Entidad de Certificación Digital

THOMAS SIGNE

SOLUCIONES TECNOLÓGICAS GLOBALES

Política de Certificados de Componente

Información del documento

Nombre	POLÍTICA DE CERTIFICADOS DE COMPONENTE
Realizado por	THOMAS SIGNE S.A.S.
País	COLOMBIA
Versión	2.2
Fecha	NOVIEMBRE DEL 2020
Tipo de Documento	PÚBLICO
Código	**THS-CO-AC-PC-COR-01**

Historial de versiones

Versión	Fecha	Descripción
1.0	28/06/2017	Elaboración de documento inicial.
1.1	12/05/2018	Precisiones en el procedimiento del ciclo de vida. Cambios menores de nomenclatura.
1.2	20/05/2018	Se agrega la sección de Obligaciones. Se especifica el Procedimiento operativo del certificado.
1.3	24/05/2018	Se agrega el apartado de Circunstancias para la revocación de un certificado.
1.4	08/06/2018	Se agregan apartados para formatos y registros.
1.5	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".
1.6	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.
1.7	09/05/2019	Integración en el sistema de gestión del Grupo. Cambio de nombre del documento de THS-PC-CC-01 a THS-CO-POL-COR-AC-01.

		Se añade la posibilidad de que, opcionalmente, el certificado se emita en el soporte Otros Dispositivos, a partir de una petición de certificado en formato PKCS #10 entregada por el Solicitante, en vez de en el soporte HSM Centralizado. Se eliminan las secciones de formatos y registros aplicables. Correcciones menores.
1.8	18/09/2019	Ajuste de la codificación según el GSIGNE-GRAL-PR-01 Control de la Informacion Documentada Ed 2.1. Se añaden las posibilidades de que el Suscriptor pueda ser una Persona Natural, de que el Solicitante pueda ser una Persona Jurídica distinta al Suscriptor, y de que, en el caso de que el tipo de soporte sea Otros Dispositivos, haya dos Solicitantes (una Persona Jurídica distinta al Suscriptor y una Persona Natural). En la solicitud del certificado, en los casos que el Solicitante no sea el Representante Legal o haya dos Solicitantes, se adjuntará el documento de identidad del Representante Legal, además de la autorización firmada por éste con los datos de la Persona Natural o de la Persona Jurídica autorizada a obtener el certificado. En la revisión de la solicititud del certificado, en la validación del documento de identidad del Solicitante (Persona Natural), se elimina la consulta ante una Base de datos online. Se indica que la emisión e instalación del certificado en el HSM Centralizado son realizadas automáticamente por la RA al recibir la petición de certificado en formato PKCS #10, sin intervención de un OR (cambio implementado en enero de 2019). Se añaden las secciones de Formatos y Registros. En el contrato de suscripción (*Anexo II*), se cambia la Firma del Solicitante por la Firma del Suscriptor (el Solicitante y el Suscriptor son Personas Naturales o Personas Jurídicas distintas). Correcciones menores.
1.9	29/11/2019	Cambio del No. de cuenta corriente para realizar el depósito de la cuantía respectiva a cada servicio. Añadidos un formato y un registro para las videconferencias de verificación de identidad. Correcciones menores.
2.0	31/01/2020	Revisión general del contenido de la PC con base en la legislación y normativa aplicable y el contenido de la documentación del Sistema de Gestión por parte de un equipo de trabajo multidisciplinar. Cambio del nombre del documento de “Política de Certificación de Certificados de Componente” a “Política de Certificados de Componente”. Cambios en la organización del contenido del documento para seguir recomendaciones del estándar RFC 3647. Se añade la posibilidad de que el Suscriptor pueda ser una Persona Natural que desempeñe una actividad económica del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario.

		Se añaden las posibilidades de que el Solicitante pueda ser una Corporación o Entidad Persona Natural distinta al Suscriptor y de que, en el caso de que haya dos Solicitantes, el primer Solicitante sea una Corporación o Entidad Persona Natural distinta al Suscriptor. Se describe con más detalle el caso en el que el Solicitante es una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta al Suscriptor, incluyendo las funciones del Operador de Grupo (OG) y del Administrador del certificado. Se elimina el No. de cuenta corriente para realizar el depósito de la cuantía respectiva a cada servicio (se indicará en la Propuesta Comercial).
2.1	19/06/2020	Correcciones menores.
2.2	06/11/2020	Se añade la posibilidad de que el certificado presentado por un Operador de Grupo (OG) en el acceso a la plataforma SAR pueda ser un certificado de Persona Natural, como alternativa a un certificado de Pertenencia a Empresa, emitido previamente al OG por la ECD en HSM Centralizado. Se añade la posibilidad de que el tipo de documento de identidad del Solicitante (Persona Natural) y del Representante Legal del Suscriptor (Persona Jurídica) o del propio Suscriptor (Persona Natural) sea el Pasaporte. Correcciones menores.

