Entidad de Certificación Digital

THOMAS SIGNE

SOLUCIONES TECNOLÓGICAS GLOBALES

Política de Certificación de Pertenencia a Empresa

Información del documento

Nombre	POLÍTICA DE CERTIFICACIÓN DE PERTENENCIA A EMPRESA
Realizado por	THOMAS SIGNE S.A.S.
País	COLOMBIA
Versión	1.6
Fecha	MAYO DEL 2019
Tipo de Documento	PÚBLICO
Código	**THS-CO-POL-COR-AC-02**

Historial de versiones

Versión	Fecha	Descripción
1.0	28/06/2017	Elaboración de documento inicial.
1.1	20/05/2018	Se agrega la sección de Obligaciones. Se especifica el Procedimiento operativo del certificado.
1.2	24/05/2018	Se agrega el apartado de Circunstancias para la revocación de un certificado.
1.3	08/06/2018	Se agregan apartados para formatos y registros aplicables.
1.4	02/11/2018	Se elimina del pie de página la referencia al THS-PR-GRAL-02-F01 Estructura de documento v1.0. Se elimina el apartado “INTRODUCCIÓN”.
1.5	22/01/2019	Se añade la posibilidad de que, opcionalmente, el OR realice la verificación de la identidad del Solicitante de forma presencial, en vez de por videoconferencia. Correcciones menores.
1.6	09/05/2019	Integración con el sistema de gestión del Grupo. Cambio de nombre del documento de THS-PC-PE-01

		a THS-CO-POL-COR-AC-02. Se eliminan las secciones de formatos y registros aplicables. Correcciones menores.

ÍNDICE

1 OBJETIVO

Este documento tiene como objetivo la descripción de las prácticas, los perfiles y los tipos de usuarios y usos definidos para Thomas Signe S.A.S., de acuerdo a lo estipulado en las Políticas de Certificación de Signe, para la administración de los certificados digitales en el marco del cumplimiento de los "Criterios específicos de acreditación Entidades de Certificación Digital - CEA-4.1-10 Versión 01" establecida por el Organismo Nacional de Acreditación de Colombia – ONAC.

2 DEFINICIONES Y ABREVIACIONES

2.1 ACRÓNIMOS Y ABREVIACIONES

CA Autoridad de Certificación

CRL Lista de Certificados Revocados

DPC Declaración de Prácticas de Certificación

ECD 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.

HSM Hardware Security Module

NIT Número de Identificación Tributaria

ONAC Organismo Nacional de Acreditación de Colombia

OCSP Servicio del estado del certificado en línea

OR Operador de Registro

PC Política de Certificación

PKI Infraestructura de llave pública

RA Autoridad de Registro

RUE Registro Único Empresarial

SHA Secure Hash Algorithm (Algoritmo de seguridad HASH)

2.2 DEFINICIONES Y CONCEPTOS

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.

Certificado digital: mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de éste último.

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

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

Entidad de Certificación: De acuerdo con lo indicado en la Ley 527 de 1999, Artículo 2, Literal d, es aquella persona natural o jurídica que, autorizada conforme a dicha Ley, está facultada para emitir certificados digitales en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

Entidades de Certificación Digital – ECD: Denominación que se establece con el fin de particularizar y diferenciar este tipo de organizaciones como Entidades de Certificación de los demás Organismos de Certificación que ONAC acredita.

Autoridad de Registro: Persona jurídica, con excepción de los notarios públicos, o parte interna de las ECD necesariamente independiente de su CA, que acorde con la normatividad vigente, es la encargada de recibir las solicitudes relacionadas con certificación digital, para: Registrar las peticiones que hagan los solicitantes para obtener un certificado; y comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones. Enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.

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.

Lista de Certificados Digitales Revocados: es aquella relación que debe incluir todos los certificados revocados por la entidad de certificación digital.

PKI: Infraestructura de llave 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 suscriptor 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 suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío (no repudio).

Políticas de Certificación: 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 Declaración de Prácticas de Certificación. .

Servicio del estado del certificado en línea OCSP: Actividad de consulta en tiempo real al sistema de la ECD, sobre el estado de un certificado digital a través del protocolo OCSP

Servicio de certificación digital: Conjunto de actividades certificación que ofrece la ECD 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 que con el propósito de obtener servicios de certificación digital de una ECD, demuestra el cumplimiento de los requisitos establecidos en la DPC y PC de éstas, para acceder al servicio de certificación digital.

