Autoridad de Certificación

THOMAS SIGNE

SOLUCIONES TECNOLÓGICAS GLOBALES

PO01

Política de Certificado de Firma Electrónica Avanzada de Pertenencia a Empresa

Información del documento

Nombre	PO01 POLÍTICA DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA DE PERTENENCIA A EMPRESA
Realizado por	THOMAS SIGNE
País	CHILE
Versión	1.2
Tipo de documento	PÚBLICO
Código	THS-CL-AC-PC-COR-02
Requisito	PO01

Historial de versiones

Versión	**Fecha**	**Descripción**
1.0	18/06/2019	Elaboración de documento inicial.
1.1	31/01/2020	Ajuste de la codificación según el procedimiento de control de la información documentada v2.3
1.2	21/04/2020	Se agrega emisión y custodia de certificados en HSM Centralizado. Se agrega la utilización de Clave Única Se cambia el nombre de documento

ÍNDICE

1 INTRODUCCIÓN

Thomas Signe es una empresa multinacional dedicada a desarrollar soluciones tecnológicas a la medida para garantizar el éxito de empresas tanto públicas como privadas; a través de una estrategia de creación de valor sustentada sobre una oferta de gestión global de las necesidades del cliente, desde la consultoría, pasando por el desarrollo de proyectos, la integración e implementación de soluciones.

Thomas Signe fue constituida en Chile en el año 2018 con el objetivo de convertirse en proveedor de servicios de firma electrónica, siendo acreditado y sometiéndose anualmente a las auditorías realizadas por el Ministerio de Economía. Para lo cual, Thomas Signe ha demostrado cumplir con todos los estándares operacionales, de seguridad, privacidad y calidad exigidos en los servicios de certificación brindados a sus clientes.

Como Proveedor de Servicios de Certificación - PSC, Thomas Signe provee servicios de emisión, distribución y revocación de certificados digitales. Además, brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas naturales como personas jurídicas.

2 OBJETIVO

Declarar el conjunto de reglas aplicadas a los Certificados de Pertenencia a Empresa emitidos por Thomas Signe S.A. en el marco del cumplimiento de los "Criterios Específicos de Acreditación establecidos por la "Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación" – EA-103 Versión 2.4 establecida por la Entidad Acreditadora, conforme a la legislación chilena y las disposiciones de los entes reguladores. Esta PC establece los requisitos particulares de los Certificados de Pertenencia a Empresa emitidos por Thomas Signe S.A, siguiendo el estándar RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

3 DEFINICIONES Y ABREVIACIONES

3.1 ACRÓNIMOS Y ABREVIACIONES

AR Autoridad de Registro

CRL Lista de Certificados Revocados

DPC Declaración de Prácticas de Certificación

FIPS Federal Information Standard (Estándares federales de procesamiento de la información)

HSM Módulo de Seguridad Hardware

OCSP Servicio del Estado del Certificado en Línea

PC Políticas de Certificación

PKI Infraestructura de la Clave Pública

PSC Prestador de Servicios de Certificación

SHA Secure Hash Algorithm (Algoritmo de seguridad HASH)

3.2 DEFINICIONES

Autoridad de Certificación – AC: pertenencia a Empresa pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Autoridad de Registro: persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Certificado Digital: mensaje de datos electrónico firmado por la Autoridad de Certificación, el cual identifica tanto a la Autoridad de Certificación que lo expide, como al titular y contiene la clave pública de este último.

Cliente: en los servicios de certificación digital, el término cliente identifica a la persona natural o jurídica con la cual la AC establece una relación comercial.

Clave Única: es un mecanismo de identificación digital que permite a los usuarios demostrar su identidad en plataformas digitales, ya que el Servicio de Registro Civil e Identificación verifica que la identidad digital corresponde a determinada persona, validándola contra su base de datos.

Declaración de Prácticas de Certificación: es el documento en el que consta de manera detallada los procedimientos que aplica el PSC para la prestación de sus servicios. Una declaración de las prácticas que un PSC emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.

Entidad Acreditadora: de acuerdo con la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, se establece en su artículo segundo, inciso "e", que la Entidad Acreditadora es la Subsecretaría de Economía, Fomento y Reconstrucción, actualmente denominada Subsecretaría de Economía y Empresas de Menor Tamaño.