ÍNDICE

1 INTRODUCCIÓN

1.1 PRESENTACIÓN DEL DOCUMENTO

Este documento constituye la Política de Certificados (PC) de Componente emitidos por Thomas Signe S.A.S, en el marco del cumplimiento de los "Criterios Específicos de Acreditación Entidades de Certificación Digital - CEA-4.1-10" establecidos por el Organismo Nacional de Acreditación de Colombia – ONAC, conforme a la legislación colombiana y las disposiciones de los entes reguladores.

Los Certificados de Componente emitidos por Thomas Signe S.A.S son certificados que permiten identificar y firmar al Suscriptor como Corporación o Entidad (persona jurídica o persona natural, ya sea ésta una empresa, una organización pública o privada, un colegio profesional o la propia persona natural en el caso de que desempeñe una actividad económica sea ésta del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario) que se emiten para dispositivos informáticos, programas o aplicaciones dedicados a firmar en nombre de la Corporación o Entidad en sistemas de firma digital para la actuación administrativa automatizada.

Esta PC establece los requisitos particulares de los Certificados de Componente emitidos por Thomas Signe S.A.S, 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.

- ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal 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 Componente emitidos por Thomas Signe S.A.S. se rigen por las prácticas establecidas en la Declaración de Prácticas de Certificación (DPC) para la emisión de certificados de Thomas Signe S.A.S. Esta DPC se encuentra publicada en la misma página web de Thomas Signe S.A.S. que el presente documento (ver sección 1.2).

El presente documento es de carácter público y se encuentra dirigido a todas las personas naturales y jurídicas, Solicitantes, Suscriptores, 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 S.A.S se encargará de informar de tal hecho a ONAC, 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 los siguientes OID, contenidos en la extensión X.509 v3 Certificate Policies de los Certificados de Componente emitidos por Thomas Signe S.A.S. en los tipos de soporte indicados.

OID DE LA PC DE CERTICADOS DE COMPONENTE DE THOMAS SIGNE S.A.S.	
1.3.6.1.4.1.51362.0.2.1.4.3	Soporte HSM Centralizado
1.3.6.1.4.1.51362.0.2.1.4.2	Soporte Otros Dispositivos

Este documento se encuentra publicado en la siguiente página web:

https://thomas-signe.co/declaracion-de-practicas-y-politicas-de-certificacion/

1.3 PARTICIPANTES PKI DE THOMAS SIGNE S.A.S

1.3.1 JERARQUÍA DE CERTIFICADOS DE LA PKI DE THOMAS SIGNE S.A.S.

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

1.3.2 THOMAS SIGNE ROOT

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

1.3.3 ECD THOMAS SIGNE S.A.S. (ECD THOMAS SIGNE COLOMBIA)

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

1.3.4 SOLICITANTE

En esta PC, Solicitante es la persona natural o jurídica que solicita a la ECD Thomas Signe S.A.S. la emisión de un Certificado de Componente.

En el caso de que el Solicitante no sea la misma persona natural o jurídica que el Suscriptor, éste deberá firmar una autorización con los datos del Solicitante, como la persona natural o jurídica autorizada a solicitar y obtener su certificado.

En el caso de que el Solicitante sea una Corporación o Entidad (persona jurídica o persona natural) distinta al Suscriptor, el Solicitante deberá designar a una o varias personas naturales individuales (denominadas Operadores de Grupo) como responsables de ingresar los datos en el formulario de solicitud del certificado y de adjuntar los documentos solicitados. A su vez, el Operador de Grupo ingresará en el formulario de solicitud del certificado los datos de otra persona natural individual (que podrá ser él mismo) como Administrador del certificado, que será a quien se entregará el certificado, una vez que haya sido emitido.

1.3.5 SUSCRIPTOR

En esta PC, Suscriptor es la persona natural o jurídica a cuyo nombre la ECD Thomas Signe S.A.S. expide un Certificado de Componente 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 S.A.S. y habiendo firmado el respectivo Contrato de Suscripción con Thomas Signe S.A.S., acepta las condiciones del servicio de emisión de certificados prestado por éste.