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

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

3 PUBLICACIÓN DEL DOCUMENTO

La presente PC establece las políticas y procedimientos que lleva a cabo Thomas Signe S.A.S. para brindar los servicios de emisión, revocación y distribución de los certificados digitales; siguiendo el estándar RFC 3647, conforme a las leyes colombianas y las disposiciones de los entes reguladores.

Las PCs, así como las DPCs y otros documentos relacionados al servicio de certificación digital, se encuentran publicados en la página web de Thomas Signe S.A.S.: www.thomas-signe.co

4 CARACTERÍSTICAS DE CERTIFICADOS

4.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los certificados de Pertenencia a Empresa tienen un periodo de validez de hasta 2 años (730 días).

4.2 TIPOS DE SOPORTE

Los Certificados de Pertenencia a Empresa de Thomas Signe S.A.S. pueden ser emitidos en dos tipos de soporte: Tarjeta/Token y HSM Centralizado. La emisión en soporte Tarjeta/Token se encuentra limitada a Operadores de Registro de Thomas Signe S.A.S. Por otro lado, la emisión mediante HSM Centralizado se encuentra disponible para todos los usuarios en general que cumplan con los requisitos estipulados por la ECD.

4.2.1 TARJETA/TOKEN

Las claves privadas de los Certificados de Pertenencia a Empresa emitidos en Tarjeta/Token se generan y almacenan en un dispositivo del tipo tarjeta o token criptográfico.

La emisión de los Certificados de Pertenencia a Empresa en Tarjeta/Token se encuentra limitada a Operadores de Registro de Thomas Signe S.A.S.

Los Certificados de Pertenencia a Empresa emitidos en este soporte hacen uso de dispositivos criptográficos 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 Suscriptor en la custodia de dispositivos criptográficos
- Daño físico del módulo criptográfico

Los Certificados de Pertenencia a Empresa en Tarjeta/Token están identificados mediante el OID (1.3.6.1.4.1.51362.0.2.1.2.1) en la extensión "X509v3 Certificate Policies".

4.2.2 HSM CENTRALIZADO

Los Certificados de Pertenencia a Empresa pueden ser emitidos mediante HSM Centralizado.

Los Certificados de Pertenencia a Empresa emitidos en este soporte hacen uso de un dispositivo criptográfico centralizado 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 Suscriptor en la custodia de dispositivos criptográficos
- Daño físico del módulo criptográfico

Los Certificados de Pertenencia a Empresa en HSM Centralizado están identificados mediante el OID (1.3.6.1.4.1.51362.0.2.1.2.3) en la extensión "X509v3 Certificate Policies".

4.3 USO PARTICULAR DE LOS CERTIFICADOS DE PERTENENCIA A EMPRESA

4.3.1 USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados emitidos por Thomas Signe S.A.S. podrán usarse en los términos establecidos por la 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 Suscriptor y su vinculación con la empresa.

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

4.3.2 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 S.A.S.

4.4 TARIFAS

Las Tarifas especificadas son referenciales, por lo que puede variar de acuerdo al tipo de certificado y al contrato con cada cliente:

CERTIFICADO	**COSTO**
Pertenencia a Empresa	170 000 pesos colombianos

Las mismas tarifas se encuentran publicadas en la página Web de Thomas Signe: www.thomas-signe.co

4.5 MÉTODOS DE PAGO

Thomas Signe S.A.S. pone a disposición del público, una cuenta bancaria para realizar el depósito de la cuantía respectiva a cada servicio. La cuenta a nombre de THOMAS SIGNE SOLUCIONES TECNOLOGICAS GLOBAL S.A.S., se indica a continuación:

BANCO DE BOGOTÁ, CTA CORRIENTE No. 017346362

No obstante, Thomas Signe S.A.S. puede precisar de un método alternativo de pago en el caso de un Contrato de Prestación de Servicios con el cliente.

5 PROCEDIMIENTOS OPERATIVOS

5.1 COMERCIALIZACIÓN

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

- Consultando la página web www.thomas-signe.co
- Mediante el correo electrónico informativo comercial@thomas-signe.co
- 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.

