Política de Certificados (CP)

Firma Electrónica Avanzada

PSC
CERTINET

Confidencial

Audiencia

Profesionales del área de operaciones y tecnología de los Bancos o de empresas que estén involucrados con la puesta en marcha u operación de la Aplicaciones que reciben objetos electrónicos firmados electrónicamente.

Versión	Descripción	Fecha	Autor
0.1	Primer borrador del documento	28/04/04	R. Riveros
0.2	Segundo borrador	02/05/04	A. Carratalá
1.0	Primera Versión del Documento	26/03/04	R.Riveros
1.1a	Entra en vigencia el 1/6/04	31/05/04	R. Riveros
1.2	Eliminación de referencia a texto de firma electrónica	03/11/10	C. Ríos
1.3	Incorporación en Punto 2 - Especificar a quien se debe otorgar certificado de firma avanzada Incorporación Obligaciones Incorporación Responsabilidades Incorporación Propósitos	20/12/2011	C. Ríos
1.4	Actualización Formatos	30/09/2014	S.Mercado
1.5	Actualización formatos e Índice	09/03/2015	A.Carreño
1.6	Actualización tipo de algoritmo de firma SHA1 a SHA2	13/01/2016	A.Carreño
1.7	Actualiza CPS e incorpora mecanismo de custodia de Certificados y Clave Privada y características de nuevo Certificado	01/04/2019	A. Carreño R. Riveros

Contenido

1 Introducción

1.1 Modelo Certinet

El Modelo de certificación de Certinet (Certinet S.A.) tiene como objetivo proveer servicios de certificación para firma electrónica que permita apoyar el desarrollo de negocios electrónicos para la Banca y otros clientes. Dentro de los roles de Certinet está el identificar en conjunto con las áreas de negocios de nuestros clientes, las mejores prácticas de operación comunes a la industria.

En el establecimiento de esta certificadora se han considerado los aspectos legales, tecnológicos, comerciales y operacionales de un Modelo de Confianza que aplica como respuesta a las necesidades detectadas por las áreas de negocio de nuestros clientes y quienes decidan libremente confiar en este.

El Modelo incorpora los requisitos de la ley de firma electrónica, su reglamento asociado, las guías de acreditación para que la firma electrónica tenga carácter legal y cumpla con los requisitos de la firma electrónica avanzada, mediante la aplicación de procedimientos y normas de nivel mundial, que Certinet adopta como Autoridad Certificadora en la provisión de Servicios de Certificación. Y que se plasman en la declaración de prácticas de certificación (CPS), de Certinet S.A.

Visión de Globalización: Se dispone de una visión de evolución clara del Modelo que incluye la interoperación y adherencia a los estándares cuando sea requerido con otros modelos de confianza globales, por lo que la selección de la entidad o la plataforma de PKI que provea el servicio de raíz global es primordial.

Visión de largo plazo: Este modelo se ha establecido siguiendo una visión de largo plazo considerando en esto; procedimientos y otros elementos legales y tecnológicos asociados, que garanticen que los productos derivados (tales como documentos firmados digitalmente), tengan validez más allá de los plazos que la ley prevé.

Principales características del modelo Certinet:

- Modelo de Confianza para el e-Business: Certinet estableció un Modelo de Confianza Bancario integral soportado en la infraestructura de claves públicas y privadas (PKI), lo que considera integrar todo el conjunto de elementos tecnológicos y operacionales que lo conforman, considerando específicamente lo que son las prácticas y procedimientos comunes a la industria de los Bancos.

Este modelo es aplicado y ajustado de acuerdo a las necesidades específicas de cada cliente o grupo de clientes y las Leyes y normas que los rigen.

- El Modelo se desarrolla sobre la infraestructura PKI, por el hecho de que dispone de la aceptación tecnológica y legal adecuada para otorgar seguridad a los negocios electrónicos, tanto a nivel local como mundial.
- Disponer de un punto de convergencia del know-how: desde el punto de vista operacional, tecnológico y de las prácticas asociadas, lo que permite compartir la experiencia de los diferentes clientes en particular los bancos y, así disminuir costos ofreciendo beneficios concretos en un ambiente de negocio.
- Soporte a la No Repudiación: para disponer de adecuada confianza para los negocios, es fundamental no solo disponer de la tecnología adecuada, sino que también asegurar que los procesos críticos no la afecten, entre ellos se incluyen el registro homogéneo de los clientes, la adecuada seguridad tecnológica y operacional junto con la adecuada disponibilidad de servicios.
- Los servicios prestados por Certinet están diseñados para disponer de Alta Disponibilidad en sus procesos críticos, por este motivo se tiene conciencia de los aspectos relevantes a ser solucionados ante eventualidades, para disminuir las posibles afecciones a los procesos electrónicos y operativos de Certinet.

