Prestador de Servicios de Certificación

THOMAS SIGNE
Soluciones Tecnológicas Globales

PO01Política de Certificados Firma Electrónica Avanzada de Persona Natural

Información del documento

Nombre	PO01 POLÍTICA DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA DE PERSONA NATURAL
Realizado por	THOMAS SIGNE
País	CHILE
Versión	1.4
Fecha	FEBRERO DE 2023
Tipo de Documento	PÚBLICO
Código	THS-CL-AC-PC-PER-01

Historial de versiones

Versión	**Fecha**	**Descripción**
1.0	02/02/2019	Elaboración de documento inicial.
1.1	21/04/2020	Se agrega emisión y custodia de certificados en HSM Centralizado. Se cambia el nombre de documento.
1.3	10/09/2021	Se cambia el formato mas no el contenido a recomendación de RFC 3674, Cambio en Imagen de Título
1.4	14/02/2023	Se incluye la función de revocación al rol del OV Ajuste del indice con el resto de PC. Eliminando Vista General Ajustes del procedimiento de emisión en Token y HSM. Ajustes del procedimiento de validación de identidad ante notario. Ajustes del procedimiento de revocación. Ajustes de la suspensión de certificados. Canales de venta y atención cliente Política de reembolso Dispositivos Token admitidos.

ÍNDICE

1 INTRODUCCIÓN

1.1 PRESENTACIÓN DEL DOCUMENTO

Este documento constituye la Política de Certificados (PC) de FEA Persona Natural emitidos por Thomas Signe S.A., conforme a la legislación chilena y las disposiciones de los entes reguladores.

Los Certificados de FEA Persona Natural emitidos por Thomas Signe, son certificados que permiten identificar y firmar al Titular como una persona natural.

Esta PC establece los requisitos particulares de los Certificados de Persona Natural emitidos por Thomas Signe, siguiendo el estándar RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", y conforme a los siguientes estándares:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

- ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

- ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates. Actualizado por ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

- ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

Adicionalmente a los requisitos particulares establecidos en esta PC, los Certificados de Persona Natural emitidos por Thomas Signe, se rigen por las prácticas establecidas en la Declaración de Prácticas de Certificación (DPC) para la emisión de certificados de Thomas Signe, esta DPC se encuentra publicada en la misma página web de Thomas Signe que el presente documento.

El presente documento es de carácter público y se encuentra dirigido a todas las personas naturales y jurídicas, Solicitantes, Titulares, Terceros que confían y público en general.

En el caso de que se detecten vulnerabilidades o se pierda la vigencia de los estándares técnicos o infraestructura indicados en la presente PC, Thomas Signe se encargará de informar de tal hecho a ENTIDAD ACREDITADORA, para proceder con la respectiva actualización.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Los datos de identificación del presente documento están especificados en la tabla inicial *Identificación del documento*.

Adicionalmente, el presente documento se identifica con el siguiente OID, contenido en la extensión X.509 v3 Certificate Policies de los Certificados de Persona Natural emitidos por Thomas Signe S.A. en los tipos de soporte indicados.

OID DE LA PC DE CERTICADOS FEA DE PERSONA NATURAL DE THOMAS SIGNE S.A.	
1.3.6.1.4.1.51362.0.4.1.1	Políticas de Certificados

Este documento se encuentra publicado en la siguiente página web:

https://www.thomas-signe.cl/ppc

1.3 PARTICIPANTES PKI DE THOMAS SIGNE S.A.

1.3.1 JERARQUÍA DE CERTIFICADOS DE LA PKI DE THOMAS SIGNE.

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe.

1.3.2 THOMAS SIGNE ROOT

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe.

1.3.3 PSC THOMAS SIGNE

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe.

1.3.4 SOLICITANTE

En esta PC, Solicitante es la persona natural que solicita a la PSC Thomas Signe S.A. la emisión de un Certificado FEA de Persona Natural.

En esta PC, Solicitante es siempre la misma persona natural que el Titular.

1.3.5 TITULAR

En esta PC, Titular es la persona natural a cuyo nombre la PSC Thomas Signe expide un Certificado de FEA Persona Natural y, por tanto, actúa como responsable del mismo, y que, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta PC y en la DPC para la emisión de certificados de Thomas Signe y habiendo aceptado el respectivo Contrato de Suscripción con Thomas Signe, acepta las condiciones del servicio de emisión de certificados prestado por éste.

El Titular es el responsable del uso de la clave privada asociada al Certificado de Persona Natural expedido a su nombre por la PSC Thomas Signe, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando dicha clave privada.

En esta PC, Titular es una persona natural sin vinculación a ninguna Corporación o Entidad.

1.3.6 TERCERO QUE CONFÍA

En esta PC, Tercero que confía (o Tercero aceptante) son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en un Certificado FEA de Persona Natural emitido por la PSC Thomas Signe.

1.4 TIPOS DE SOPORTE Y USOS DE CERTIFICADOS

1.4.1 SOPORTE

Las claves privadas de los Certificados de Persona Natural de Thomas Signe son generadas en soporte hardware. Estos certificados hacen uso de un dispositivo de creación de firma seguro como un token, una tarjeta o un HSM Centralizado, los cuales cuenta con certificación FIPS 140-2 nivel 3, dando lugar a un nivel de aseguramiento alto, para proteger las claves privadas frente a riesgos como:

- Ataques de código malicioso

- Exportación no autorizada de claves

- Suplantación de identidad por descuido del Titular en la custodia de dispositivos criptográficos

El acceso a la clave privada de un Certificado FEA de Persona Natural, está protegido por una contraseña, definida por el Titular al generar las claves en el instante previo a la emisión del certificado.