Luego de ser informado, el Solicitante enviará un mensaje de correo electrónico a comercial@thomas-signe.co indicando (1) el tipo de certificado requerido, (2) su nombre completo, (3) tipo y número de identificación y (4) cuenta de correo electrónico que estará asociada al certificado digital y por medio de la cual la ECD realizará notificaciones y comunicaciones oficiales.

5.2 CONTRATACIÓN Y PAGO

El Área comercial enviará un mensaje de correo electrónico al Solicitante con la Propuesta Comercial, Contrato de Suscripción, opcionalmente un enlace a la plataforma SAR, y las indicaciones respectivas.

Para proceder, el Solicitante deberá:

- Realizar el pago de la tarifa respectiva por un método válido (ver sección *4.5. Métodos de pago*). La evidencia de este proceso será el voucher o comprobante de pago.
- Aprobar todos los términos y condiciones dispuestos en el Contrato entre Thomas Signe S.A.S. y el Solicitante, mediante la firma y/o aceptación respectiva. La evidencia de este proceso será el Contrato firmado.

5.3 SOLICITUD DEL CERTIFICADO

Para solicitar la emisión propiamente dicha de un certificado digital en HSM Centralizado, el Solicitante deberá ingresar al enlace de la plataforma SAR y completar sus datos correctamente (Ver Anexo I). Además, dentro de la plataforma, procederá a adjuntar los documentos solicitados indicados a continuación:

- Documentos que sustentan los datos registrados en dicho Formulario:
  - Documento de identidad escaneado por ambas caras: Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte; expedidos en Colombia (por defecto) o en el país emisor del documento.
  - Certificado de Cámara de Comercio virtual o escaneado.
  - Registro Único Tributario en copia virtual o escaneado.
  - Autorización firmada por el Representante Legal con los datos de la(s) persona(s) autorizada(s) a obtener un Certificado de Pertenencia a Empresa.
- Constancia del pago de la tarifa de Certificado de Pertenencia a Empresa.
- Contrato de suscripción firmado.

Alternativamente, el Solicitante podrá entregar personalmente o enviar los documentos solicitados al OR, y éste ingresará en la plataforma SAR los datos del Solicitante y adjuntará los documentos solicitados.

5.4 REVISIÓN

El OR verificará que toda la documentación adjuntada se encuentre completa y validará los documentos presentados de la siguiente manera:

- El documento de identidad del Solicitante: En caso se trate de un ciudadano colombiano y el documento presentado sea la Cédula de Ciudadanía, el OR validará la identidad consultando ante una Base de datos on line. Asimismo, verificará que el documento enviado se encuentre vigente.
- La identidad de la Persona Jurídica: Se validará que el Certificado de la Cámara de Comercio y el RUT sean legítimos, se encuentren vigentes y que el NIT coincida en ambos documentos. Además, se consultará el NIT en la Base de datos RUE para verificar la existencia de la empresa, si se encuentra activa y los Representantes legales.

- Además, se verificará que el documento que lo autoriza a solicitar dicho certificado, se encuentre firmado por el Representante que figura en el Certificado de Existencia.

En caso de que todos los requisitos de validación se encuentren conformes, el OR coordinará con el Solicitante una cita para realizar una videoconferencia en la que verificará la identidad del Solicitante.

Alternativamente a la videoconferencia, el OR podrá haber verificado la identidad del Solicitante de forma presencial, en cuyo caso deberá haber recibido del Solicitante y haber archivado la documentación y evidencias requeridas en formato papel, así como haber ingresado los mismos en la plataforma SAR en formato digital.

Una vez validada satisfactoriamente la identidad del Solicitante, el OR aprobará la solicitud de emisión en la plataforma de la RA.

En caso de no aprobarse, el OR informará al Solicitante las razones que generaron el rechazo.

5.5 DECISIÓN

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

5.6 GENERACIÓN DE CLAVES

Las claves serán generadas por el Solicitante en el HSM Centralizado o por el OR en Tarjeta/Token en presencia del Solicitante (limitado a certificados de Operadores de Registro de Thomas Signe S.A.S), haciendo entrega a la RA de una petición de certificado en formato PKCS#10.

5.7 EMISIÓN

La RA procederá a la emisión del certificado, firmando la petición de certificado en formato PKCS#10 y enviándola a la CA.