Firma Digital: se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Función Hash o Hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

HSM: un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. La seguridad que proporcionan los dispositivos HSM de Thomas-Signe es muy elevada pues están sujetos a estrictas políticas de seguridad

Lista de Certificados Revocados: es aquella relación que debe incluir todos los certificados revocados por la Autoridad de Certificación.

OID: identificador único de objeto (Object identifier). OID. Acrónimo del término en idioma inglés "Object Identifier", que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado.

PKI: infraestructura de clave pública (Public key infraestructure): es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el titular del servicio y una pública, que se incluye en el certificado digital, logran: Identificar al emisor de un mensaje de datos electrónico, impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos, impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos y evitar que el titular del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío (no repudio).

Políticas de Certificado: es el conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.

Revocación: para este documento, es el proceso por el cual se inhabilita el certificado digital emitido y se da por terminado su periodo de validez de uso a partir de la fecha de revocación; al presentarse alguna de las causas establecidas en la DPC.

Segundo Factor Autenticación: la autenticación con dos factores es un método para confirmar que un titular de un certificado es quien dice ser; consiste en combinar dos elementos diferentes que son de conocimiento o propiedad del titular, uno algo que él sabe (ejemplo, una contraseña) y dos algo que él tiene (ejemplo, un teléfono, dispositivo de generación de códigos entre otros). Un ejemplo de un segundo factor lo vemos al realizar una trasferencia bancaria, donde se utiliza una tarjeta de coordenadas, un generador de números o se recibe un SMS, en todos estos casos, se tiene un conjunto de caracteres que se debe introducir para confirmar la transacción.

Servicio del Estado del Certificado en Línea OCSP: actividad de consulta en tiempo real al sistema de la AC, sobre el estado de un certificado digital a través del protocolo OCSP.

Servicio de Certificación Digital: conjunto de actividades de certificación que ofrece el PSC para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública (PKI).

Solicitante: persona natural o jurídica que, con el propósito de obtener servicios de certificación digital de una AC, demuestra el cumplimiento de los requisitos establecidos en la DPC y PC de estas, para acceder al servicio de certificación digital.

Titular: persona natural o jurídica a cuyo nombre se expide un certificado digital.

Tercero que confía: también llamado Tercero aceptante, es la persona natural o jurídica que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

4 PUBLICACIÓN DEL DOCUMENTO

La PC de Certificado de Pertenencia a Empresa, así como la DPC y otros documentos relacionados al servicio de certificación digital, se encuentran publicados en la página web de Thomas Signe Chile SA: www.thomas-signe.cl

5 CARACTERÍSTICAS DE CERTIFICADOS

5.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los certificados de Pertenencia a Empresa emitidos por Thomas Signe tienen una vigencia máxima de tres (03) años.

5.2 TIPOS DE SOPORTE

Las claves privadas de los Certificados de Pertenencia a Empresa de Thomas Signe pueden ser 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.

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 autentificación, que cumple con las pautas de identidad digital NIST 800-63-3.

5.3 USO PARTICULAR DE LOS CERTIFICADOS DE PERTENENCIA A EMPRESA

5.3.1 USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados de Pertenencia a Empresa, emitidos por Thomas Signe Chile SA, podrán usarse en los términos establecidos por la PC, DPC y lo establecido en la legislación vigente al respecto.

Los certificados de Pertenencia a Empresa deben ser, en general, utilizados dentro del marco de la relación jurídica de servicio entre el empleado y la empresa. En concreto, pueden ser utilizados con los siguientes propósitos:

- Integridad del documento firmado.
- No repudio de origen.
- Identificación del Titular y su vinculación con la empresa.

Se permite el uso de estos certificados en las relaciones personales del Titular con las Entidades Públicas y Privadas, y en otros usos estrictamente personales siempre y cuando no exista una prohibición de la empresa.

5.3.2 USOS NO AUTORIZADOS DE LOS CERTIFICADOS

No se permite la utilización distinta de lo establecido en esta Política y en la Declaración de Prácticas de Certificación de Thomas Signe Chile SA. Tampoco se recomienda su uso para el cifrado de documentos.