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

En esta PC, Suscriptor es una Corporación o Entidad, ya sea ésta una empresa, una organización pública o privada, un colegio profesional o la propia persona natural en el caso de que desempeñe una actividad económica sea ésta del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario.

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 de Componente emitido por la ECD Thomas Signe S.A.S.

El Tercero que confía, a su vez, puede ser o no Solicitante y/o Suscriptor.

1.4 TIPOS DE SOPORTE Y USOS DE CERTIFICADOS

1.4.1 SOPORTE HSM CENTRALIZADO

La emisión de Certificados de Componente en HSM Centralizado se encuentra disponible para cualquier Suscriptor que cumpla con los requisitos establecidos en esta PC y en la DPC para la emisión de certificados de Thomas Signe S.A.S.

Las claves privadas de los Certificados de Componente emitidos en este soporte se generan y almacenan en un dispositivo criptográfico del tipo HSM Centralizado con certificación FIPS 140-2 nivel 3, dando lugar a un nivel de seguridad 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

El acceso a la clave privada de un Certificado de Componente emitido en este dispositivo criptográfico está protegido por una contraseña, definida por el Solicitante al generar las claves en el HSM Centralizado en el instante previo a la emisión del certificado, y por unos códigos proporcionados al Solicitante por la RA. Esta contraseña y estos códigos constituyen, por tanto, los datos de activación de la clave privada.

Los Certificados de Componente emitidos en HSM Centralizado están identificados mediante el OID (1.3.6.1.4.1.51362.0.2.1.4.3) en la extensión X.509 v3 Certificate Policies.

1.4.2 SOPORTE OTROS DISPOSITIVOS

La emisión de los Certificados de Componente en Otros Dispositivos se encuentra limitada al caso en el que un Solicitante entrega una petición de certificado en formato PKCS #10, que contenga una clave pública RSA de tamaño 2048 bits.

Para la emisión de los Certificados de Componente en este soporte, se contempla la posibilidad de que haya dos Solicitantes. El primer Solicitante será una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta al Suscriptor que entrega la petición de certificado en formato PKCS #10 y algunos datos del formulario de solicitud de certificado (ver Anexo I), mientras que el segundo Solicitante será una Persona Natural individual que completa los datos del formulario de solicitud de certificado y adjunta los documentos requeridos en la plataforma SAR (ver sección 4.1.4).

Las claves privadas de los Certificados de Componente emitidos en este soporte, asociadas a las claves publicas contenidas en las peticiones de certificado en formato PKCS #10 entregadas por los Solicitantes, habrán sido generadas y almacenadas en dispositivos criptográficos de cualquier tipo (software, HSM, token/tarjeta), conforme al nivel de seguridad que los Suscriptores consideren adecuado.

Estos dispositivos criptográficos podrán tener certificación FIPS 140-2 nivel 3, dando lugar a un nivel de seguridad 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

El acceso a la clave privada de un Certificado de Componente emitido en uno de estos dispositivos criptográficos está protegido mediante los datos específicos determinados por el tipo de dispositivo criptográfico utilizado, los cuales constituyen, por tanto, los datos de activación de la clave privada.

Los Certificados de Comonente emitidos en Otros Dispositivos están identificados mediante el OID (1.3.6.1.4.1.51362.0.2.1.4.2) en la extensión X.509 v3 Certificate Policies.

1.4.3 USOS APROPIADOS DE LOS CERTIFICADOS

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

Los Certificados de Componente pueden ser usados como mecanismo de identificación y autenticación en sistemas de firma electrónica para la actuación administrativa automatizada.

Se permite el uso de estos certificados en las relaciones personales del Suscriptor con las Administraciones Públicas.

1.4.4 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.S.

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.S.

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.S.

Adicionalemente, en esta PC las siguientes definiciones también son aplicables:

Administrador del certificado: persona natural individual a quien se entregará el certificado digital del Suscriptor, una vez que haya sido emitido. Es la misma persona natural que el Solicitante, excepto cuando éste es una Corporación o Entidad distinta al Suscriptor, en cuyo caso el Administrador del certificado será la persona natural individual con los datos ingresados por el Operador de Grupo en el formulario de solicitud del certificado.

Operador de Grupo: persona natural individual designada por una Corporación o Entidad distinta al Suscriptor como responsable de ingresar los datos en el formulario de solicitud del certificado y de adjuntar los documentos solicitados.

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 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.

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 estándades usados en las comunidades más amplias (ANSA, IEEE, ISO, etc).