1.2 Objetivos del Documento

El presente documento presenta las acciones que debe efectuar toda persona titular de un certificado digital emitido por Certinet para producir una firma digital, la aplicación utilizada para generar dicha firma y el tipo de dispositivo o servicio que utilizará para custodiar y activar dicha firma, como así, almacenar los datos generados por la misma, así como toda persona, empresa, aplicación que recibe un documento u otro objeto firmado electrónicamente y debe determinar si las condiciones de validación son correctas.

Los criterios para otorgar confianza de una firma electrónica, tal como se encuentra establecido por Certinet, también se encuentra descrita dentro de este documento.

2 Titular del Certificado

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

Todo titular de un certificado digital emitido por la Autoridad Certificadora CERTINET lo puede utilizar para firmar documentos o recibir documentación encriptada para él.

Sus responsabilidades se encuentran descritas en el Acuerdo de Suscriptor y/o contrato aceptado previamente a la emisión del mismo y Prácticas de Certificación disponibles en Sitio Web Público de Certinet www.Certinet.cl. Sin detrimento de ninguna de las responsabilidades allí indicadas, es importante resaltar:

- El certificado es personal e intransferible. Todo acto generado por el mismo será considerado como propio aunque el mismo haya sido realizado por otra persona a la cual le ha entregado una copia o acceso al dispositivo de firma o de activación de la misma.
- Si bajo cualquier circunstancia considera que el dispositivo de firma o activación de la misma ha sido vulnerado debe solicitar inmediatamente la revocación del certificado.

3 Obligaciones

3.1 Certinet

Se obliga a:

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

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

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

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

e) Emitir los certificados en conformidad al procedimiento establecido en las “CPS Certinet”.

f) Proveer mecanismos de custodia de llaves del cliente como Token, y/o la custodia y la disponibilidad de las llaves que el cliente libremente haya escogido guardar en repositorio seguro central de Certinet.

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

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

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

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

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

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

3.2 Autoridad de Registro (RA)

Son funciones de la Autoridad de Registro

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

b) Registrar y custodiar los antecedentes requeridos a los solicitantes que permitan una identificación plena de los mismos, de conformidad con los requisitos establecidos en las Prácticas Específicas (CP) correspondientes a los Certificados.
c) Aprobar o denegar las Solicitudes de Emisión de Certificados.
d) Entregar al Suscriptor su Certificado o dar las instrucciones para su retiro, y/o uso, según el mecanismo de custodia que el cliente haya elegido libremente.
e) Recibir las Solicitudes de revocación o suspensión de Certificados, e informarlas a Certinet.
f) Obtener la aceptación de los términos y condiciones del servicio por parte del Solicitante mediante la firma de la Solicitud o Contrato.
g) Conservar en forma segura, la información recibida en el proceso de emisión, suspensión y revocación de un certificado por el período que la Ley de Firma Electrónica y su Reglamento indiquen.
h) Permitir operar solamente certificados que hayan sido aceptados por el Solicitante.
i) Prestación de otros servicios que Certinet le solicite.
j) Todas las actuaciones indicadas en las letras anteriores, las realiza la Autoridad de Registro en representación y por cuenta y riesgo de Certinet.