En el caso que el Certificado se genere en token/tarjeta, únicamente se permite la instalación en dispositivos certificados con la norma FIPS 140-2 nivel 3. La generación del token requiere de la instalación del controlador, que es realizada por los sistemas de Thomas Signe. En caso de que el dispositivo no sea compatible con los controladores definidos, no se podrá realizar la instalación en dicho dispositivo.

En el caso de emisión de certificados en HSM Centralizado, el titular delega explícitamente la custodia de su certificado, en un HSM de Thomas-Signe el cual cuenta con todas las medidas de seguridad físicas y lógicas para garantizar que solo el titular podrá hacer uso de este. Para hacer uso de su certificado, el titular accede de forma segura, mediante la clave que el creo durante la emisión del certificado y un segundo factor de seguridad, que cumple con las pautas de identidad digital NIST 800-63-3.

Los Certificados FEA de Persona Natural están identificados mediante el OID (1.3.6.1.4.1.51362.0.4.1.1) en la extensión X.509 v3 Certificate Policies.

1.4.2 USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados de Persona Natural emitidos por Thomas Signe S.A. podrán usarse en los términos establecidos en la presente PC, en la DPC para la emisión de certificados FEA de Thomas Signe y en lo establecido en la legislación vigente al respecto.

Los Certificados FEA de Persona Natural pueden ser utilizados con los siguientes propósitos:

- Integridad del documento firmado.

- Identificación del Titular.

1.4.3 USOS NO AUTORIZADOS DE LOS CERTIFICADOS

No se permite la utilización distinta de lo establecido en esta PC y en la DPC para la emisión de certificados de Thomas Signe S.A.

1.5 ADMINISTRACIÓN DE LA DPC Y LAS PC

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

1.6 DEFINICIONES Y SIGLAS

1.6.1 DEFINICIONES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

1.6.2 SIGLAS

CA Certification Authority (Autoridad de Certificación)

CRL Certificate Revocation List (Lista de Certificados Revocados)

DN Distinguished Name (Nombre distinguido)

DPC Declaración de Practicas de Certificación

PSC Entidad de Certificación Digital que prestan servicios de certificación digital y equivale a una Entidad Certificadora definida en la ley 527 de 1999. También se debe entender como un Organismo de Evaluación de la Conformidad – OEC de acuerdo con lo definido en la ISO/IEC 17000.

ETSI European Telecommunications Standards Institute

FIPS Federal Information Processing Standards (FIPS, en español Estándares Federales de Procesamiento de la Información). Son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSA, IEEE, ISO, etc.).

IEC International Electrotechnical Commission

ISO International Organization for Standardization

ITU International Telecommunication Union

RUT Rol único Tributario

RUN Rol único Nacional

OCSP Online Certificate Status Protocol (Servicio del estado del certificado en línea)

ENTIDAD ACREDITADORA Organismo Público de Acreditación de CHILE

OR Operador de Registro

OV Operador de Validación

PC Política de Certificados

PKCS Public-Key Cryptography Standards. Estándares de criptografía de llave pública concebidos y publicados por los laboratorios de RSA.

PKI Public Key Infrastructure (Infraestructura de clave pública)

RA/AR Registration Authority (Autoridad de Registro)

RFC Request For Comments. Son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento del Internet y otras redes de computadoras, como protocolos, procedimientos, etc.

RSA Rivset, Shamir y Adleman. Es un sistema criptográfico de llave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

SAR Signe Autoridad de Registro

SHA Secure Hash Algorithm (Algoritmo de seguridad HASH)

2 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 NOMBRES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

3.2 VALIDACIÓN INICIAL DE LA IDENTIDAD

3.2.1 MÉTODO DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA

Cuando el certificado se emite en Token/Tarjeta, la clave privada es generada en el token/tarjeta en el instante previo a la emisión del certificado y a su instalación en el token/tarjeta.

Cuando el certificado se emite en HSM Centralizado, la clave privada se genera en el HSM en el instante previo a la emisión del certificado, mediante un procedimiento que garantiza su confidencialidad y su vinculación con el Solicitante.

Para el caso en que el certificado se encuentre custodiado en HSM Centralizado, los datos de creación de firma se encuentran protegidos mediante un segundo factor de seguridad que permita al titular control exclusivo del acceso y utilización de éstos.

3.2.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA CORPORACIÓN O ENTIDAD

No es aplicable a los certificados de Persona Natural.

3.2.3 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA NATURAL INDIVIDUAL

3.2.4 AUTENTICACIÓN PRESENCIAL DE IDENTIDAD

Si el Solicitante, se encuentra interesado en contratar los servicios de Thomas Signe, se coordinará una cita presencial. Una vez concretada la cita, Thomas Signe visitará o será visitado por el Solicitante para realizar la validación de la identidad, llevando a cabo las siguientes actividades:

- Validar presencialmente la identidad del Solicitante

- Tomar la firma y huella digital del Solicitante en el Contrato de Prestación de Servicios de Certificación de Firma Electrónica.

- Tomar una fotografía del Solicitante

- Ingresar las evidencias digitales al sistema SAR, para efectos de custodia y prueba de los actos de validación realizados.