5.4 TARIFAS

Las tarifas de los certificados de Pertenencia a Empresa y sus métodos de pago pueden ser consultados al correo electrónico de comercial@thomas-signe.cl

6 PROCEDIMIENTOS OPERATIVOS

6.1 COMERCIALIZACIÓN

El Solicitante podrá recibir información acerca del proceso de certificación digital de las siguientes maneras:

- Consultando la página web www.thomas-signe.cl
- Mediante el correo electrónico informativo comercial@thomas-signe.cl
- El trato directo con Agentes comerciales.

Por cualquiera de estos medios, se le brindará información acerca de dicho proceso, requisitos, tarifas u otros relativos. Asimismo, se le facilitará un Formulario para que el Solicitante complete sus datos.

6.2 VERIFICAR IDENTIDAD DEL SOLICITANTE

Si el Solicitante, se encuentra interesado en contratar los servicios de Thomas Signe, se ponen a su disposición los siguientes métodos para verificar su identidad

6.2.1 PERSONACIÓN

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.
- Recibir la autorización firmada por el Representante Legal con los datos de la(s) persona(s) autorizada(s) a obtener un Certificado de Pertenencia a Empresa.
- Tomar una fotografía del Solicitante.
- Fotografiar el documento de identidad del Solicitante por ambas caras.
- Digitalizar las escrituras públicas, contratos, estatutos, pactos o cualesquiera otros documentos que puedan acreditar la constitución de la Entidad, su vigencia e identificación de los miembros que la integran.

Esta validación podrá ser realizada por un Notario según formato de validación.

Cabe destacar que todas estas evidencias serán recolectadas y custodiadas por Thomas Signe.

6.2.2 Clave Única

Otra forma de verificar fehacientemente la identidad del Solicitante es mediante la Clave Única, que es un mecanismo de identificación digital que permite a los usuarios demostrar su identidad en plataformas digitales, ya que el Servicio de Registro Civil e Identificación verifica que la identidad digital corresponde a determinada persona, validándola contra su base de datos. Además, para la emisión de un certificado de firma electrónica avanzada, se implementa un segundo factor digital complementario de comprobación de identidad del Solicitante, que cumple con las pautas de identidad digital NIST 800-63-3.

6.3 CONTRATACIÓN Y PAGO

Para proceder, el Solicitante deberá realizar el pago de la tarifa respectiva por un método válido y aprobar todos los términos y condiciones dispuestos en el Contrato de Prestación de Servicios de Certificación de Firma Electrónica, tal como se describe en el apartado anterior.

6.4 SOLICITUD DEL CERTIFICADO

Para solicitar la emisión propiamente dicha de un certificado digital, Thomas Signe completará los datos del Solicitante dentro de la plataforma de registro. Además, procederá a adjuntar los documentos solicitados indicados en el apartado 6.2.1 y 6.2.2.

6.5 REVISIÓN

Thomas Signe verificará que todas las evidencias presentadas se encuentren completas y validará la vigencia de estas.

Una vez verificada satisfactoriamente la identidad del Solicitante y de la Persona Jurídica, Thomas Signe aprobará la solicitud de emisión en la plataforma de registro.

Por otro lado, si se encuentran inconsistencias o irregularidades en las evidencias presentadas, Thomas Signe se lo comunicará al Solicitante, a fin de presentar la evidencia regularizada o actualizada.

6.6 GENERACIÓN DE CLAVES

La generación de claves es siempre realizada en un dispositivo FIPS 140-2 level 3, pudiendo ser este un HSM Centralizado, un token o tarjeta inteligente, según la preferencia del Solicitante.

En el caso de token o tarjeta inteligente, las claves serán generadas por el Solicitante en dicho dispositivo, utilizando aplicaciones compatibles con los estándares de PKI, haciendo entrega a la AR de una petición de certificado en formato PKCS #10 o equivalente.

En el caso de HSM Centralizado, las claves serán generadas por el Solicitante en dicho dispositivo, haciendo entrega a la RA de una petición de certificado en formato PKCS #10.

6.7 EMISIÓN DE CERTIFICADOS

La emisión del certificado es siempre realizada en el mismo dispositivo FIPS 140-2 level 3 en el que se hayan generado previamente el par de claves.

6.7.1 EMISIÓN EN TOKEN O TARJETA INTELIGENTE

Una vez las claves sean generadas, la AR procederá a la emisión del certificado, firmando la petición de certificado recibida y los datos que han sido ingresados en la plataforma SAR y enviándola a la CA y recibiendo de esta el correspondiente certificado emitido.