HSM Hardware Security Module

IEC International Electrotechnical Commission

ISO International Organization for Standardization

ITU International Telecommunication Union

NIT Número de Identificación Tributaria

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

ONAC Organismo Nacional de Acreditación de Colombia

OG Operador de Grupo

OR Operador de Registro

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)

PQRSA Peticiones, Quejas, Reclamos, Sugerencias y Apelaciones

RA 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.

RUES Registro Único Empresarial y Social

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.S.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 NOMBRES

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

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 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.

Cuando el certificado se emite en Otros Dispositvos, el método de prueba de la posesión de la clave privada será la entrega a la RA de una petición de certificado en formato PKCS #10.

3.2.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA CORPORACIÓN O ENTIDAD

La RA verificará la identidad de la Corporación o Entidad (Persona Jurídica o Persona Natural) Suscriptor según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.S.

Adicionalmente, si el Solicitante es una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta al Suscriptor, la RA verificará la identidad de esta Entidad mediante los siguientes procedimientos:

- La firma previa de un Contrato de Prestación de Servicios entre la Entidad y Thomas Signe S.A.

- La verificación de la identidad de la persona natural individual (denominada Operador de Grupo u OG) designada por la Entidad como responsable de ingresar los datos en el formulario de solicitud de certificado y de adjuntar los documentos solicitados en la plataforma SAR, de la forma indicada en la sección 3.2.3. A su vez, el OG ingresará en el formulario de solicitud del certificado en la plataforma SAR los datos de otra persona natural individual (que podrá ser él mismo) como Administrador del certificado, que será a quien se entregará el certificado, una vez que haya sido emitido, mediante un proceso en el que el Administrador del certificado deberá pulsar en enlaces con códigos únicos que recibirá en la dirección de correo electrónico ingresada por el OG en el formulario de solicitud del certificado. La RA no verificará la identidad de este Administrador del certificado.

- La comprobación de los datos de la Entidad en la autorización firmada adjuntada por el OG en la solicitud de certificado en la plataforma SAR, por medio de la cual el Suscriptor autoriza a la Entidad a solicitar y obtener su certificado.

3.2.3 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA NATURAL INDIVIDUAL

La RA verificará de forma fehaciente la identidad de la Persona Natural individual Solicitante según lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.S.

Además, en el caso de los certificados de Componente cuyo Solicitante es una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta al Suscriptor, la RA verificará la identidad del OG designado por dicha Entidad (ver sección 3.2.2), mediante comprobación automática, en el acceso del OG a la plataforma SAR, del nombre y contraseña de usuario ingresados y del certificado presentado, el cual deberá ser un certificado de Pertenencia a Empresa o de Persona Natural emitido previamente al OG por la ECD en HSM Centralizado. Para poder presentar este certificado al acceder a la plataforma SAR, el OG deberá ingresar su usuario y contraseña de acceso al HSM Centralizado, y después, como datos de activación de la clave privada, una contraseña, definida por él al generar las claves en el HSM Centralizado en el instante previo a la emisión del certificado, y un código que el OG recibirá en su teléfono celular.

3.2.4 INFORMACIÓN DE SUSCRIPTOR Y SOLICITANTE NO VERIFICADA

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

La RA no verificará los siguientes datos del Suscriptor y del Solicitante ingresados en el formulario de solicitud del certificado en la plataforma SAR, por otros medios que no sean la comprobación de los mismos en la correspondiente autorización firmada, por la cual el Suscriptor autoriza al Solicitante a solicitar y obtener el certificado, en los casos que se requiera dicha autorización, presumiendo la buena fe de la información aportada por el Solicitante:

- En todos los casos: nombre descriptivo de la aplicación, área y correo electrónico del Suscriptor (contenidos en el certificado). En los casos que se requiera una autorización firmada al Solicitante, sea éste una Persona Natural independiente o una Entidad (Persona Jurídica o Persona Natural), la RA comprobará que los datos ingresados en el formulario de solicitud del certificado son conformes a los datos en dicha autorización.

- En los casos en los que el Solicitante es una Persona Natural independiente: celular y correo electrónico del Solicitante y Administrador del certificado (no contenidos en el certificado). En los casos que se requiera una autorización firmada al Solicitante, la RA comprobará que los datos ingresados en el formulario de solicitud del certificado son conformes a los datos en dicha autorización.

- En los casos en los que el Solicitante es una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta al Suscriptor, todos los datos del Administrador del certificado ingresados en el formulario de solicitud del certificado en la plataforma SAR por el OG designado por el Solicitante (no contenidos en el certificado). La RA no realizará ninguna comprobación de los datos ingresados en el formulario de solicitud del 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.S.