Dicha validación podrá ser realizada por un Notario según formato de validación. Cabe destacar que, en este caso, todas estas evidencias serán recolectadas y custodiadas por Thomas Signe.

3.2.5 AUTENTICACIÓN DE IDENTIDAD POR NOTARIO

Si el Solicitante, se encuentra interesado en contratar los servicios de Thomas Signe, y no puede coordinar una cita presencial, puede realizar la validación de identidad ante Notario. Para realizar la validación de la identidad, deben realizarse las siguientes actividades:

- El notario debe validar presencialmente la identidad del Solicitante
- Tomar la firma y huella digital del Solicitante
- Fotocopia de la cédula de identidad
- Datos y firma del solicitante
- Datos y firma del notario

Instrucciones de envío: Si el documento notarial es firmado digitalmente debe ser enviado, junto con el formulario de solicitud y la fotocopia de la cedula de identidad del solicitante, al correo electrónico: certificados@thomas-signe.cl con copia al agente comercial asignado, de lo contrario debe ser enviado en original a nuestras oficinas en Av. Presidente Kennedy 5600, Of. 806, Vitacura

El operador debe ingresar las evidencias digitales al sistema SAR, para efectos de custodia y prueba de los actos de validación realizados.

3.2.6 AUTENTICACIÓN DE IDENTIDAD SEGÚN DECRETO 24/2019

En esta modalidad la verificación fehaciente de identidad del solicitante se realiza totalmente en línea, en completa adhesión a los lineamientos establecidos por el sistema de Clave Única y cumpliendo la normativa establecida por el decreto 24 Norma Técnica de Seguridad, Santiago, 22 de febrero de 2019. Para ello el solicitante de un certificado FEA, debe validar su identidad con su clave única, si la validación del solicitante por clave única es exitosa, se pasa al paso dos, que consiste en la autentificación del solicitante por medio de un mecanismo complementario de verificación fehaciente de identidad del solicitante, como lo exige la norma técnica referida.

El mecanismo complementario de verificación fehaciente de identidad utilizado por Thomas Signe, consiste en la obligación del solicitante de responder satisfactoriamente un cuestionario de desafío de preguntas y respuestas, realizadas al azar, de hechos de su vida. Estas respuestas son evaluadas por un Buró (actualmente Equifax), si y solo si, el solicitante responde correctamente el conjunto de preguntas de este mecanismo complementario, Thomas Signe considerara que se ha efectuado una verificación fehaciente de la identidad del solicitante equivalente a la verificación presencial de la identidad.

En caso de cambiar el mecanismo complementario de verificación fehaciente de identidad, ello será, previa evaluación y autorización de la Entidad Acreditadora y publicación en esta Declaración de Practicas de Certificación.

Detalles del proceso de verificación fehaciente de identidad del solicitante con clave única y con el mecanismo complementario se encuentran disponibles en el documento THS-CL-AC-PR-09 Proceso de Compra de FEA Online publicado en el enlace Prácticas y Políticas.

3.2.7 INFORMACIÓN DE TITULAR Y SOLICITANTE NO VERIFICADA

Bajo ninguna circunstancia la AR omitirá las labores de verificación de información que conduzcan a la identificación del Titular y Solicitante según lo especificado en las secciones 3.2.2 y 3.2.3.

La AR no verificará los siguientes datos del Titular y Solicitante ingresados en el formulario de solicitud del certificado en la plataforma SAR, presumiendo la buena fe de la información aportada por el Titular:

- Correo electrónico del Titular (contenido en el certificado. Entregado por solicitante).

- Celular del Titular (no contenido en el certificado).

3.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN CON CAMBIO DE CLAVES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

3.4 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

El Titular que desee revocar su certificado digital, podrá comunicarse con el Responsable de certificados de la PSC Thomas Signe, enviando la solicitud de revocación a la dirección de correo electrónico certificados@thomas-signe.cl, la cual será derivada a un Operador de Validación. Cabe destacar que la solicitud de revocación tendrá que ser enviada desde la respectiva dirección de correo electrónico declarada en el formulario de solicitud para la emisión del certificado

4 REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 SOLICITUD DE CERTIFICADOS

4.1.1 QUIÉN PUEDE SOLICITAR UN CERTIFICADO

Sólo puede solicitar un Certificado de Persona Natural el propio Titular.

Para los certificados emitidos en token, es necesario disponer o solicitar a Thomas Signe un token del modelo SafeNet eToken 5110 para garantizar que se emite en un dispositivo FIPS 140-2 level 3.

4.1.2 COMERCIALIZACIÓN

El Solicitante (y Titular) podrá recibir información acerca del proceso de certificación digital de las siguientes maneras:

- Consultando la página web https://www.thomas-signe.cl

- Mediante correo electrónico informativo desde la dirección comercial@thomas-signe.cl

- El trato directo con Agentes comerciales.

Por cualquiera de estos medios, se le brindará información acerca de dicho proceso, requisitos necesarios, tarifas u otros relativos.

Los canales de venta de los certificados emitidos por Thomas Signe son los siguientes:

- En la página web de Thomas Signe, se puede realizar una solicitud online siguiendo los pasos de la contratación online.
- Mediante una solicitud al correo electrónico comercial@thomas-signe.cl.
- Trato directo con Agentes comerciales.
- Disponemos de una opción de integración a través de API para la solicitud de emisión de certificados. Para más información consultar con los agentes comerciales en los medios de contacto indicados anteriormente.

