma.
- Evidencias de emisión de Certificado y cierre de enrolamiento
  - Se solicita al Titular/usuario para que realice pruebas de funcionamiento en el sitio web que CertiNet dispone para ello. Se obtiene evidencia de esta validación.
  - Se entrega información general sobre el certificado de Firma Electrónica Avanzada, ley que la regula, vigencia del certificado, aviso de vencimiento.
  - Contrato Titular/usuario firmado.
  - Ejecutivo de enrolamiento adjunto las evidencias de enrolamiento en las instancias definidas por CertiNet para el resguardo.
- Requisitos Copulativos:

- Es requisito que el teléfono móvil tenga elemento seguro y método activo de desbloqueo,
- No es posible el cambio o recuperación de la clave de autorización.
- Después de varios intentos erróneos (15 ídem a Token) se bloquea el certificado. Dado que es un parámetro se podrá definir en 5 dependiendo del modelo de seguridad.

4.3 Aceptación del Certificado por parte del Titular/usuario

Se entiende que un certificado ha sido aceptado por parte del Titular/usuario una vez que: i) haya firmado el contrato de Suscriptor, ii) 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, iii) No se haya formulado un reclamo por error o inexactitud en la emisión, al momento de su recepción, iv) La utilización, por parte del "Titular/usuario", 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 "Titular/usuario".

Aceptando el Certificado, el Titular/usuario confirma y acepta lo siguiente:

a) que cada firma electrónica avanzada creada utilizando sus datos de creación de firma o llave privada combinada con la Contraseña es la firma del Titular/usuario,
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 ni la Contraseña,
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

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, de acuerdo al modelo comercial que el cliente libremente opte.

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 llave privada se corresponde con la llave pública contenida en el Certificado del Titular/usuario

(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 Titular/usuario con esta firma. Para lo anterior, debe verificar que los atributos del certificado del Titular/usuario, sean los adecuados para firmar dicho mensaje o documento.

4.5.2 Efecto de validar al Titular/usuario

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

(1) fue creada durante el período de vigencia de un certificado de Firma Electrónica Avanzada válidamente emitido de acuerdo a la "CPS-FEA 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-FEA CertiNet" por parte del Titular/usuario y,

(4) el tercero que confía ha cumplido con todos los requisitos de esta "CPS-FEA 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 Tercero que confía en un mensaje o documento firmado electrónicamente por un Titular/usuario, puede confiar en la Firma Electrónica Avanzada acorde a esta "CPS-FEA 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) Si las circunstancias indican que se deben tomar medidas de confirmación adicionales, tales como recibos digitales, consultas en línea u otros.

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 Titular/usuario 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 Titular/usuario 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 llave privada del Titular/usuario ha sido comprometida, etc.

Para los efectos señalados en la letra a) el Titular/usuario 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 Titular/usuario, o por la verificación en el sistema de Clave Única.
- Notificación enviada por el Titular/usuario a la Autoridad de Registro o a CertiNet utilizando Firma Electrónica Avanzada, según corresponda.
- Por comparecencia presencial 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. Por seguridad la *suspensión* corresponde a una *revocación* donde se le reconoce el periodo pendiente de uso del certificado, si el titular lo determina se procede a enrolar con otro 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 Titulares/Usuarios deberán cuidar con igual diligencia que para un certificado vigente, la llave privada correspondiente a todo el período de un certificado suspendido, hasta la destrucción de las llaves.

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) Reconocimiento del periodo de pendiente de uso.
c) Nuevo Enrolamiento del Suscriptor, si así lo desea.

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 Contraseña del Titular/usuario.
g) Por cese de la actividad de CertiNet, a menos que los Certificados sean transferidos a otro Prestador.
h) Por incumplimiento de parte del Titular/usuario 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 afectará el valor de los Certificados y los derechos y obligaciones constituidos bajo su vigencia, en un momento anterior a la adopción de la medida.

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 Titular/usuario, mediante:

- Notificación enviada por este último y además su comparecencia presencial ante CertiNet o ante la Autoridad de Registro correspondiente, a fin de ratificar la información enviada.
- Notificación usando Clave Única.
- 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 Titular/usuario desea continuar usando un Certificado. Para esto el Titular/usuario 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 Titular/usuario. Este aviso se enviará con la antelación necesaria para que el Titular/usuario pueda iniciar el proceso de Renovación correspondiente.