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.S.

La identificación y autenticación del Suscriptor o Solicitante, en el caso de que éste utilice el procedimiento de revocación online, a través de los enlaces contenidos en la página web de Thomas Signe S.A.S., se realiza según el método siguiente, dependiendo del tipo de soporte en el que haya sido emitido el certificado:

- HSM Centralizado: el Suscriptor o Solicitante deberá ingresar su usuario y contraseña de acceso al HSM Centralizado, y un código que recibirá en su teléfono celular.

- Otros Dispositivos: el Suscriptor o Solicitante deberá ingresar el código de revocación proporcionado en la entrega 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

Pueden solicitar un Certificado de Componente:

1) El Representante Legal del Suscriptor que sea Persona Jurídica.

2) El Suscriptor que sea Persona Natural.

3) Una Persona Natural individual (no Corporación o Entidad) autorizada por 1) o 2) para solicitar y obtener el certificado del Suscriptor.

4) Una Corporación o Entidad (Persona Jurídica o Persona Natural) autorizada por 1) o 2) para solicitar y obtener el certificado del Suscriptor.

En el caso de que el único Solicitante sea 4), éste deberá designar a una o varias Personas Naturales individuales (denominadas Operadores de Grupo) como responsables de ingresar los datos en el formulario de solicitud del certificado y de adjuntar los documentos solicitados. A su vez, el Operador de Grupo ingresará en el formulario de solicitud del certificado los datos de otra Persona Natural individual (que podrá ser él mismo) como Administrador del certificado, que será a quien se entregará el certificado, una vez que haya sido emitido.

4.1.2 COMERCIALIZACIÓN

El Solicitante y/o el Suscriptor podrán recibir información acerca del proceso de certificación digital de las siguientes maneras:

- Consultando la página web www.thomas-signe.co

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

- El trato directo con Agentes comerciales.

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

Luego de ser informado, si el Solicitante es una Persona Natural individual, el Solicitante y/o el Suscriptor indicarán al Área Comercial y/o a un OR:

1) El tipo de certificado y el tipo de soporte requeridos (Certificado de Componente en HSM Centralizado o en Otros Dispositivos).

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 corporativa del Solicitante que estará asociada al certificado digital y por medio de la cual la ECD le realizará notificaciones y comunicaciones oficiales.

6) El nombre o la razón social del Suscriptor.

7) El NIT del Suscriptor.

Si el Solicitante es una Persona Natural individual, el Área Comercial y/o un OR enviarán por correo electrónico al Solicitante y/o al Suscriptor: la Propuesta Comercial (enviada por el Área Comercial), en los casos que sea aplicable; el Contrato de Suscripción; un modelo de autorización para la solicitud y obtención del certificado en el caso de que se requiera; opcionalmente, un enlace a la plataforma SAR; y las indicaciones respectivas.

4.1.3 CONTRATACIÓN Y PAGO

Para proceder con la contratación y el pago, el Solicitante y/o el Suscriptor deberán:

- 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.S. pone a disposición del público una cuenta bancaria para realizar el depósito de la cuantía respectiva a cada servicio (ver sección 9.1). En la Propuesta Comercial se indicarán los datos de esta cuenta bancaria. No obstante, Thomas Signe S.A.S. 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 S.A.S. y el Suscriptor, mediante la firma respectiva. La evidencia de este proceso será el Contrato de Suscripción firmado.

- Si el Solicitante es una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta al Suscriptor, aprobar todos los términos y condiciones dispuestos en un Contrato de Prestación de Servicios entre Thomas Signe S.A.S. y el Solicitante, mediante la firma respectiva. La evidencia de este proceso será el Contrato de Prestación de Servicios firmado.

- Si el Solicitante es una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta al Suscriptor, designar una o varias Personas Naturales individuales (Operadores de Grupo) como responsables de ingresar los datos en el formulario de solicitud del certificado y de adjuntar los documentos solicitados en la plataforma SAR.

4.1.4 SOLICITUD

Para solicitar la emisión de un certificado digital, el Solicitante y/o el Suscriptor deberán ingresar a la plataforma SAR y completar correctamente los datos del formulario de la solicitud de certificado (ver Anexo I). Además, dentro de la plataforma SAR, procederán a adjuntar los documentos indicados a continuación:

- En los casos que el Solicitante sea una Persona Natural individual, documento de identidad del Solicitante, escaneado por ambas caras: Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte; expedido en Colombia (por defecto) o en otro país (documento equivalente).