Luego de ser informado, el Solicitante (y Titular) indicará al Área Comercial y/o a un OR:

1) El tipo de certificado requerido (Certificado de Persona Natural).

2) La vigencia del certificado requerida.

3) El nombre completo del Solicitante.

4) El tipo y el número del documento de identidad del Solicitante.

5) La cuenta de correo electrónico personal del Solicitante que estará asociada al certificado digital y por medio de la cual la PSC le realizará notificaciones y comunicaciones oficiales.

El Área Comercial y/o un OR enviarán por correo electrónico al Solicitante (y Titular): la Propuesta Comercial, en los casos que sea aplicable; el Contrato de Suscripción; opcionalmente, un enlace a la plataforma SAR; y las indicaciones respectivas.

4.1.3 CONTRATACIÓN Y PAGO

Para proceder, el Solicitante (y Titular) deberá:

- Realizar el pago de la tarifa respectiva por un método válido, en los casos que sea aplicable. La evidencia de este proceso será el voucher o comprobante de pago.

  Thomas Signe S.A. pone a disposición del público una cuenta bancaria para realizar el depósito de la cuantía respectiva a cada servicio. En la Propuesta Comercial se indicarán los datos de esta cuenta bancaria. No obstante, Thomas Signe S.A. puede precisar un método alternativo de pago en el caso de un Contrato de Prestación de Servicios.

- Aprobar todos los términos y condiciones dispuestos en el Contrato entre Thomas Signe. y el Titular, mediante la firma respectiva. La evidencia de este proceso será el Contrato de Suscripción firmado.

4.1.4 SOLICITUD

Para solicitar la emisión propiamente dicha de un certificado digital, Thomas Signe completará los datos del Solicitante se de forma manual o automática dentro de la plataforma de registro. Además, procederá a adjuntar las evidencias solicitadas indicadas:

- Documento de identidad del Solicitante.
- Constancia del pago de la tarifa del certificado indicada en la Propuesta Comercial, en los casos que sea aplicable.
- Contrato de Suscripción aceptado.
- Contrato de Prestación de Servicios aceptado

Alternativamente, el Solicitante podrá entregar personalmente o enviar los datos y los documentos requeridos al Área Comercial y/o a un OR, y éstos ingresarán los datos en el formulario de la solicitud de certificado y adjuntarán los documentos solicitados en la plataforma SAR.

4.2 TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

4.2.1 REVISIÓN

Thomas Signe verificará que todos los documentos requeridos hayan sido adjuntados en la plataforma SAR y que todos ellos cumplen lo siguiente:

- Están completos y son legibles.

- Son aparentemente legítimos.

- En los casos que sea aplicable, estaban vigentes cuando se adjuntaron en la plataforma SAR.

- Los datos que contienen relativos al Titular, al tipo y a la vigencia del certificado, y al pago de la tarifa del certificado son conformes a los correspondientes datos ingresados en el formulario de solicitud de certificado y, en los casos que sea aplicable, en la Propuesta Comercial.

Si hace falta regularizar pagos o documentación, se notificará lo requerido a la dirección de correo electrónico declarada por el Solicitante.

El OR verificara la identidad del Solicitante, mediante la revisión de la documentación que la ha sido entregada, que deberá haber ingresado en la plataforma SAR en formato digital y, además, deberá archivar y conservar en formato papel los documentos originales recibidos en dicho formato (no escaneados).

Una vez que el OV ha validado los documentos presentados y los datos ingresados en el formulario de solicitud de certificado y que ha verificado su identidad, el OV aprobará la solicitud de emisión en la plataforma de la RA.

Si la información o verificación de identidad no fuese correcta, Thomas Signe deberá denegar la petición, contactando al Solicitante para comunicarle el motivo.

Para el caso de verificación de identidad con plataforma Clave Única, las evidencias y revisiones son realizadas en forma automática por los sistemas informáticos de THSC, en apego al decreto 24[1].

La evidencia que genera Clave Única, los mecanismos complementarios de validación de identidad y aceptación de los términos y condiciones del servicio, realizados por el solicitante en la plataforma de venta de certificados en línea, constituyen la evidencia del proceso y son almacenados digitalmente.

4.2.2 DECISIÓN

La PSC Thomas Signe S.A. es responsable de la decisión tomada con respecto a la certificación digital. Es decir, es responsable de aprobar o denegar la certificación digital. En el caso de denegación, la PSC se encarga de comunicar el motivo del rechazo al Solicitante.

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 ACCIONES DE LA PSC DURANTE LA EMISIÓN DE CERTIFICADOS

Una vez aprobada la solicitud, se procederá a la emisión del certificado, durante la cual la PSC Thomas Signe realiza las siguientes acciones:

1) Las claves serán generadas por el Titular en el HSM centralizado o en el Token/Tarjeta, haciendo entrega a la RA de una petición de certificado en formato PKCS#10 o equivalente.

2) La RA firmará la petición de certificado recibida en formato PKCS#10 o equivalente y los datos que estarán contenidos en el certificado que han sido ingresados en la plataforma SAR, y enviará la petición resultante a la CA, recibiendo de ésta el correspondiente certificado emitido.

- En caso HSM centralizado con Clave Única, este proceso será realizado automáticamente al recibir la RA la petición de certificado en formato PKSC#10 o equivalente, sin intervención de un OR.

---

[1] NORMA TÉCNICA PARA LA PRESTACIÓN DEL SERVICIO DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA Núm. 24.- Santiago, 22 de febrero de 2019

3) Finalmente, la RA realizará la entrega del certificado.