Esta notificación está establecida sólo en beneficio del Titular/usuario, 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, Auditorías 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 realización de la última auditoría 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 cesará voluntariamente de realizar su actividad, se obliga a:

a) Solicitar la cancelación de la inscripción del registro de prestadores acreditados con una antelación no inferior a un mes a la Entidad Acreditadora, indicando el destino que dará a los certificados y sus datos ya sea por la transferencia a otro PSC o si los dejará sin efecto.
b) Comunicar el cese de la actividad a cada uno de los Titulares/usuarios con Certificados vigentes, por medio de correo electrónico, con una antelación mínima de dos meses a la fecha de término.
c) Transferir con consentimiento previo del Titular/usuario, los datos del Certificado a otro Prestador de Servicio de Certificación activo. Se entenderá que existe consentimiento del Titular/usuario si una vez recibida la comunicación señalada en la letra a), el Titular/usuario no manifiesta su oposición dentro los quince días hábiles siguientes.
d) Existiendo oposición del Titular/usuario, el Prestador de Servicios de Certificación deberá dejar sin efecto los Certificados correspondientes.
e) Hacer esfuerzos razonables para que el término de sus servicios cause los mínimos inconvenientes a sus Titulares/usuarios y Terceros que ha confiado o quienes necesiten verificar firma electrónica y/o firma electrónica avanzada cuando corresponda.
f) Pagar una restitución razonable que no excederá el costo de los certificados a los Titulares/usuarios 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.

g) Indicar a la Entidad Acreditadora cualquier circunstancia relevante que pueda impedir su funcionamiento, en particular el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos.

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 Paseo Huérfanos 1052, piso 12, comuna y ciudad de Santiago, Chile. El acceso físico a la sociedad dispone de un esquema de control de acceso acorde a las prácticas de las empresas del sector financiero.

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 24/7 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 Clave Única, OCSP 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 (OCSP), 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 incorporadas 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 Llaves e Instalación

Modelo de Certificación para Firma Electrónica Avanzada las llaves serán generadas por un mecanismo el que estará siempre bajo el control exclusivo del Titular/usuario. Las llaves podrán ser creadas y almacenadas, solo con la contraseña creada por el Titular/usuario 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 un puerto USB dentro del cual se pueden generar, guardar y efectuar procesamientos con las llaves 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 CertiNet están descritos en el Sitio Web de CertiNet. Al utilizar un *Token FIPS-140-2* autorizado por CertiNet, lea cuidadosamente las indicaciones de generación de llaves y almacenamiento de llave privada.

En el caso que el Cliente disponga de su propio Token FIPS-140-2, debe ser dentro de los modelos autorizados por CertiNet y debe dejar constancia que cumple con los requisitos de seguridad, si no los cumple no será posible de usar con CertiNet,

6.2 Protección de la Llave Privada

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

a) La llave privada, contraseñas y factores secundarios de autentificación deben ser protegidas permanentemente por el Titular/usuario, incluso cuando el certificado esté en calidad de suspendido.
b) La Autoridad de Certificación CertiNet y/o La Autoridad de Registro, bajo ninguna circunstancia mantienen, custodian, protegen o acceden a las llaves privadas, contraseñas o factores secundarios de autentificación pertenecientes a Titulares/usuarios, independientemente del mecanismo que hayan escogido. Excepto que en caso del Servicio de Custodia Central Segura de CertiNet en el cual se aplican los más altos estándares de seguridad y protección conforme a las normas vigentes y el decreto 24 de 2019 de la Subsecretaría de Economía.

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

- ✓ Las llaves generadas por la CA se generarán utilizando un algoritmo reconocido por la industria como apto para los usos identificados en esta política durante el tiempo de validez del certificado.
- ✓ Las llaves generadas por la CA tendrán una longitud de clave y se utilizarán con un algoritmo de clave pública que reconocida por la industria como apta para los fines establecidos en esta política durante el tiempo de validez del certificado.
- ✓ Las llaves generadas por la CA, se generarán y almacenarán de forma segura antes de la entrega del certificado al Titular/Usuario.
- ✓ Tanto la llave privada, contraseñas o factores secundarios de seguridad del Titular/Usuario se generarán bajo el exclusivo control de este, conforme a lo descrito en la CP-FEA CertiNet y esta CPS, de manera que no se comprometa el secreto y la integridad de la misma.
- ✓ Tanto la llave privada, contraseñas o factores secundarios de seguridad del certificado de firma electrónica avanzada del Titular/Usuario, están siempre bajo el control exclusivo de este. CertiNet no tiene ni mantiene ninguna copia.

6.2.1 Llaves en *Token* USB

CertiNet publicará en la página WEB la lista de los *Tokens* autorizados que deben cumplir con el Estándar de seguridad FIPS 140-2 y con los requisitos de seguridad de CertiNet, indicando específicamente las opciones de llaves que se requiere manejar.