5.8 ENTREGA

Finalmente, el OR genera el certificado en Tarjeta/Token (limitado a certificados de Operadores de Registro de Thomas Signe S.A.S) o mediante HSM Centralizado para ser entregado al Suscriptor. Asimismo, hace entrega de instructivos y manuales para el uso de certificado e información de políticas.

5.9 REVOCACIÓN DE CERTIFICADOS

El Suscriptor 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 *5.9.1. Circunstancias para la revocación de un certificado*.

Para solicitar la revocación del certificado el Suscriptor puede:

- Revocar online su certificado en la página web de Thomas Signe S.A.S., en el caso de que el tipo de soporte sea HSM Centralizado. El Suscriptor deberá ingresar su usuario y contraseña de acceso al HSM Centralizado.

- De forma alternativa, el Suscriptor que desee revocar su certificado digital, podrá comunicarse con el Responsable de PQRSA de Thomas Signe S.A.S. a la dirección pqrsa@thomas-signe.com, la cual será derivada al Operador de Registro. Cabe destacar que la solicitud de revocación tendrá que ser desde la cuenta de correo electrónico declarada en el Formulario de solicitud respectivo.

Para toda información complementaria referente a la revocación de los certificados, referirse al apartado correspondiente de la DPC.

5.9.1 CIRCUNSTANCIAS PARA LA REVOCACIÓN DE UN CERTIFICADO

Un certificado podrá ser revocado debido a las siguientes causas:

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.

- 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 la ECD, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

- Infracción, por parte de la ECD 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 Suscriptor.

- Acceso o utilización no autorizados, por un tercero, de la clave privada del Suscriptor.

- El incumplimiento por parte del Suscriptor de las normas de uso del certificado expuestas en la DPC o en el Contrato de Suscripción.

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, en el caso de que el tipo de soporte sea Tarjeta/Token.

- Acceso no autorizado, por un tercero, a los datos de activación del Suscriptor.

- El incumplimiento por parte del Suscriptor de las normas de uso del dispositivo criptográfico expuestas en la DPC o en el Contrato de Suscripción.

d) Circunstancias que afectan al Suscriptor:

- Finalización de la relación jurídica entre la ECD y el Suscriptor.

- Terminación del Contrato de suscripción, 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 Suscriptor.

- Oposición o modificación, por parte del Suscriptor y Solicitante, de los datos contenidos en el fichero de datos de carácter personal de Thomas Signe S.A.S.

- Infracción por el Solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

- Infracción por el Suscriptor, de sus obligaciones, responsabilidad y garantías, establecidas en el Contrato de suscripción.

- La incapacidad sobrevenida, total o parcial por el fallecimiento del Suscriptor.

e) Otras circunstancias:

- Por pérdida, inutilización del certificado digital que haya sido informado a la ECD.

- 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.

6 PERFIL DE LOS CERTIFICADOS

6.1 NOMBRE DISTINGUIDO (DN)

Los Certificados de Pertenencia a Empresa contendrá 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	*Código de dos letras mayúsculas según ISO 3166-1 del país de la empresa* [1] Por defecto: CO
State or Province Name (ST)	Estado/Provincia	*Departamento de la empresa* [2]
Locality Name (L)	Localidad	*Municipio de la empresa* [2]
Street Address (STREET)	Dirección	*Dirección de la empresa* [2]
Organization Identifier (2.5.4.97)	Identificador de Organización	*Número de identificación fiscal de la empresa* [2]
Organization Name (O)	Nombre de Organización	*Razón social de la empresa* [2]
Organization Unit Name (OU)	Unidad Organizativa	*Área* [2]
Title (title)	Cargo	*Cargo* [2]
Serial Number (serialNumber)	Número de Serie	*TipoDoc-NumDoc* [1] *TipoDoc*: *Tipo de documento de identificación del Suscriptor* *NumDoc*: *Número de documento de identificación del Suscriptor*
Surname (SN)	Apellidos	*Apellidos del Suscriptor* [2]
Given Name (givenName)	Nombre de Pila	*Nombre de pila del Suscriptor* [2]
Common Name (CN)	Nombre	*Nombre completo (nombre y apellidos) del*

[1] Codificado en PrintableString

[2] Codificado en UTF8String

		Suscriptor [2]