- En el caso de que el tipo de soporte sea HSM Centralizado, el certificado es instalado automáticamente en el HSM Centralizado asociado a las claves generadas en éste por el Titular.

- En el caso de que el tipo de soporte sea Token/Tarjeta, el certificado es instalado en el Token asociado a las claves generadas por el titular.

4.3.2 EMISIÓN DE CERTIFICADOS EN TOKEN

Para los certificados emitidos en token, es necesario disponer o solicitar a Thomas Signe un token del modelo SafeNet eToken 5110 para garantizar que se emite en un dispositivo FIPS 140-2 level 3.

El procedimiento de emisión de certificados en token admite exclusivamente los drivers específicos del modelo indicado anteriormente.

4.3.3 EMISIÓN DE CERTIFICADOS EN HSM

Para los certificados emitidos en HSM, exclusivamente se emiten en los dispositivos criptográficos puestos a disposición y gestionados por Thomas Signe.

4.3.4 NOTIFICACIÓN AL SOLICITANTE POR LA PSC DE LA EMISIÓN DEL CERTIFICADO

Se notificará por correo al Solicitante que su solicitud ha sido aceptada, este correo contendrá un enlace y las instrucciones para que el Titular, genere sus claves y descargue el certificado

Además, la RA envía un correo electrónico al Solicitante (y Titular) que incluye información sobre el contenido del certificado, la página web donde se encuentran publicadas la DPC y PC, así como manuales para el uso del certificado.

4.4 ACEPTACIÓN DEL CERTIFICADO

4.4.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

El certificado se considerará aceptado por el Titular, una vez que la RA ha realizado su entrega y la PSC ha notificado la misma al Solicitante, según lo especificado en las secciones 4.3.1 y 4.3.2.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA PSC

La PSC Thomas Signe S.A. no publica los certificados emitidos en ningún repositorio.

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR LA PSC A OTRAS ENTIDADES

La PSC Thomas Signe S.A. no notifica la emisión de certificados a terceros.

4.5 USOS DE LAS CLAVES Y EL CERTIFICADO

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

4.6 RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

4.7 RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

4.8 MODIFICACIÓN DE CERTIFICADOS

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

El Titular deberá solicitar la revocación de su certificado en caso de pérdida, riesgos y compromisos de seguridad de claves contenidas en el dispositivo criptográfico u otras causas especificadas en la DPC para la emisión de certificados de Thomas Signe S.A.

Para solicitar la revocación del certificado el Titular:

- Revocar el certificado a través del servicio de revocación online utilizando los enlaces contenidos en el correo que recibió con las instrucciones de creación de claves o en el siguiente enlace.

- El Titular que desee revocar su certificado digital, podrá comunicarse con el Responsable de certificados de la PSC Thomas Signe S.A. enviando la solicitud de revocación a la dirección de correo electrónico certificados@thomas-signe.cl, la cual será derivada a un Operador de Validación. Cabe destacar que la solicitud de revocación tendrá que ser enviada desde la respectiva dirección de correo electrónico declarada en el formulario de solicitud para la emisión del certificado.

En la DPC para la emisión de certificados de Thomas Signe S.A. se encuentra toda la información complementaria referente a la revocación y suspensión de los certificados

4.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

Un certificado podrá ser revocado debido a las siguientes circunstancias:

a) Circunstancias que afectan a la información contenida en el certificado:
   - Modificación de alguno de los datos contenidos en el certificado.
   - Confirmación de que alguna información o hecho contenido en el certificado digital es falso.
   - Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   - Pérdida o cambio del Suscriptor de la vinculación con la Corporación, en el caso de Certificados Corporativos.
   - Liquidación de la persona jurídica representada que consta en el certificado digital.

b) Circunstancias que afectan a la seguridad de la clave privada o del certificado:
   - Compromiso de la clave privada o de la infraestructura o sistemas de Thomas Signe, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
   - Infracción, por parte de Thomas Signe, relativa a los requisitos previstos en los procedimientos de gestión de certificados establecidos en la DPC.
   - Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del Titular.
   - Acceso o utilización no autorizados, por un tercero, de la clave privada del Titular.
   - El incumplimiento por parte del Titular de las normas de uso del certificado expuestas en la presente DPC o en el instrumento jurídico vinculante entre Thomas Signe y el Titular.
   - El incumplimiento del Contrato de Prestación de Servicios de Firma Electrónica Avanzada proporcionado por Thomas Signe.

c) Circunstancias que afectan a la seguridad del dispositivo criptográfico:
   - Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
   - Pérdida o inutilización por daños del dispositivo criptográfico.
   - Acceso no autorizado, por un tercero, a los datos de activación del Titular.
   - Manejo indebido por parte del titular del certificado digital.
   - El incumplimiento por parte del Titular de las normas de uso del dispositivo criptográfico expuestas en la presente DPC o en el Contrato de Prestación de Servicios de Firma Electrónica Avanzada.

d) Circunstancias que afectan al Titular:
- Finalización de la relación jurídica entre Thomas Signe y el Titular.
- Terminación del Contrato de Prestación de Servicios de Firma Electrónica Avanzada, de conformidad con las causales establecidas en dicho contrato.
- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al Titular.
- Oposición o modificación, por parte del Firmante, de los datos contenidos en el fichero de datos de carácter personal de Thomas Signe.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
- Infracción por el Titular, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en las condiciones generales de contratación.
- La incapacidad sobrevenida, total o parcial por el fallecimiento del Titular.

e) Otras circunstancias:
- Por pérdida, inutilización del certificado digital que haya sido informado a Thomas Signe.
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la DPC.
- Por cualquier causa que induzca a creer razonablemente que el servicio de certificación haya sido comprometido, poniendo en duda la confiabilidad del certificado digital.