6.2.2 Llaves 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 claramente respecto a su fiabilidad que cumplen con las siguientes normas 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 Llaves

CertiNet informa a sus Titulares/usuarios, la importancia sobre la protección de su llave privada, contraseñas o factores secundarios de seguridad. Para que utilice con precaución el medio de almacenamiento o acceso a la llave privada que haya seleccionado libremente. Para el dispositivo de almacenamiento individual (Token) y para el mecanismo de acceso a las llaves almacenadas por Custodia Central Segura de CertiNet (HSM), el Titular/Usuario debe proteger con una Contraseña el acceso a utilizar la llave privada para funciones criptográficas, por lo que debe prevenir tanto que la contraseña no sea vista

al momento de ingresarla, ni copiarla del contenedor, ni adulterarla, para lo cual el Titular/Usuario debe tener a lo menos las siguientes precauciones:

- Mantener la llave privada protegida bajo *contraseña* considerada segura.
- Mantener solamente registrada en la memoria la *Contraseña* utilizada para proteger la llave privada
- No copiar la *Contraseña* en papel u otro medio fácilmente legible
- Mantener un respaldo de la información de certificados en un lugar seguro, protegido también bajo mecanismos de protección pertinentes.
- Sin perjuicio de lo anterior CertiNet, expresa claramente que sea, por pérdida o caducidad de la *Contraseña* señalada por exceder el número máximo de intentos, se traducirá en la pérdida total de esta y por tanto se producirá la imposibilidad de acceder a su certificado.

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 Llave 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.

CertiNet declara que las llaves de la CA-Raíz y las de Titular/Usuario se han generado en circunstancias controladas. La generación de llaves se lleva a cabo en un entorno físicamente seguro por personal en roles de confianza bajo al menos doble control utilizando una longitud de llave y algoritmo reconocido por la industria. Tanto la “Llave privada” como así y la “contraseña que dará acceso al certificado”, son generadas por un mecanismo que está bajo el control exclusivo del Titular/Usuario.

Tanto la llave raíz como los repositorios críticos en términos de seguridad se encuentran en las instalaciones seguras de CertiNet, usando 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 a considerar respecto de la seguridad en este caso están cubiertos en por CertiNet, estos aspectos se representan en el siguiente esquema:

6.4.1 Seguridad de Redes

La implantación de la Certificadora incluye un perímetro de seguridad que permita 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.

El segmento de LAN donde se instalan 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, ésta residirá en un ambiente de seguridad estándar de la industria.

- **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 del hardware. Adicionalmente el sistema que administra el servicio fue acreditado para operar 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 auditoría tecnológica.
- Auditoría del modelo de generación de la Llave 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 Llave Raíz

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

La 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 Llave Raíz tanto del 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.

En particular:

- ✓ La clave de firma privada de CA se mantendrá y utilizará dentro de un dispositivo criptográfico seguro que:
  - Cumple con los requisitos identificados en FIPS PUB 140-1 [2], o FIPS PUB 140-2 [3] nivel 3 o superior; o
  - cumple con los requisitos identificados en uno de los siguientes acuerdos de taller CEN 14167-2 [6], CWA 14167-3 [7], CWA 14167-4 [8]

- ✓ Cuando se encuentre fuera del dispositivo de creación de firmas la clave de firma privada de la CA deberá ser protegida de una manera que garantice el mismo nivel de protección que proporciona el dispositivo de creación de firmas.
- ✓ La clave de firma privada de la CA debe ser respaldada, almacenada y recuperada solo por personal en roles de confianza utilizando, al menos, doble control en un entorno físicamente seguro. El número de personal autorizado para llevar a cabo esta función se reducirá al mínimo y serán coherentes con las prácticas de la CA.
- ✓ Las copias de seguridad de las claves privadas de firma de la CA estarán sujetas al mismo o mayor nivel de controles de seguridad que las llaves actualmente en uso.
- ✓ Cuando las claves se almacenen en un módulo de hardware de procesamiento de claves dedicado, se deberán implementar controles de acceso para asegurarse que no se pueda acceder a las teclas fuera del módulo de hardware.

6.4.3 Distribución de la llave pública CA-Raíz

CertiNet declara que la integridad y autenticidad de la llave (pública) de verificación de firma del Ca-raíz y cualquier parámetro asociado se distribuyen a Titulares/usuarios o terceras partes que confían a través de la Entidad Acreditadora de la Subsecretaría de Economía y empresas de menor tamaño en https://www.entidadacreditadora.gob.cl/entidades/ y/o https://www.certinet.cl/acreditacion

6.4.4 Usos de la llave de la autoridad de certificación:

CertiNet declara que la llave de firma privada de esta solo se utiliza para generar certificados y/o emitir información de estado de revocación.