6.2 EXTENSIONES DE LOS CERTIFICADOS

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. 51362.0.2.1.2.x [3] URI de la DPC: http://thsigne.com/cps
Subject Alternative Name		rfc822Name: *correo electrónico empresarial del Suscriptor*
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-co.thsigne.com/ecd_thomas_signe_colombia.crl
Authority Information Access	-	URI del certificado de la CA Subordinada: http://thsigne.com/certs/ecd_thomas_signe_colombia.crt URI del servicio OCSP de la CA Subordinada: http://ocsp-co.thsigne.com

7 OBLIGACIONES

7.1 OBLIGACIONES DE LA ECD

Thomas Signe S.A.S. se obligan según lo dispuesto en este documento, principalmente a:

a) Respetar lo dispuesto en las Políticas y Prácticas de Certificación (la presente DPC), así como en el Contrato de Suscripción.

b) Publicar esta PC en su página Web.

c) Informar sobre las modificaciones de esta PC a los Suscriptores, mediante la publicación de éstas 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.

[3] Tarjeta/Token (OR): x=1; HSM Centralizado: x=3

e) Utilizar sistemas fiables para almacenar certificados 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 Suscriptor 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 período mínimo exigido por la normativa vigente, cuando sea aplicable.

b) No almacenar ni copiar los datos de creación de firma del Suscriptor, 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.

f) Remitir a ONAC, con frecuencia anual, para la realización de la Etapa 1 de cada evaluación de la acreditación:

- Archivo con los certificados emitidos y su respectivo contenido.

- Archivo con totales de control (emitidos, vigentes, revocados y expirados).

7.2 OBLIGACIONES DE LA RA

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 la ECD.

c) Respetar lo dispuesto en los contratos firmados con el Suscriptor y/o Solicitante. 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 la ECD.

- Verificar la exactitud y autenticidad de la información suministrada por el 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 la ECD, de la DPC y de la PC correspondiente al certificado.

- Tramitar y entregar los certificados conforme a lo estipulado en esta DPC y en la CP correspondiente.

- Formalizar el contrato de suscripción según lo establecido por la Política de Certificación aplicable.

- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor y/o Solicitante.

- Informar a la ECD las causas de revocación.

- Realizar las comunicaciones con los Suscriptores, por los medios que consideren adecuados, para correcta gestión del ciclo de vida de los certificados. Concretamente realizar las comunicaciones relativas a la proximidad de la caducidad de los certificados y a las suspensiones, rehabilitaciones y revocaciones de los mismos.

7.3 OBLIGACIONES DE LOS PROVEEDORES

El Proveedor de infraestructura tecnológica de Thomas Signe S.A.S. se encuentra obligado a cumplir con los requisitos mínimos exigidos por ONAC, dispuestos en el documento CEA 4.1-10 vigente, tales como:

a) Responsabilidad y financiación

b) Confidencialidad

c) Requisitos para los recursos

d) Requisitos del proceso – Ciclo de vida del certificado digital

e) Requisitos del sistema de gestión

f) Requisitos de la CA

g) Requisitos de la RA

h) Requisitos técnicos

7.4 OBLIGACIONES DE LOS SOLICITANTES

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

a) Suministrar a la RA la información necesaria 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 la ECD y la RA.

7.5 OBLIGACIONES DE LOS SUSCRIPTORES

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

a) Custodiar sus claves privadas 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 la ECD y la RA.

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 la ECD o la RA de la revocación del mismo, o una vez expirado el plazo de validez del certificado.

7.6 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 S.A.S. cualquier situación irregular con respecto al servicio prestado por la ECD.

8 ANEXOS

8.1 ANEXO I: FORMULARIO DE SOLICITUD DE CERTIFICADO DE PERTENCIA A EMPRESA

Datos del Solicitante	
País de expedición del Documento	*Seleccionar de acuerdo al país:* *CO = Colombia*
Tipo de Documento	*Seleccionar de acuerdo al tipo de documento:* *Cédula de Ciudadanía = CC* *Cédula de Extranjería =CE* *Pasaporte = PA*
N° de Documento de identidad	*Completar el Número del Tipo de documento seleccionado*
Nombres	*Completar los Nombres como aparecen en el Documento de identidad*
Apellidos	*Completar los Apellidos como aparecen en el Documento de identidad*
Área	*Completar el Área del Solicitante en la Empresa*
Cargo del Solicitante	*Completar el Cargo del Solicitante en la Empresa*
Celular	*Completar el Número de celular del Solicitante*
Correo electrónico	*Completar el Correo electrónico corporativo*