3.3 Obligaciones del Suscriptor

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

a) Establecer una solicitud formal de emisión de certificado, en la que acepta los términos y condiciones descritos en la “CPS Certinet”.
b) Cumplir con los requerimientos de información solicitados por Certinet y/o la Autoridad de Registro de conformidad a la presente “CPS Certinet”.
c) Seleccionar, Token y custodiar el dispositivo para almacenamiento seguro de los datos asociados a la generación de firma, ya sea individual o custodiado, y generar en él, el par de claves utilizadas en el proceso de firma por medios que estén bajo su exclusivo control.
d) El usuario puede elegir libremente almacenar las llaves para creación de firma en un Dispositivo individual físico o bien usar el servicio de custodia central seguro que CERTINET mantiene en alta disponibilidad con acceso remoto y bajo los mismos resguardos establecidos por el PSC en su Política de Seguridad, no obstante se deja

especial constancia que el Usuario Titular de un Certificado es el único que puede accesar a la Llave Privada de su Certificado, teniendo por lo mismo un exclusivo control y acceso a ésta.

e) No revelar la clave de acceso al dispositivo que contiene la clave privada asociada al certificado y/o no relevar el mecanismo de activación de la firma.

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

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

Una vez emitido el certificado el Suscriptor se obliga a:

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

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

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

k) Utilizar correctamente el Certificado, el que se entrega en depósito.

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

m) Comunicar inmediatamente a la Autoridad de Registro y/o a Certinet el compromiso, pérdida, hurto, robo, extravío, falsificación de su clave privada o certificado o cualquier circunstancia que pudiera ser causal de suspensión o revocación de un Certificado.

n) Comunicar la pérdida o destrucción del dispositivo enrolado para utilización de los certificados ya sea en dispositivo físico o en custodia.
o) Custodiar la clave privada, tomando precauciones razonables para evitar su pérdida, modificación y uso no autorizado.
p) Solicitar la suspensión o revocación del Certificado cuando se presente alguna de las causales indicadas para este efecto
q) Abstenerse de usar la clave privada una vez que el Certificado haya expirado o haya sido solicitada la suspensión o revocación.
r) Destruir la clave privada en caso de que Certinet así lo exija y haya sido revocado previamente el certificado.

3.4 Obligaciones de los Usuarios

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

a) Verificar la validez del certificado mediante consulta al registro de certificados,
b) Verificar la firma del Suscriptor,
c) Comprobar las restricciones de uso que figuren en el certificado y las prácticas “CPS Certinet” y,
d) Validar el uso de certificado para propósitos autorizados de conformidad con la legislación vigente.

4 Responsabilidades

4.1 Certinet

Es responsable de:

a) Emitir el Certificado cumpliendo todas las exigencias materiales requeridas en la “CPS Certinet”, y de conformidad con los datos entregados por el Suscriptor.
b) Que el Certificado no contenga errores de trascripción de los datos recogidos del Suscriptor, y se ha emitido ejerciendo la actividad con diligencia y cuidado razonable.
c) Que la información incluida o incorporada por referencia en el Certificado sea exacta.
d) Publicar el Certificado en el directorio correspondiente.

e) La aplicación correcta del procedimiento empleado.

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

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

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

4.2 Limitaciones de Responsabilidad de Certinet.

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

Clase	Tope Máximo de Responsabilidad
Firma Electrónica Avanzada	La establecida en 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. Certinet no podrá ser obligado a indemnizar una suma mayor que el tope máximo de responsabilidad estipulado, por cada certificado.

4.3 Autoridad de Registro

Es responsable de:

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

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

4.4 Suscriptor

El Suscriptor es responsable de:

a) La veracidad de la información entregada a Certinet y/o la Autoridad de Registro al momento de solicitar un certificado.
b) El pago de los servicios solicitados.
c) Mantener bajo su custodia y exclusivo control la clave privada y/o el acceso al mecanismo de activación de firma, desde el momento de su generación hasta su extinción.
d) Abstenerse de usar la clave privada antes de la aceptación del certificado. El Suscriptor es el único responsable de los daños y perjuicios que con su actuación se causen en el evento que use su clave privada y/o mecanismo de creación o autorización de firma mientras no se haya efectuado tanto la aceptación como la entrada en vigencia del certificado.
e) Durante el período de vigencia del certificado, el Suscriptor es responsable y así lo acepta y declara, que cada Firma Electrónica Avanzada creada utilizando su clave privada asociada a la clave pública contenida en el certificado, corresponde a la Firma Electrónica Avanzada del Suscriptor y que el Certificado ha sido aceptado y se encontraba vigente, al momento de la creación de dicha firma.
f) Desde el momento que acepta el Certificado, según lo indicado en el punto 3.3, Letra (g) el Suscriptor será responsable de indemnizar al Prestador de Servicios de Certificación y/o a la Autoridad de Registro, todo daño o perjuicio proveniente de cualquier acción u omisión negligente, culposa o dolosa de su parte.
g) Ratificar que todas las declaraciones que realizó al momento de solicitar el Certificado son verdaderas.
h) Ratificar que todas las declaraciones contenidas en el Certificado se tienen por verdaderas.