6.4.5 Fin del ciclo de vida de la llave de CA-Raíz:

CertiNet no utiliza la llave privada más allá del final de su ciclo de vida.
En particular:

- ✓ El uso de la llave privada de la CA se limitará a la compatible con el algoritmo hash, el algoritmo de firma y la longitud de la llave de firma utilizada en los certificados generadores, de acuerdo con la práctica actual.
- ✓ Todas las copias de las llaves privadas de firma de la CA se destruirán o dejarán de utilizarse al final de su ciclo de vida.

6.4.6 Gestión del ciclo de vida del hardware criptográfico utilizado para firmar certificados:

CertiNet durante el ciclo de vida del dispositivo criptográfico:

- ✓ La información de estado de revocación y/o vigencia del certificado que firma el hardware criptográfico no se manipula durante el envío.
- ✓ La información de estado de revocación y/o Vigencia del certificado que firma el hardware criptográfico no se manipula mientras se almacena.

- ✓ La instalación, activación, respaldo y recuperación de las llaves de firma privada de CA-Raíz en el hardware criptográfico se mantiene bajo el control simultáneo de al menos dos empleados de confianza.

7. Perfiles de Certificados y CRL

7.1 Perfil del Certificado

7.1.1 Clases de Certificados

CertiNet Modelo de Certificación 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, Titulares/usuarios o terceros que confían, quienes deberán en forma individual establecer el uso que le darán.

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 llave pública.
b) Código de Identificación del Certificado.
c) Identificación del Titular/Usuario del Certificado.
d) Llave pública del Titular/Usuario o bien un elemento de verificación de firma que corresponda a un elemento de creación de firma.
e) Algoritmo de firma del Titular/Usuario 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 (128-bit), encriptación asimétrica con largo de llaves de 1.024 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 Titular/Usuario: ● 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. Excepto que el Titular/Usuario determine alguna de las opciones comerciales disponibles.

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 Titular/Usuario y CertiNet.

7.2 Perfil de CRL (Lista de Certificados revocados)

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.

Estructura de la CRL:

7.2.1 Número de Versión

Cada CRL emitida cuenta con un número de versión que permite identificarla.

7.2.2 Periodo de emisión y validez:

Las CRL, son archivos públicos que tienen una vigencia de 24 horas. Estas se reemiten cada 4 horas o cada vez que un certificado es revocado.

7.2.3 Publicación:

Las CRLs se Publican y difunden a través de nuestra página web en:
https://www.certinet.cl/acreditacion

7.2.4 CRLs y Extensiones:

Las CRLs, contienen la siguiente información:

- ✓ Número de Versión
- ✓ Emisor
- ✓ Fecha Efectiva
- ✓ Fecha de Actualización
- ✓ Algoritmo de firma y de Hash de firma
- ✓ Identificador llave pública de Entidad Emisora
- ✓ Número de la CRL

8. Administración de esta Declaración de prácticas:

8.1 Procedimientos de Modificación de la CPS

Esta Declaración de prácticas, podrá ser modificada por CertiNet según lo requiera para mantener los estándares de calidad de sus servicios, las imposiciones normativas y en general cualquiera otra que CertiNet estime pertinente.

8.2 Procedimientos de Aprobación de las CPS

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

- ✓ Desarrollo y presentación a los organismos técnicos y fiscalizadores competentes para recepción de observaciones y sugerencias.
- ✓ Presentación y Aprobación intermedia ante el Comité de Seguridad de la Información.
- ✓ Presentación y Aprobación de la Gerencia General de CertiNet.
- ✓ Presentación y Aprobación de la Entidad Acreditadora del MMEE.

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

8.3 Políticas de Publicación y Notificación

- ✓ Será publicada en su sitio https://www.certinet.cl al menos 30 días antes de su entrada en vigencia.

- ✓ Se entenderá notificada en concordancia con los numerales 2.1.6 y 2.5 de la política de Certificación CP-FEA CertiNet. Los Titulares/usuarios que no estén de acuerdo con actualizaciones o modificaciones efectuadas, tendrán derecho a solicitar voluntariamente la revocación o término del servicio sin devolución económica por la parte no consumida del mismo. Sin perjuicio de las garantías legales respecto a las eventuales validaciones posteriores que se requieran a petición de parte competente para efectos de garantizar el No-Repudio de las firmas efectuadas y/o los derechos que pudiere haber adquirido respecto de la versión de esta CPS-FEA CertiNet y la política CP-FEA CertiNet, vigentes al momento de la contratación de los mismos.

  Sin perjuicio de lo anterior, esta Política se entenderá vigente y válida, solo cuando esté firmada por la Gerencia General de CertiNet o quien le subrogue.

9. Control Documental

Cuando sea necesario se actualizará la Política, asociado a los servicios de certificación, para garantizar la excelencia del servicio y mejora continua, a fin de adecuarlo a las características de uso del momento.

Roberto Riveros Durán
Gerente General

Ignacio Infante Pinto
Oficial de Seguridad