Datos de la Entidad	
Razón social	*Completar la Razón social de la Empresa*
NIT	*Completar el Número de Identificación Tributaria de la Empresa*
País	*Completar el País donde se localiza la Empresa*
Estado/Provincia	*Completar el Departamento donde se localiza la Empresa*
Localidad	*Completar el Municipio donde se localiza la Empresa*
Dirección	*Completar la Dirección exacta donde se localiza la Empresa*

8.2 ANEXO II: CONTRATO DE SUSCRIPCIÓN

INTERVIENEN
Por una parte,
La Entidad de Certificación Digital de THOMAS SIGNE SOLUCIONES TECNOLÓGICAS GLOBALES SAS, en adelante ENTIDAD, con N° de NIT 900962071-5, con domicilio en la Av. Las Américas No 45-57 Bogotá D.C.

Por otra parte, en adelante CLIENTE.
Nombre del Suscriptor: _____
Tipo de documento: _____
Número de documento: _____
Dirección: _____
Correo electrónico: _____

Las partes involucradas tienen conocimiento y se encuentran conformes con los siguientes términos y condiciones:

1. DEFINICIONES Y ABREVIACIONES
Los términos, abreviaciones, acrónimos y definiciones aplicables al presente contrato se indican a continuación:
- Certificado Digital: mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la clave pública de este último.
- Clave Privada: Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.
- Clave Pública: Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.
- DPC – Declaración de Prácticas de Certificación: Documento en el que consta de manera detallada los procedimientos que aplica la ECD para la prestación de sus servicios.
- ECD – Entidad de Certificación Digital: Entidad que presta servicios de emisión, revocación y otras gestiones propias de certificados digitales, de acuerdo a la regulación establecida por el ONAC.
- ONAC – Organismo Nacional de Acreditación de Colombia: Organismo colombiano que presta el servicio de acreditación a los organismos de evaluación de la conformidad.
- PC – Política de Certificación: Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
- Repositorio: sistema de información utilizado para almacenar y recuperar certificados, políticas u otra información relacionada con los mismos.
- Solicitante: persona natural que con el propósito de obtener servicios de certificación digital de una ECD, demuestra el cumplimiento de los requisitos establecidos en la DPC y PCs de estas, para acceder al servicio de certificación digital.
- Suscriptor: persona natural o jurídica a cuyo nombre se expide un certificado digital.

2. DE LA ENTIDAD QUE PRESTA SUS SERVICIOS
2.1. Obligaciones legales y generales
- Cumplir con las obligaciones especificadas por el ONAC y los Criterios específicos de acreditación Entidades de Certificación Digital - CEA-4.1-10 en su versión vigente, establecidos por él.
- Encontrarse regulada por la Ley 527 de 1999 y sus modificaciones; el Decreto de Ley 0019 de 2012 y sus modificaciones; el Decreto 333 de 2014 y sus modificaciones; y el Decreto 1471 de 2014 y sus modificaciones y demás normas que le resulten aplicables.
- Cumplir con lo dispuesto en su respectiva DPC y PCs.
2.2. Obligaciones financieras
2.2.1. Política de reembolso
La ENTIDAD cuenta con una Política de reembolso acorde con las leyes vigentes.
2.2.2. Cobertura de seguro
La ENTIDAD dispone de una garantía de cobertura de su responsabilidad civil suficiente para el pago de indemnizaciones o pagos afín, bien mediante un seguro de responsabilidad civil profesional por errores y omisiones, bien mediante una fianza o aval. En cualquier caso, la cuantía garantizada cubrirá la cuantía mínima establecida por el ONAC en todo momento.
2.3. Excepciones de garantía

- La ENTIDAD limita su responsabilidad mediante la inclusión de límites de uso del certificado, y límites de valor de las transacciones para las que puede emplearse el certificado, de acuerdo con lo establecido en su DPC y PCs.
- Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse del uso del certificado fuera de tales límites quedan a cargo del CLIENTE. En ningún caso podrá el CLIENTE ni los terceros perjudicados reclamar a la ENTIDAD compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados para fines de cifrado.

2.4. Eventos eximentes de responsabilidad

La ENTIDAD limita su responsabilidad en el evento de caso fortuito y/o fuerza mayor, respecto de la emisión y uso de certificado.