4.5 Usuario

El Usuario que confía y usa libre y espontáneamente un Certificado asumirá la responsabilidad y riesgos derivados de la aceptación de dicho Certificado, cuando no

haya realizado en forma previa los pasos necesarios para la verificación de su validez de acuerdo a la "CPS Certinet".

5 Usos del Certificado

5.1 Composición de los Certificados Certinet

Actualmente, CERTINET, tiene en funcionamiento dos CA Root, las que cumplen con los mismos protocolos de seguridad y estándares exigidos por la Ley 19.799 y su reglamento, y aprobadas por la Entidad Acreditadora del Ministerio de Economía.

Por lo anterior y hasta que nuestra Empresa lo determine, se han puesto a disposición de nuestros clientes estos dos tipos de Certificados de Firma electrónica Avanzada, los que tienen orientaciones de uso y funcionamiento específicos.

En forma complementaria y según sea el caso, el usuario puede elegir libremente almacenar las llaves para creación de firma en un Dispositivo individual físico o bien usar el servicio de custodia central seguro que CERTINET mantiene en alta disponibilidad con acceso remoto y bajo los mismos resguardos establecidos por el PSC en su Política de Seguridad, no obstante se deja especial constancia que el Usuario Titular de un Certificado es el único que puede accesar su Certificado, teniendo por lo mismo un exclusivo control y acceso a este.

Sin perjuicio de lo anterior los certificados de Firma Electrónica Avanzada emitidos por Certinet observan un número de extensiones para mejorar la explotación

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

5.1.1 Certificado tipo provisto por CERTINET - Verising:

Nombre	Descripción	Tipo dato	Valor
Versión	Versión del certificado que deberá ser versión 3	fijo	V3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los certificados de firma electrónica avanzada emitidos por Certinet.	variable	75 46 73 7c 9e ba bd 67 98 e3 1b 9f 6b 95 97 37

Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	fijo	SHA2
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = e-mail del Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor C = País	variable	E = Certinet@Certinet.cl CN = Certinet S.A. Firma Electronica Avanzada OU = Class 2 Onsite Individual Subscriber CA OU = Terms of use www.certisur.com/rpaCertinetavanzada (c)06 OU = VeriSign Trust Network O = Certinet S.A. C = CL
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado.	variable	miércoles, 28 de Marzo de 2019 21:00:00 viernes, 28 de Marzo de 2020 20:59:59
Nombre del titular	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500.	variable	E = jperez@enable.cl CN = Jorge Alejandro Pérez Parra OU = Condiciones en www.certisur.com/rpa-Certinet- avanzada (c)06 OU = Certinet OU = Firma Electrónica Avanzada O = Certinet S.A. C = CL
Clave pública	Clave pública del titular del certificado	variable	30 82 01 0a 02 82 01 01 00 84 0b 19 be 0e 6e e0 5f 71 69 55 68 ae 63 5a 81 c5 4c ba 88 dd 9a 06 1a 58 43 88 e4 a4 51 7a aa cc d6 3c 3d a4 bf d8 7e 58 ed a6 bb a5 b0 34 7d c6 6c d2 7f 54 73 fa fc af 86 24 eb a8 40 27 68 54 fe 61 c2 98 c2 ce 1b 50 90 8e 78 70 04 1d f3 a7 0d c2 59 7c 42 65 cb 96 30 af 87 6e eb 2d 87 66 7c 40 c9 bd 43 67 37 ea 08 78 16 ce 8b 6a d5 a6 0f d3 c2 5b a4 ee c8 d0 a2 61 8a 0f aa 47 7c 45 16 80 4e 05 da de 01 49 a0 6b 80 b6 9b 88 87 96 4c 17 c9 af 88 41 7e 81 28 63 e5 e3 57 ed c4 ef 38 e6 bb 85 77 73 50 bc 26 de 78 23 93 5d 7e af 5e 55 71 20 be 6f 41 61 83 45 ff ac ab e0 ce 8e 0b 89 6e 45 31 01 93 0a df b0 12 43 c6 f0 75 92 e9 1b ac 63 17 b7 5c 08 b1 59 1a 37 15 66 96 b6 37 09 05 87 92 69 29 47 c8 df 0e a5 8b d7 b6 43 7a 31 c5 85 08 fb 93 8b e6 d0 e9 83 3a fe 8d 02 03 01 00 01