4.9.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

Pueden solicitar la revocación de un certificado:

a) El propio Titular, que deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.
b) Cualquier persona podrá solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

Podrán tramitar la revocación del certificado:

- Los operadores autorizados por Thomas Signe de acuerdo con la Política de certificación correspondiente.).

4.9.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

Existen varias alternativas a la hora de solicitar la revocación del certificado.

En todo caso, en el momento de revocarse el certificado, se enviará un comunicado al Titular, comunicando la hora y la causa de la misma.

Procedimiento online

Thomas Signe S.A. brinda el servicio de revocación online a través de los enlaces contenidos en el correo que recibió con las instrucciones de creación de claves o en el siguiente enlace.

Debe seguir las instrucciones de la web de revocación. Debe proporcionar correctamente los datos que le identifiquen o disponer del código de revocación proporcionado durante el proceso de generación de su certificado digital junto con su documento de identidad. Una vez aceptada la tramitación, el certificado será inmediatamente revocado.

Mediante Correo electrónico

De forma alternativa, se podrá solicitar la revocación de un certificado mediante comunicación enviando correo a la dirección de correo electrónico **certificados@thomas-signe.cl**, la cual será derivada a un Operador de Registro/Validación.

Cabe destacar que la solicitud de revocación tendrá que ser enviada desde la cuenta de correo electrónico declarada en el Formulario de solicitud respectivo (revocación solicitada por el Titular o Solicitante) o, en otro caso, el Operador de Validación deberá verificar la causa de revocación comunicada y que ésta se corresponde con alguna de las circunstancias anteriormente indicadas.

Revocación telefónica

Para cualquier perfil de certificado, podrá solicitar la revocación de un certificado telefónicamente, en horario de oficina (8.30 a 17.00h) contactando con el número de teléfono (+56) 2 3259 7821. El suscriptor deberá identificar y autenticar su identidad mediante los procedimientos que Thomas Signe considere oportunos.

Una vez realizado el proceso de identificación de manera correcta, un operador de la Entidad de Registro procederá a efectuar la revocación.

4.9.4 PLAZO EN EL QUE EL PSC DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

Una vez la identidad del Titular haya sido autenticada según lo expuesto anteriormente, y la revocación debidamente tramitada por la AR, la revocación se hará efectiva inmediatamente.

4.9.5 OBLIGACIÓN DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

4.9.6 FRECUENCIA DE EMISIÓN DE LAS CRLS

La CRL de Thomas Signe Root (CA Raíz) se emite antes de que hayan transcurrido 180 días desde la emisión de la anterior CRL (antes de su fin de validez) o cuando se produzca una revocación.

La CRL del PSC Thomas Signe CHILE (CA Subordinada) se emite al menos cada 4 días (antes del fin de validez de la anterior CRL); en condiciones normales, la CRL se emite cada 24 horas o cuando se produzca una revocación.

4.9.7 TIEMPO MÁXIMO ENTRE LA GENERACIÓN Y LA PUBLICACIÓN DE LAS CRLS

Una vez emitida la CRL de Thomas Signe Root (CA Raíz), ésta se publica al menos antes del fin de validez de la anterior CRL (180 días después de su emisión); en condiciones normales, la CRL se publica el mismo día de su emisión.

Una vez emitida la CRL del PSC Thomas Signe CHILE (CA Subordinada), ésta se publica al menos antes del fin de validez de la anterior CRL (4 días después de su emisión); en condiciones normales, la CRL se publica en el momento de la generación de la misma, por lo que se considera cero o nulo el tiempo transcurrido.

4.9.8 DISPONIBILIDAD DEL SISTEMA EN LÍNEA DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control del PSC, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

4.9.9 REQUISITOS DE COMPROBACIÓN DE REVOCACIÓN EN LÍNEA

Para el uso del servicio de CRLs, de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión CRL Distribution Points.

- Se deberá comprobar adicionalmente la(s) CRL(s) pertinentes de la cadena de certificación de la jerarquía.
- Se deberá comprobar que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.
- Los certificados revocados que expiren podrán ser retirados de la CRL.

También se puede comprobar la revocación en línea por medio del servicio OCSP, de libre acceso, en la dirección URL contenida en el propio certificado en la extensión Authority Information Access.

4.9.10 CIRCUNSTANCIAS PARA LA SUSPENSIÓN

Thomas Signe podrá suspender un certificado en los casos siguientes:

- Si se sospecha el compromiso de una clave, hasta que este hecho sea confirmado o desmentido.
- Si el suscriptor ha incurrido en falta de pago de su certificado
- Si no disponen de toda la información necesaria para determinar la revocación de un certificado.

4.9.11 QUIEN PUEDE SOLICITAR LA SUSPENSIÓN

Solamente podrán realizar la suspensión del certificado:

- Los operadores de la RA del suscriptor del certificado
- Los operadores autorizados de la CA.

4.9.12 PROCEDIMIENTO DE SOLICITUD DE SUSPENSIÓN

Existen varias alternativas para el suscriptor o el firmante a la hora de solicitar la suspensión del certificado. Ver punto 4.9.3.