6.7.2 EMISIÓN EN HSM

Una vez las claves sean generadas, la AR procederá a la emisión del certificado, firmando la petición de certificado recibida y los datos que han sido ingresados en la plataforma SAR y enviándola a la CA y recibiendo de esta el correspondiente certificado emitido.

El certificado es instalado automáticamente en el HSM Centralizado asociado a las claves generadas en éste por el Solicitante.

El propio HSM Centralizado notifica al Solicitante que el certificado ha sido emitido y que ha sido instalado en el HSM. Además, la AR envía un correo electrónico al Solicitante 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.

6.7 REVOCACIÓN 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 descritas en la sección Circunstancias para la revocación de un certificado.

El Titular podrá solicitar la revocación de su certificado, comunicándose por correo electrónico con la AR de Thomas Signe a la dirección soporte@thomas-signe.cl. Thomas Signe se encargará de realizar las validaciones necesarias para la verificación de identidad.

Asimismo, Thomas Signe brinda la opción de revocación en línea, para lo cual el Titular deberá ingresar a al enlace emitido electrónicamente por Thomas Signe para que se autentique y coloque el código de revocación que le fue enviado durante la etapa inicial de emisión de su certificado digital.

6.7.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

Un certificado podrá ser revocado debido a las siguientes causas:

- A solicitud del titular del certificado.
- Por fallecimiento del titular.
- Por incumplimiento de obligaciones del usuario como: proporcionar datos incorrectos de su identidad personal, no custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema que le proporcione el PSC.
- Por cancelación de la acreditación y de la inscripción del prestador en el registro de prestadores acreditados o del cese de la actividad del prestador
- Por cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador.

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 Titular de la vinculación con la Corporación.
- Liquidación de la Pertenencia a Empresa representada que consta en el certificado digital.

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 de los requisitos previstos en los procedimientos de gestión de certificados establecidos en la DPC o PC.
- 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 DPC o en el Contrato de Prestación de Servicios de Certificación de Firma Electrónica.

Circunstancias que afectan a la seguridad del dispositivo criptográfico:

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Manejo indebido por parte del Titular del certificado digital.

Circunstancias que afectan al Titular:

- Finalización de la relación jurídica entre Thomas Signe y el Titular.
- Terminación del Contrato de Prestación de Servicios de Certificación de Firma Electrónica, 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.
- Infracción por el Titular, de sus obligaciones, responsabilidad y garantías, establecidas en el Contrato de Prestación de Servicios de Certificación de Firma Electrónica.
- La incapacidad sobrevenida, total o parcial por el fallecimiento del Titular.

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.

7 PERFIL DE LOS CERTIFICADOS

7.1 CAMPO SUBJECT DEL CERTIFICADO

Los Certificados de Pertenencia a Empresa contendrán como mínimo los elementos que se citan con el formato siguiente. Todos los valores de los componentes serán autenticados por la Autoridad de Registro:

Atributo del DN	Descripción	Valor
Country Name (C)	País	*CL*

Organization Name (O)	Nombre de Organización	*Razón social de la empresa*
Organization Identifier (2.5.4.97)	Identificador de Organización	*RUT de la empresa*
Organization Unit Name (OU)	Unidad Organizativa	*Área de la empresa donde trabaja el titular*
Title (title)	Cargo	*Cargo del titular en la empresa*
Serial Number (serialNumber)	Número de Serie	*RUT del titular*
Surname (SN)	Apellidos	*Apellidos del titular*
Given Name (givenName)	Nombre de Pila	*Nombre del titular*
Common Name (CN)	Nombre	*Nombre completo (nombre y apellidos) del titular*

7.2 EXTENSIONES DE LOS CERTIFICADOS

Extensión	Crítica	Valor
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA Subordinada Chile, 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. 51362.0.4.1.2.1 URI de la DPC: http://cl.thsigne.com/cps User Notice: Certificado para firma electrónica avanzada
Subject Alternative Name		otherName: type-id = OID 1.3.6.1.4.1.8321.1 value = *RUT del titular* rfc822Name: dirección de correo electrónico del titular
Issuer Alternative Name		otherName: type-id = OID 1.3.6.1.4.1.8321.2 value = 76934091-2 (RUT de Thomas Signe Chile S.A.) rfc822Name: psc-cl@thsigne.com