KeyUsage	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	fijo	Firma digital, Cifrado de clave (a0)
BasicConstrains	Permite diferenciar entre un certificado de PSC y uno de suscriptor final.	fijo	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno
ExtendedKeyUsage	Esta extensión define una serie de propósitos respecto al uso del certificado, adicionalmente a las definidas en KeyUsage. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	fijo	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
AuthorityKeyIdentifier	Medio para identificar la llave pública de Certinet El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier	fijo	Id. de clave=24 35 92 fb b1 5f 82 b8 84 0e de 1f 0d 73 d6 c2 7e 6e 81 94
CertificatePolicy	Ver Política de Certificados	fijo	[1]Directiva de certificados: Identificador de directiva=2.16.840.1.113733.1.7.23.2 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Calificador: https://www.Certinet.cl/cps [1,2]Información de calificador de directiva: Id. de calificador de directiva=Aviso de usuario Calificador: Texto de aviso = Certificado para Firma Electrónica Avanzada. Responsabilidad limitada según CPS(c)06
IssuerAltName	Identificador alternativo del emisor, corresponde al RUT.	fijo	Otro nombre: 1.3.6.1.4.1.8321.2=16 0a 39 39 35 33 32 38 33 30 2d 35

SubjectAltName	Permite definir términos que identifican al sujeto o titular del certificado, adicionalmente a lo establecido en el campo estándar Subject.	variable	Otro nombre: 1.3.6.1.4.1.8321.1=16 0a 31 30 37 31 36 36 39 34 2d 37
CrlDistributionPoint	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la siguiente. estructura: DistribuitonPoint: Un URI para identificar el CRL	fijo	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://onsitecrl.verisign.com /CertinetSAFirmaElectronicaAvanzada/LatestCRL.crl
Algoritmo de identificación		fijo	Sha1
Huella digital		variable	61 3a 05 8e 1e e2 9b 5f f9 55 64 c8 79 fd ea d6 9c a2 4e 04

5.1.2 Certificado tipo provisto por CERTINET - Ascertia:

Nombre	Descripción	Tipo dato	Valor
Versión	Versión del certificado que deberá ser versión 3	fijo	V3
Nº de Serie	Número que identifica unívocamente al certificado dentro de los certificados de firma electrónica avanzada emitidos por Certinet.	variable	75 ee 53 36 c9 fb f3 00 ca 26 0f 94 40 98 a8 ef dc 5f 3c 05
Algoritmo de Firma	Algoritmo utilizado por el PSC para firmar el certificado	fijo	sha256RSA
Nombre del Emisor	Nombre distintivo (DN) del emisor, en el formato del estándar X.500. Deben incluirse los siguientes tipos: CN =Tipo de certificado E = e-mail del Prestador de Servicios de Certificación emisora Número de serie = Número identificador del Emisor C = País	variable	CN = Certinet S A Firma Electronica Avanzada OU = MPKI CA ADSS CertiNet OU = Firma Electrónica O = CertiNet S.A. E = ca-certinet@certinet.cl C = CL
Periodo de Validez	Fecha de inicio y termino en que es válido el certificado.	variable	miércoles, 21 de agosto de 2019 12:50:36 viernes, 21 de agosto de 2020 12:50:36
Nombre del titular (Sujeto)	Nombre distintivo (DN) del titular del certificado, en el formato del estándar X.500.	variable	CN = Felix Gabriel Donoso Zelada E = fdonoso@certinet.cl OU = CertiNet O = CertiNet S.A. L = Santiago S = Metropolitana C = CL
Clave pública	Clave pública del titular del certificado	variable	30 82 01 0a 02 82 01 01 00 cf aa 2e aa 8b 8c b7 f4 f3 7a 46 48 d5 ed 78 3f 6b 18 9c 88 7d f2 21 3d ce 98 93 a8 0e 9e d9 4e 8e 83 6c bb 72 a6 58 6d 64 c5 89 5d 51 4b d6 35 7d 7e 34 87 06 ad 23 81 c3 96 3a fe 95 90 4b 85 07 f4 e4 90 f9 1e e7 f4 fd 28 11 51 60 08 cb 35 be c3 e3 c2 ba 9a 1d bb 58 a4 7b cc 75 a0 4f cd 4b 72 6c c7 aa 16 11 13 a7 02 b3 52 b1 0b ef 3a 71 ed 41 12 d1 6e 85 71 ba 1e c1 35 fb 72 d2 86 f5 b9 64 6c c6 c2 b7 fb 88 b2 08 6c 85 f4 a2 95 07 7a 23 58 b1 66 04 96 4a 87 68 e2 7a 3d 42 0c 69 95 39 b4 0f c0 2e 2a 8d 2f 04