4.9.13 LÍMITES DEL PERIODO DE SUSPENSIÓN

Al cabo de 15 días de suspensión, la CA podrá proceder a la revocación del certificado.

4.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

4.11 FINALIZACIÓN DE LA SUSCRIPCIÓN

La suscripción del certificado finalizará en el momento de expiración o revocación del certificado.

4.12 CUSTODIA Y RECUPERACIÓN DE CLAVES (KEY ESCROW AND RECOVERY)

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

4.13 ATENCIÓN AL CLIENTE

Para cumplimiento de la ley 19.496 de Derechos de los Consumidores, cualquier petición, queja, reclamo o solicitud se debe comunicar a Thomas Signe S.A. por medio de los canales relacionados a continuación detallando la situación por la que se presenta.

Los canales de atención al cliente son los siguientes:

- Escribiendo a los siguientes correos electrónicos:
  - Prestador de Servicios de Confianza: psc-cl@thsigne.com
  - Comercial: comercial@thomas-signe.cl

- Soporte: soporte.cl@thsigne.com

❖ En la sección de "Contacta" de la Página Web: www.thomas-signe.cl
❖ En las oficinas de Thomas Signe en horario de oficina en la dirección:
Avenida Presidente Kennedy 5600, Oficina 806, Comuna Vitacura, Santiago de Chile
❖ En el teléfono +56 2 32597822, en horario de oficina

En el caso de que el usuario comunique una petición, queja o reclamo por medios diferentes a correo electrónico de soporte, se informará al usuario de que debe enviar dicha solicitud a la dirección de correo soporte.cl@thsigne.com con el detalle de la solicitud.

Toda petición, queja, reclamo o sugerencia recibida producirá un registro en la aplicación de ticketing y una respuesta inmediata al usuario, indicando que su solicitud se encuentra en proceso de evaluación y que cuando se tenga la solución se le comunicará la respuesta de la misma.

Las solicitudes enviadas a la dirección de correo soporte.cl@thsigne.com se registrarán de forma automática en la herramienta de ticketing y su tratamiento será gestionado por el equipo de soporte. La información registrada para cada solicitud será:

- Fecha de apertura: DD/MM/AAAA (hora de Chile)
- SLAs:
  - Tiempo hasta primera respuesta: está asociado un periodo de 48 horas para responder automáticamente al usuario sobre la recepción de la petición correspondiente.
  - Tiempo hasta resolución: está asociado un periodo planificado para resolución (establecido en máx 15 días).
- Tipo: clasificar según la tipología:
  - Petición
  - Queja
  - Reclamo
  - Solicitud
- Reporter: persona que registra la petición
- Asignee: persona encargada del tratamiento y control de la petición
- Estado: campo para indicar el estado de la petición a lo largo de su tratamiento.
- Prioridad: la prioridad dependerá del tipo de petición y se clasificará según lo indicado en la siguiente tabla.

Tipo de petición	Prioridad
Petición	Media (Medium)
Queja	Alto (High)
Reclamo	Muy Alto (Highest)
Solicitud	Media (Medium)

- Título: se copiará el asunto del correo del usuario
- Descripción: en este campo se copiará el cuerpo de la comunicación del usuario.

En la herramienta de ticketing se podrán registrar los seguimientos necesarios y la solución/validación final dada a las peticiones.

En caso de que el detalle de la información de la petición no sea claro, el equipo de soporte se comunicará con el usuario mediante el correo electrónico de origen de la solicitud a fin de obtener una mayor precisión.

Con la información recibida, el área afectada procede a analizar si la petición es procedente y decidir las acciones de subsanación y/o compensaciones correspondientes. Nunca se encargará la investigación a personas con responsabilidad directa sobre las actividades reclamadas.

Los resultados de la investigación, así como las decisiones tomadas se incorporan a los registros correspondientes y serán analizados en las Revisiones por la Dirección del Sistema de Gestión.

Una vez finalizados los procesos internos, se procede a elaborar una respuesta al usuario que incluya la resolución tomada (motivada adecuadamente) y comunique las medidas a tomar. Esta respuesta se remitirá al usuario. Si este se da por satisfecho, se procede a cerrar la petición correspondiente. En caso contrario se vuelve a tratar como si fuese un nuevo caso.

El plazo máximo para la resolución de la solicitud es de quince (15) días calendario, luego de haber sido recibida.

Este periodo puede cambiar para el caso de consultas y reclamos relacionados con la protección de datos personales para adaptarse a la legislación vigente.

Adicionalmente a la tramitación de comunicaciones del usuario que transmiten alguna insatisfacción con los servicios brindados, todas las peticiones de información y preguntas de los usuarios serán debidamente respondidas, por parte del equipo de soporte, y registradas en la herramienta de ticketing como petición.

Se podrán usar herramientas de videollamada exclusivamente para el soporte de usuarios finales para los servicios que brinda Thomas Signe.

4.14 POLÍTICA DE REEMBOLSO

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

5 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

6 CONTROLES TÉCNICOS DE SEGURIDAD

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

7 PERFIL DE CERTIFICADO, CRL Y OCSP

7.1 PERFIL DE CERTIFICADO

7.1.1 FORMATO Y PERIODO DE VALIDEZ DEL CERTIFICADO

El formato de los certificados de Persona Natural cumple lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A., excepto que para estos certificados no es aplicable el estándar ETSI EN 319 412-3.