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 Chile: http://thsigne.com/certs/acfea_thomas_signe_chile.crt URI del servicio OCSP de la CA Subordinada Chile: http://ocsp-cl.thsigne.com

8 OBLIGACIONES

8.1 OBLIGACIONES DE LA AC

Thomas Signe se obliga, según lo dispuesto en este documento, principalmente a:

a) Respetar lo dispuesto en las Políticas y Prácticas de Certificación, así como en el Contrato de Prestación de Servicios de Certificación de Firma Electrónica.

b) Publicar esta PC en su página Web.

c) Informar sobre las modificaciones de esta PC a los Titulares, mediante la publicación de estas y sus modificaciones en su página web.

d) Disponer de un seguro de responsabilidad civil que cubra el valor mínimo exigido por la normativa vigente.

e) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el Firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

Por lo que a certificados respecta:

a) Emitir certificados conforme a la DPC y a los estándares de aplicación.

b) Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.

c) Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.

d) Publicar los certificados emitidos en un Registro de Certificados, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.

e) Suspender y revocar los certificados según lo dispuesto en la DPC y publicar las mencionadas revocaciones en la CRL (Lista de Certificados Revocados).

Sobre custodia de información:

a) Conservar la información sobre el certificado emitido por el periodo mínimo exigido por la normativa vigente, cuando sea aplicable.

b) No almacenar ni copiar los datos de creación de firma del Titular, cuando así lo disponga la normativa vigente.

c) Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia

si así se contemplase.

d) Proteger sus claves privadas de forma segura.

e) Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.

8.2 OBLIGACIONES DE LA AR

La Autoridad de Registro también se obliga en los términos definidos en la DPC para la emisión de certificados, principalmente a:

a) Respetar lo dispuesto en la DPC y en la PC correspondiente al tipo de certificado que emita.
b) Respetar lo dispuesto en los contratos firmados con el Titular. En el ciclo de vida de los certificados:

- Comprobar la identidad de los solicitantes de certificados según lo descrito en esta DPC o mediante otro procedimiento que haya sido aprobado por Thomas Signe.
- Verificar la exactitud y autenticidad de la información suministrada por el Titular o Solicitante.
- Informar al solicitante, antes de la emisión de un certificado, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la pérdida o utilización indebida de los datos o dispositivos de creación y de verificación de firma, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, y de la página web donde puede consultar cualquier información de Thomas Signe de la DPC y de la PC correspondiente al certificado.
- Tramitar y entregar los certificados conforme a lo estipulado en esta PC y en la DPC.
- Formalizar el Contrato de Prestación de Servicios de Certificación de Firma Electrónica según lo establecido en esta PC.
- Resguardar, por periodo dispuesto en la legislación vigente, la evidencia suministrados por el Titular.
- Realizar las comunicaciones con los Titulares, por los medios que consideren adecuados, para la correcta gestión del ciclo de vida de los certificados.

8.3 OBLIGACIONES DE LOS PROVEEDORES

El Proveedor de infraestructura tecnológica de Thomas Signe se encuentra obligado a cumplir con los requisitos que le resulten aplicables, dispuestos en el documento Guía de Evaluación Procedimiento de Acreditación PSC FEA en su versión vigente.

8.4 OBLIGACIONES DE LOS SOLICITANTES

El solicitante de un certificado estará obligado a cumplir con lo dispuesto por la normativa y, además:

a) Suministrar a la AR la información necesaria y completa para realizar una correcta identificación.

b) Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.

c) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

d) Respetar lo dispuesto en los documentos contractuales firmados con Thomas Signe.

8.5 OBLIGACIONES DE LOS FIRMANTES

El firmante estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

a) Custodiar sus claves privas y códigos secretos de manera diligente.

b) Usar el certificado según lo establecido en la presente PC.

c) Respetar lo dispuesto en los instrumentos jurídicos vinculantes con Thomas Signe.

d) Informar a la mayor brevedad posible de la existencia de alguna causa de revocación.

e) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

f) No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por Thomas Signe de la revocación de este, o una vez expirado el plazo de validez del certificado.

g) Actualizar sus datos en la medida que éstos vayan cambiando.

8.6 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Será obligación de los usuarios cumplir con lo dispuesto por la normativa vigente y, además:

a) Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

b) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

c) Notificar a Thomas Signe cualquier situación irregular con respecto al servicio prestado por el PSC.