			c4 6b c9 cf f6 d7 56 38 3c c3 7b f8 6f d4 9b 2e 69 a2 ba 0c 08 f0 a1 9b c1 ab bd 78 89 5b 1f 61 2c 0a a8 aa b9 98 0b cf 21 7d 6a de 24 0a b9 3d 37 4e 80 45 68 03 d7 68 35 bb 9f a4 da 78 76 01 c9 27 bc 9d b2 f3 91 63 5e bc 02 bd ad 8a 71 a1 5b 7c e7 3a 89 02 03 01 00 01
Uso de la clave	Esta extensión define el propósito para el cual deben ser usadas las claves correspondientes al certificado. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	fijo	Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (f0)
Restricciones Básicas	Permite diferenciar entre un certificado de PSC y uno de suscriptor final.	fijo	Tipo de asunto=Entidad final Restricción de longitud de ruta=Ninguno
Uso mejorado de claves	Esta extensión define una serie de propósitos respecto al uso del certificado, adicionalmente a las definidas en KeyUsage. El certificado debe ser utilizado sólo para los propósitos definidos por esta extensión.	fijo	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Identificador de clave de entidad emisora	Medio para identificar la llave pública de Certinet El campo KeyId es idéntico al valor de la extensión SubjectKeyIdentifier	fijo	Id. de clave=6a c5 55 0f 4f bc 89 17 f5 e1 65 98 51 01 9a 1e e3 1e 22 19
Directiva del certificado	Ver Política de Certificados	fijo	[1]Directiva de certificados: Identificador de directiva=1.3.6.1.4.1.52428.100 [1,1]Información de certificador de directiva: Id. de certificador de directiva=CPS Certificador: https://pltwww.certinet.cl/cps-clt-FEA [1,2]Información de certificador de directiva: Id. de certificador de directiva=Aviso de usuario Certificador: Texto de aviso=Certificado para Firma Electrónica Avanzada (FEA) Piloto. Sólo para propósitos de desarrollo y pruebas.

Nombre alternativo del emisor	Identificador alternativo del emisor, corresponde al RUT.	fijo	Otro nombre: 1.3.6.1.4.1.8321.2=16 0a 39 39 35 33 32 38 33 30 2d 35
Nombre alternativo del titular	Permite definir términos que identifican al sujeto o titular del certificado, adicionalmente a lo establecido en el campo estándar Subject.	variable	Otro nombre: 1.3.6.1.4.1.8321.1=0c 0a 31 35 33 38 30 31 36 35 2d 37
Puntos de distribución de CRL	En este campo se establece la localización del CRL correspondiente para consultar sobre revocaciones. Contiene la siguiente. estructura: DistribuitonPoint: Un URI para identificar el CRL	fijo	[1]Punto de distribución CRL Nombre del punto de distribución: Nombre completo: Dirección URL=http://crl-adss.certinet.cl/adss/crls/FEA-CA-ADSS-Certinet.crl
Algoritmo de identificación		fijo	Sha1
Huella digital		variable	89 45 cc 94 45 f9 0c db e4 37 f0 57 70 a2 61 84 5c 10 22 0a

6 Aplicación de Firma

Para la generación de una firma electrónica es necesaria la intervención de una aplicación que realice los cálculos computacionales necesarios sobre el documento a ser firmado. También es necesario acceder a los datos de firma del titular del certificado.