Los Certificados de Persona Natural tienen un periodo de validez de hasta 3 años (1095 días).

7.1.2 EXTENSIONES DEL CERTIFICADO

En la tabla siguiente se especifican las extensiones de los Certificados de Persona Natural.

Extensión	Crítica	Valor
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA Subordinada, obtenido a partir del hash SHA-1 de la misma
Subject Key Identifier	-	Identificador de la clave pública del certificado, obtenido a partir del hash SHA-1 de la misma
Key Usage	Sí	digitalSignature nonRepudiation
Certificate Policies	-	OID 1.3.6.1.4.1.51362.0.4.1.1 URI de la DPC: http://thomas-signe.cl/ppc
Subject Alternative Name		rfc822Name: *correo electrónico del Titular*
Basic Constraints	Sí	CA: FALSE
Extended Key Usage	-	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
CRL Distribution Points	-	URI de la CRL: http://crl-cl.thsigne.com/acfea_thomas_signe_chile.crl
Authority Information Access	-	URI del certificado de la CA Subordinada: http://thsigne.com/certs/acfea_thomas_signe_chile.crt URI del servicio OCSP de la CA Subordinada: http://ocsp-cl.thsigne.com/

7.1.3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

7.1.4 FORMATOS DE NOMBRES

En la tabla siguiente se especifican los correspondientes atributos del DN del titular de un Certificado de Persona Natural (Titular del certificado).

Atributo del DN	Descripción	Valor
Country Name (C)	País	*Código de dos letras mayúsculas según ISO 3166-1 del país donde reside el Titular* [1] Por defecto: CL
Serial Number (serialNumber)	*Número de Serie*	*RUN del titular*[2]
Surname (SN)	Apellidos	*Apellidos del titular*[2]
Given Name (givenName)	Nombre de Pila	*Nombre del Titular* [2]
Common Name (CN)	Nombre	*Nombre completo del titular*[2]

7.1.5 RESTRICCIONES DE LOS NOMBRES

Según lo especificado en la sección 7.1.4 y en la DPC para la emisión de certificados de Thomas Signe S.A.

7.1.6 IDENTIFICADORES DE OBJETO (OID) DE LAS POLÍTICAS DE CERTIFICADOS

Los OID de la Política de Certificados de Persona Natural se encuentran especificados en las secciones 1.3, 1.5.1 y 7.1.2, así como en la DPC para la emisión de certificados de Thomas Signe S.A.

7.1.7 USO DE LA EXTENSIÓN POLICY CONSTRAINTS

Los Certificados de Persona Natural no contienen la extensión Policy Contraints.

7.1.8 SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

---

[1] Codificado en PrintableString

[2] Codificado en UTF8String

7.1.9 TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICY

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

7.2 PERFIL DE CRL

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

7.3 PERFIL OCSP

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

8 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9 OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

9.1.1 TARIFAS DE EMISIÓN DE CERTIFICADOS

Las tarifas están indicadas en la página de venta de certificados en línea y pueden variar de acuerdo al tipo de certificado y al contrato establecido con cada cliente, lo cual quedará indicado en la propuesta comercial que indicará el precio final con IVA para el certificado solicitado.

9.1.2 TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso a la consulta del estado de los certificados emitidos, es libre y gratuito.

9.1.3 TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

No se establece ninguna tarifa para la revocación de certificados, ni para el acceso a la información de estado de los certificados.

9.1.4 TARIFAS DE OTROS SERVICIOS

Las tarifas aplicables a otros posibles servicios se negociarán entre Thomas Signe S.A. y los clientes de los servicios ofrecidos.

9.1.5 POLÍTICA DE REEMBOLSO

La PSC Thomas Signe S.A. sigue las disposiciones legales chilenas en lo referente a políticas de reembolso.

9.2 RESPONSABILIDADES FINANCIERAS

9.2.1 COBERTURA DEL SEGURO

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.4 POLÍTICA DE PROTECCIÓN DE DATOS

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.6 OBLIGACIONES

9.6.1 OBLIGACIONES DE LA PSC

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.6.2 OBLIGACIONES DE LOS PROVEEDORES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.6.3 OBLIGACIONES DE LOS SOLICITANTES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.6.4 OBLIGACIONES DE LOS TITULARES

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.6.5 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.7 RESPONSABILIDADES

9.7.1 RESPONSABILIDADES DE LA PSC

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.7.2 RESPONSABILIDADES DEL TITULAR

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.8 LIMITACIÓN DE RESPONSABILIDAD

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.9 PERIODO DE VALIDEZ

9.9.1 PLAZO

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.9.2 SUSTITUCIÓN Y DEROGACIÓN DE LA DPC Y LAS PC

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.10 CAMBIOS EN DPC Y PC

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.11 LEY APLICABLE

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.12 CONFORMIDAD CON LA LEY APLICABLE

Según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.

9.13 ESTIPULACIONES DIVERSAS

9.13.1 CLÁUSULA DE ACEPTACIÓN COMPLETA

Todos los Solicitantes, Titulares, Terceros que confían y cualquier otra parte interesada asumen en su totalidad el contenido de la última versión de esta PC y de la DPC asociada.

9.13.2 INDEPENDENCIA

En el caso de que cualquiera de los apartados recogidos en la presente PC o en la DPC asociada sea declarado, parcial o totalmente, nulo o ilegal no afectará tal circunstancia al resto del documento.

9.14 OTRAS ESTIPULACIONES

No se contemplan.