- Certificado de Cámara de Comercio o documento equivalente del Suscriptor, en copia virtual o escaneado, en los casos que sea aplicable; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.

- Registro Único Tributario o documento equivalente del Suscriptor, en copia virtual o escaneado, en todos los casos; expedido en Colombia (por defecto) o en otro país.

- Documento oficial adicional en el que conste una dirección completa actual del Suscriptor (por ejemplo, un Certificado de Residencia para Personas Naturales), en el caso de que el Solicitante desee que figure en el certificado una dirección distinta a las incluidas en el Certificado de la Cámara del Comercio y/o en el Registro Único Tributario o documentos equivalentes; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.

- En los casos que el Solicitante no sea el Representante Legal del Suscriptor (Persona Jurídica) ni el propio Suscriptor (Persona Natural), o haya dos Solicitantes (ver sección 1.4.2):

  - Autorización firmada por el Representante Legal del Suscriptor (Persona Jurídica) o por el propio Suscriptor (Persona Natural), con los datos de la Persona Natural individual o de la Corporación o Entidad (Persona Jurídica o Persona Natural) autorizada a solicitar y obtener un Certificado de Componente; expedida un máximo de 30 días antes.

  - Documento de identidad del Representante Legal o del propio Suscriptor (Persona Natural) que firma la autorización, escaneado por ambas caras: Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte; expedido en Colombia (por defecto) o en otro país (documento equivalente).

- Constancia del pago de la tarifa del certificado indicada en la Propuesta Comercial, en los casos que sea aplicable.

- Contrato de Suscripción firmado.

Adicionalmente, en el caso de que el tipo de soporte sea Otros Dispositivos, el Solicitante deberá adjuntar en la plataforma SAR la petición de certificado en formato PKCS #10, a no ser que haya dos

Solicitantes en cuyo caso ya se habrá adjuntado dicha petición en la plataforma SAR una vez enviada por el primer Solicitante.

Alternativamente, el Solicitante y/o el Suscriptor podrán 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

Un OR 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 Suscriptor, al Solicitante, 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 y/o en el Contrato de Prestación de Servicios. Se aceptará discrepancia únicamente para la dirección completa del Suscriptor contenida en el Certificado de la Cámara de Comercio y/o en el Registro Único Tributario y/o en el documento oficial adicional, en cuyo caso se considerará como válida la dirección contenida en el documento con fecha de expedición más reciente.

Además, para aquellos casos en los que sea posible, el OR consultará el NIT del Suscriptor en una Base de datos online (en Colombia, para las empresas del tipo Persona Jurídica o Persona Natural, Base de datos RUES), para verificar la existencia de la Entidad y que se encuentra activa.

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

Una vez recolectada y revisada satisfactoriamente toda la documentación y evidencias requeridas, si el Solicitante es una Persona Natural individual, el OR coordinará con él una cita para realizar una videoconferencia. En dicha sesión, el OR hará una serie de preguntas para verificar la identidad del Solicitante y le solicitará que le muestre el documento de identidad original que ha enviado escaneado, para comprobar que coincide con el documento recibido. A fin de evidenciar dicha videoconferencia, la plataforma de la RA grabará toda la sesión y se guardará la grabación junto a la información recabada del Solicitante. Este proceso será realizado previamente a la emisión del certificado.

Alternativamente a la videoconferencia, un OR podrá haber verificado la identidad del Solicitante, si éste es una Persona Natural individual, de forma presencial, en cuyo caso deberá haber recibido del Solicitante los documentos requeridos, 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), entre los cuales se incluirán obligatoriamente el Contrato de Suscripción firmado por el Suscriptor y, en los casos que sea aplicable, la autorización firmada con los datos de la Persona Natural autorizada a solicitar el certificado.

Una vez que el OR ha validado los documentos presentados y los datos ingresados en el formulario de solicitud de certificado y que, en el caso de que el Solicitante sea una Persona Natural individual, ha verificado su identidad, el OR aprobará la solicitud de emisión en la plataforma de la RA.

Si la información o verificación de identidad no fuese correcta, la RA deberá denegar la petición, contactando al Solicitante y al Sucriptor para comunicarles el motivo.

4.2.2 DECISIÓN

La ECD Thomas Signe S.A.S. 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 ECD se encarga de comunicar el motivo del rechazo al Solicitante y al Sucriptor.