Toda aplicación que sea utilizada para generar una firma electrónica o des-encriptar un documento debe garantizar que los datos de firma del titular nunca se encuentran expuestos a terceros usuarios o aplicaciones, independientemente del tipo de almacenamiento de dicho certificado, en nuestro caso, sea un Token físico o el uso de nuestro servicio de custodia central, como también el tipo de mecanismo de activación de firma.

La aplicación desarrollada debe permitir la "verificación inicial" de la firma así como contemplar las condiciones a ser cumplidas para una "verificación habitual", y por lo tanto, generar y almacenar toda la información necesaria.

6.1 Efectos

a) El mensaje o documento electrónico que contenga una Firma Electrónica 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.

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

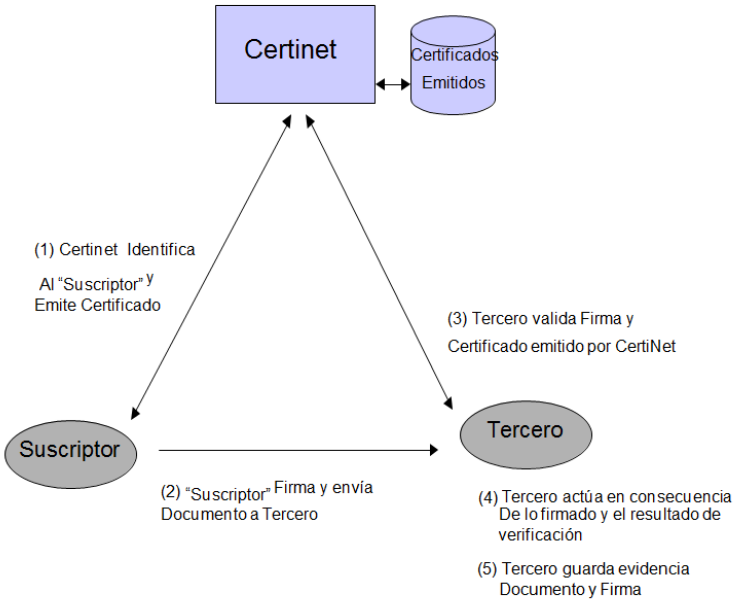
7 Tercero que Confía

El Tercero que Confía corresponde al sujeto persona o empresa el cual recibe información firmada a través de firma electrónica asociada a un certificado y que busca confiar en él.

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.

Para esto Certinet ha establecido dos Autoridades Certificadoras, según haya elegido libremente el suscriptor, las que a través de tecnologías y procedimientos que dispone, permite asegurar la identidad del suscriptor de un certificado para firma electrónica y las acciones que efectúe con él.

En un ejemplo se puede ver que la relación de confianza entre un Usuario “Suscriptor” y otro que recibe “Tercero” está dada por la confianza en una Autoridad Certificadora como Certinet, lo que se representa en el gráfico siguiente:



En el gráfico anterior se realiza la transición de confianza por medio de:

- “Tercero” confía en Certinet y dispone de llave pública de Certinet que le permite verificar su firma en el certificado emitido al “Suscriptor”.
- “Tercero” confía en el certificado del “Suscriptor” puesto que viene firmado por Certinet y puede verificar su firma. El Tercero utiliza los servicios de Certinet para validar el certificado del “Suscriptor”. El Tercero obtiene servicios de Certinet sin ser necesariamente un subscriptor de Certinet.
- El “Tercero” confía por esta transitividad en el “Suscriptor”.
- De la misma forma que el “Tercero” guarda antecedentes/Documentos asociados a una firma, debe guardar los antecedentes electrónicos que permita dar constancia en el futuro de esta firma.

Un tercero que recibe un certificado puede confiar en él, producto que ha sido emitido por una Autoridad Certificadora confiable para él, incluso puede confiar sin necesidad de efectuar validaciones en línea, confiando en la información que contiene el certificado mismo por medio de validar que dicho certificado ha sido emitido (firmado) por la autoridad certificadora en la que él confía.

Para simplificar la verificación por parte del tercero de las Autoridades Certificadoras, tanto los browser como otras aplicaciones de usuario final que utilizan certificados, permiten mantener copias de las llaves públicas de las Autoridades Certificadoras en los cuales el usuario confía, de este modo la validación desde la firma de la autoridad del certificado se puede hacer en forma automática y transparente al usuario.