2.5. Obligaciones de la ENTIDAD en relación al CLIENTE

- La ENTIDAD se hace cargo de publicar en su repositorio los documentos informativos acerca de los servicios brindados por esta. El CLIENTE podrá acceder ingresando a la página web de la ENTIDAD: www.thomas-signe.co
- Proteger y custodiar de manera segura y responsable su clave privada.
- Emitir certificados conforme a las PCs y a lo definido en la DPC.
- Generar certificados de conformidad con la información suministrada por el solicitante.
- Conservar la información sobre los certificados emitidos de conformidad con la normatividad vigente.
- Emitir certificados cuyo contenido mínimo esté de conformidad con la normativa vigente para los diferentes tipos de certificados.
- 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.
- No mantener copia de la clave privada del suscriptor.
- Revocar los certificados según lo dispuesto en la DPC.
- Publicar los certificados revocados en la lista de certificados revocados CRL.
- Informar a los suscriptores de la revocación del certificado digital de conformidad con la política de revocación de certificados digitales.
- Las modificaciones realizadas en los contratos o cambios en las políticas y prácticas de la ENTIDAD serán comunicadas al CLIENTE.
- Notificar al CLIENTE cualquier cambio en los términos y condiciones básicas (identificadores de políticas, limitaciones de uso, obligaciones de CLIENTE, forma de validación de un certificado, procedimiento de resolución de disputas, periodo dentro del cual los registros de auditoría serán conservados, sistema legal aplicable y conformidad según el marco del ONAC).

2.6. Resolución de diferencias

La solicitud de resolución de diferencias deberá ser comunicada por medio del correo electrónico brindado por el CLIENTE a través del presente contrato y el de la ENTIDAD pqrsa@thsigne.com

Dentro de los quince (15) días siguientes al envío del mensaje de correo electrónico, se buscará llegar a un arreglo directo entre el CLIENTE y la ENTIDAD, y se ejecutará el procedimiento de Peticiones, Quejas, Reclamos, Apelaciones y Sugerencias (PQRSA). En caso no se llegase a un acuerdo entre las partes, intervendría un tercero, bien mediante arbitraje, bien acudiendo a la jurisdicción que corresponda para su resolución, de conformidad con la Ley 1563 de 2012, que regula el Arbitraje Nacional e Internacional. La jurisdicción aplicable será la del territorio de Colombia independientemente de la nacionalidad o domicilio del suscriptor. Las partes fijan como domicilio contractual, para efectos judiciales, la ciudad de Bogotá.

2.7. Comunicaciones de valor legal

Ambas partes reconocen que las comunicaciones se realizarán por medio electrónico a través del correo electrónico brindado por el CLIENTE a través del presente contrato y el de la ENTIDAD pqrsa@thsigne.com

2.8. PQRSA

Los suscriptores y en general cualquier interesado podrá acceder a la página web de la ENTIDAD www.thomas-signe.co o remitir un correo electrónico a pqrsa@thsigne.com para indicar sus peticiones, quejas, reclamos, apelaciones y sugerencias.

2.9. Uso y protección de datos personales

- El CLIENTE, al completar el Formulario de Solicitud y aceptar el presente Contrato, autoriza a la ENTIDAD para la recolección, almacenamiento y uso de los datos proporcionados con la finalidad de llevar a cabo las validaciones necesarias de autenticidad para brindar servicios de certificación digital, así como para fines comerciales relacionados con los mismos.
- La ENTIDAD llevará a cabo el tratamiento de datos personales de acuerdo a su Política de Privacidad, la cual referencia a la Ley Estatuaria 1581 del 17 de octubre de 2012 de Protección de Datos Personales y Decreto 1377 de 2013 y demás normatividad aplicable.

2.10. Notificaciones

- El procedimiento por el cual las partes se notifican hechos mutuamente es mediante el correo electrónico brindado por el CLIENTE a través del presente contrato. Si el CLIENTE desea enviar correspondencia o notificaciones físicas deberá ser dirigida a la dirección Avenida de Las Américas No 44-57 – Bogotá DC –

Colombia.