4.3 EMISIÓN DE CERTIFICADOS

4.3.1 ACCIONES DE LA ECD DURANTE LA EMISIÓN DE CERTIFICADOS

Una vez aprobada la solicitud, se procederá a la emisión del certificado, durante la cual la ECD Thomas Signe S.A.S. (RA y CA Subordinada) realiza las siguientes acciones:

1) Las claves serán generadas por el Solicitante en el HSM Centralizado o habrán sido generadas previamente en sistemas del Suscriptor o del Solicitante utilizando aplicaciones compatibles con los estándares de PKI, haciendo entrega a la RA, en ambos casos, de una petición de certificado en formato PKCS #10.

2) La RA firmará la petición de certificado en formato PKCS #10 recibida 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 el caso de que el tipo de soporte sea HSM Centralizado, este proceso será realizado automáticamente al recibir la RA la petición de certificado en formato PKCS #10, sin intervención de un OR.

- En el caso de que el tipo de soporte sea Otros Dispositivos, este proceso será realizado automáticamente en el momento en el que un OR genera el certificado.

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 Solicitante.

- En el caso de que el tipo de soporte sea Otros Dispositivos, la RA enviará automáticamente al Solicitante un mensaje de correo electrónico conteniendo un enlace que le permitirá la descarga del certificado y un código de revocación aleatorio.

4.3.2 NOTIFICACIÓN AL SOLICITANTE Y AL SUSCRIPTOR POR LA ECD DE LA EMISIÓN DEL CERTIFICADO

En el caso de que el tipo de soporte sea HSM Centralizado, el propio HSM Centralizado notifica al Solicitante que el certificado ha sido emitido y que ha sido instalado en el HSM.

En el caso de que el tipo de soporte sea Otros Dispositivos, la RA notifica al Solicitante la emisión del certificado en el mismo correo electrónico en el que le envía el enlace que le permitirá su descarga y un código de revocación aleatorio.

Después, en ambos casos, la RA envía un correo electrónico al Solicitante y al Suscriptor que incluye información sobre el contenido del certificado, la página web donde se encuentran publicadas la DPC y PC, así como, en el caso de que el tipo de soporte sea HSM Centralizado, 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 Suscriptor, una vez que la RA ha realizado su entrega y la ECD ha notificado la misma al Solicitante y al Suscriptor, según lo especificado en las secciones 4.3.1 y 4.3.2.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR LA ECD

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

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

La ECD Thomas Signe S.A.S. 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.S.

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.S.

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.S.

4.8 MODIFICACIÓN DE CERTIFICADOS

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

4.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

El Suscriptor o el Solicitante deberá solicitar la revocación del 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.S.

Para solicitar la revocación del certificado el Suscriptor o el Solicitante puede:

- Revocar online el certificado a través de los enlaces contenidos en la página web de Thomas Signe S.A.S. En el caso de que el tipo de soporte sea Otros Dispositivos, el Suscriptor o el Solicitante deberá ingresar el código de revocación proporcionado en la entrega del certificado. En el caso de que el tipo de soporte sea HSM Centralizado, el Suscriptor o el Solicitante deberá ingresar su usuario y contraseña de acceso al HSM Centralizado, y un código que recibirá en su teléfono celular.

- De forma alternativa, el Solicitante o el Suscriptor que desee revocar su certificado digital, podrá comunicarse con el Responsable de PQRSA de la ECD Thomas Signe S.A.S. enviando la solicitud de revocación a la dirección de correo electrónico pqrsa@thsigne.com, la cual será derivada a un Operador de Registro. 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.S. se encuentra toda la información complementaria referente a la revocación de los certificados

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.S.

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.S.

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.S.

6 CONTROLES TÉCNICOS DE SEGURIDAD

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

7 PERFILES 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 Componente cumple lo especificado en la DPC para la emisión de certificados de Thomas Signe S.A.S.

Los Certificados de Componente tienen un periodo de validez de hasta 2 años (730 días).

7.1.2 EXTENSIONES DEL CERTIFICADO

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

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 1.3.6.1.4.1.51362.0.2.1.4.x [1] URI de la DPC: http://thsigne.com/cps
Subject Alternative Name		rfc822Name: un *correo electrónico corporativo de la Entidad (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

7.1.3 IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

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

[1] Otros Dispositivos (PKCS #10): x=2; HSM Centralizado: x=3

7.1.4 FORMATOS DE NOMBRES

En la tabla siguiente se especifican los correspondientes atributos del DN del titular de un Certificado de Componente (Suscriptor del certificado).