8 Verificación de Firma

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

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

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

El sistema de verificación debe contemplar dos tipos:

- "Verificación Inicial", es aquella que es realizada de manera próxima a la generación de la misma, de tal manera de recolectar la información adicional que permitirá realizar la verificación en el futuro, por ejemplo, la Verificación Habitual,

- "Verificación Habitual", puede ser realizada en el futuro, incluso años después que la firma fue generada. Para poder ser capaz de realizar este tipo de verificación será necesario contar con los datos recolectados en la Verificación Inicial

Para la "Verificación Inicial" es necesario contar con:

- El texto firmado,
- La firma electrónica, en formato PKCS#7, XMLDsig, ETSI PDF,
- El estatus del certificado del firmante. Para dicho fin, Certinet ofrece tres servicios:
  - Consulta del estado del certificado en el sitio Web de Certinet.
  - Consulta del estado del certificado por medio del servicio OCSP
  - Emisión diaria de la Lista de Certificados Revocados (CRL)

Para la "Verificación Habitual" es necesario contar, además de la misma información que la Verificación Inicial, un registro seguro de fecha y hora que indique el momento de creación de la firma. Es posible lograr este requerimiento por medio de un registro de "timemark" o "Timestamping". Alternativamente es posible indicar la fecha de la firma dentro del texto firmado por el titular del certificado.

La política de verificación acorde con las prácticas vigentes de Certinet, debe:

- 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 que el Certificado del firmante no ha sido revocado y se encuentra vigente en el momento en el que se ha realizado la firma.
- Delimitar la información que haya sido firmada. Para esto los mensajes o documentos firmados deben seguir los estándares PKCS, XMLDsig o ETSI PDF vigentes.
- Indicar dentro de la información firmada la fecha y hora en la que la Firma Electrónica fue creada o referenciar un *timestamp* asociado al evento debidamente emitido.
- Establecer el propósito que intenta el *Suscriptor* con esta firma. Para lo anterior, debe verificar que los atributos del certificado del *Suscriptor*, sean los adecuados para firmar dicho mensaje o documento, por ejemplo debe ser un Certificado de Firma Electrónica Avanzada.

El verificador deberá almacenar la siguiente información para ser adicionada a la firma:

- Lista de Certificados Revocados (CRL) emitida por Certinet

Certinet ofrece un repositorio histórico de CRL emitidas diariamente, el cual puede ser utilizado cómo referencia en el caso que no se desee almacenar la CRL posterior correspondiente a la fecha de generación de la firma.

En la medida que el riesgo asociado a lo firmado aumenta, la aplicación del Tercero que confía debe utilizar mecanismos de validación más eficientes, en ello inciden las razones de revocación, el esquema de publicación y notificación como también la frecuencia de actualización. Certinet publicará con la debida diligencia sus listas de acuerdo a las políticas que tenga publicadas al respecto.

El modelo más rápido de verificar un certificado es por medio del protocolo OCSP (Online Certifícate Status Protocol).

El servicio de respuesta en línea por el estado de un certificado, con o sin recibo electrónico, así como los costos de ellos deberá ser acordado con las Autoridades de Registro directamente

8.1 Efecto de validar al Suscriptor

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

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

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

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

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

8.2 Responsabilidad ante la no Verificación de una firma

Un usuario que confía en una firma 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 la *CPS Certinet.*

8.3 Confianza en la Firma Electrónica Avanzada

El usuario que confía en un mensaje o documento firmado electrónicamente por un suscriptor, puede confiar en la Firma Electrónica acorde a las prácticas definidas por Certinet si:

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

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

La decisión de confiar o no en una determinada firma electrónica avanzada, la toma en forma libre y exclusiva quien realiza la verificación.

8.4 Almacenamiento de Antecedentes

Para efectos de disponer de los adecuados antecedentes para una verificación posterior de la firma electrónica, el Tercero que confía debe mantener los siguientes antecedentes:

- Texto que se Firmó.
- Firma Electrónica.
- Certificado del Firmante o en su defecto alguna identificación que permita buscar posteriormente el certificado en los repositorios de Certinet.
- Registro o marca de fecha y hora de creación de la firma digital, o en su defecto fecha y hora dentro del documento firmado.

Idealmente estos datos deben ser guardados en una estructura de información orientada a validar firmas, tal como la estructura de PKCS#7, XMLDSig, ETSI PDF.