2.11. Imparcialidad

La ENTIDAD se compromete a cumplir con su Política de imparcialidad, la cual se encuentra publicada en su página web, por lo cual garantizará a su vez que en el desarrollo de sus actividades no permitirá presiones exógenas de índole comercial, financiera u otras comprometan la calidad del servicio prestado. De igual forma la ENTIDAD garantiza que el personal de apoyo contratado por la compañía para la ejecución del servicio contratado es idóneo para el desempeño de sus funciones y no presenta ningún tipo de inhabilidad e incompatibilidad que atenten contra la continuidad de la actividad desarrollada por las partes suscribientes.

2.12. Tarifas

Las tarifas propuestas por la ENTIDAD se encuentran descritas en la propuesta comercial entregada al cliente para la firma del presente contrato o pueden ser consultadas directamente a la ENTIDAD.

3. DEL CLIENTE

3.1. Obligaciones generales

- Manifestar ser consciente y encontrarse conforme a lo estipulado en el presente contrato y en los documentos facilitados por la ENTIDAD.
- Cumplir los requisitos del servicio de certificación digital respectivo, incluyendo la implementación de los cambios cuando los comunica la ENTIDAD.
- Cumplir con los términos y condiciones aceptadas al momento de solicitar servicios de certificación digital.
- Informar durante la vigencia del certificado digital de cualquier cambio en los datos suministrados para la emisión del certificado.
- No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para la ENTIDAD, y no hacer ninguna declaración relacionada con su certificación digital que la ENTIDAD pueda considerar engañosa o no autorizada.
- Que inmediatamente después de la cancelación o la terminación de la certificación digital, el CLIENTE deja de utilizarla en todo el material publicitario que contenga alguna referencia a ella, y emprende las acciones exigidas por el servicio de certificación digital y cualquier otra medida que se requiera en la DPC y PC.
- Que al hacer referencia al servicio de certificación digital en medios de comunicación, tales como documentos, folletos o publicidad, el CLIENTE informa de que cumple con los requisitos especificados en la DPC y PC.
- Cumplir los requisitos que pueda prescribir el servicio de certificación digital con relación al uso de las marcas de conformidad y a la información relacionada con el servicio.
- Informar a la ENTIDAD, sin retraso, acerca de los cambios que pueden afectar el servicio de certificación digital que le fue expedido por la ENTIDAD.
- El CLIENTE, al aceptar este contrato, asimismo acepta los términos de uso y condiciones del servicio especificadas en la DPC y PC respectiva de la ENTIDAD, y en el presente contrato de prestación de servicios de certificación digital.
- Al adquirir el certificado digital con la ENTIDAD, el CLIENTE se obliga a conocer y enviar el contrato de suscripción aceptado.

3.2. Obligaciones financieras

- Indemnizaciones: El CLIENTE indemnizará y liberará de toda responsabilidad a la ENTIDAD del uso que esta haga del certificado otorgado, que no sea el uso indicado en el presente contrato y en los documentos brindados por la ENTIDAD (DPC, PCs, Políticas de Seguridad y Privacidad, etc.), para lo cual existe la Política de reembolso previamente mencionada.

3.3. Revocación

La revocación de certificados digitales podrá efectuarse por medio de la página web, ingresando al link https://thomas-signe.co/emision/; o contactándose con la RA de la ENTIDAD, solicitando la revocación desde su correo declarado, a la dirección pqrsa@thsigne.com

Se deberá solicitar la revocación del certificado digital en caso de:

- Pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada.
- Compromiso potencial de la clave privada.
- Pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa.
- Las mencionadas en la DPC y PC respectiva de la ENTIDAD, las cuales se pueden consultar en la página web de la ENTIDAD.

3.4. Otras obligaciones

- Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado.
- A partir de la fecha en que el certificado expira, el CLIENTE no podrá utilizar válidamente ni el certificado ya expirado, ni su clave privada.
- Solicitar la revocación de certificados cuando incumple las obligaciones a las que se encuentra comprometido dentro del marco del ONAC.

3.5. Vigencia del servicio

- El periodo de vigencia del presente contrato de suscripción inicia desde el momento en que el solicitante envía la solicitud a la ENTIDAD y termina cuando pierde vigencia el certificado o, si ocurriere, hasta la revocación del mismo. A su vez, el presente contrato pierde vigencia en el momento que el CLIENTE incumpla con las obligaciones del presente contrato o con la DPC o PC respectiva de la ENTIDAD.

Fecha: _____

Firma de Thomas Signe S.A.S.

Fdo. _____

Firma del Solicitante

Fdo. _____