Atributo del DN	Descripción	Valor
Country Name (C)	País	*Código de dos letras mayúsculas según ISO 3166-1 del país de la Entidad* [1] Por defecto: CO
State or Province Name (ST)	Estado/Provincia	*Departamento de la Entidad* [2]
Locality Name (L)	Localidad	*Municipio de la Entidad* [2]
Street Address (STREET)	Dirección	*Dirección de la Entidad* [2]
Organization Identifier (2.5.4.97)	Identificador de Organización	Número de identificación fiscal de la *Entidad* (en Colombia: *NIT*) [2]
Organization Name (O)	Nombre de Organización	*Nombre o Razón social de la Entidad* [2]
Organization Unit Name (OU)	Unidad Organizativa	*Área de la Entidad en la que se encuentra el sistema o texto libre* [2]
Common Name (CN)	Nombre	*Nombre del sistema o proceso de firma* [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.S.

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

Los OID de la Política de Certificados de Componente se encuentran especificados en las secciones 1.2, 1.4 y 7.1.2, así como en la DPC para la emisión de certificados de Thomas Signe S.A.S.

7.1.7 USO DE LA EXTENSIÓN POLICY CONSTRAINTS

Los Certificados de Componente no contienen la extensión Policy Contraints.

---

[1] Codificado en PrintableString

[2] Codificado en UTF8String

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.S.

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.S.

7.2 PERFIL DE CRL

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

7.3 PERFIL DE OCSP

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

8 AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

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

9 OTROS ASUNTOS LEGALES Y COMERCIALES

9.1 TARIFAS

9.1.1 TARIFAS DE EMISIÓN DE CERTIFICADOS

Las tarifas especificadas son referenciales, por lo que pueden variar de acuerdo al tipo de certificado y al contrato establecido con cada cliente.

CERTIFICADO	PRECIO*
Componente	1 000 000 pesos colombianos

*Precio sin IVA para un certificado de 2 años de vigencia

Las mismas tarifas se encuentran publicadas en la página Web de Thomas Signe S.A.S.

En la propuesta comercial se 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.S y los clientes de los servicios ofrecidos.

9.1.5 POLÍTICA DE REEMBOLSO

La ECD Thomas Signe S.A.S. dispone de una Política de reembolso (THS-CO-AC-POL-07 Política de reembolso), que se referencia en los contratos celebrados con sus clientes y se publica en la página web de Thomas Signe.

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.S.

9.3 CONFIDENCIALIDAD DE LA INFORMACIÓN

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

9.4 POLÍTICA DE PROTECCIÓN DE DATOS

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

9.5 DERECHOS DE PROPIEDAD INTELECTUAL

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

9.6 OBLIGACIONES

9.6.1 OBLIGACIONES DE LA ECD

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

9.6.2 OBLIGACIONES DE LOS PROVEEDORES

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

9.6.3 OBLIGACIONES DE LOS SOLICITANTES

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

9.6.4 OBLIGACIONES DE LOS SUSCRIPTORES

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

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.S.

9.7 RESPONSABILIDADES

9.7.1 RESPONSABILIDADES DE LA ECD

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

9.7.2 RESPONSABILIDADES DEL SUSCRIPTOR

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

9.8 LIMITACIÓN DE RESPONSABILIDAD

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

9.9 INDEMNIZACIONES

9.9.1 INDEMNIZACIONES POR DAÑOS OCASIONADOS POR LA ECD

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

9.9.2 INDEMNIZACIONES POR LOS DAÑOS CAUSADOS POR LOS SOLICITANTES, POR LOS SUSCRIPTORES Y POR LOS TERCEROS QUE CONFÍAN

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

9.10 PERIODO DE VALIDEZ

9.10.1 PLAZO

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

9.10.2 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.S.

9.10.3 EFECTOS DE LA FINALIZACIÓN

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

9.11 PQRSA

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

9.12 CAMBIOS EN DPC Y PC

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

9.13 RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

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

9.14 LEY APLICABLE

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

9.15 CONFORMIDAD CON LA LEY APLICABLE

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

9.16 ESTIPULACIONES DIVERSAS

9.16.1 CONTRATO DE SUSCRIPCIÓN

El Contrato de Suscripción para el servicio de emisión de certificados vigente se encuentra publicado en la siguiente página web:

https://thomas-signe.co/declaracion-de-practicas-y-politicas-de-certificacion/

Se usa el mismo modelo de contrato para todos los tipos de certificados. En el contrato se deberán rellenar el tipo de certificado contratado y su vigencia.

En el caso de Certificados de Componente, si el Suscriptor es una Persona Jurídica, el contrato podrá ser firmado por su Representante Legal.

9.16.2 CLÁUSULA DE ACEPTACIÓN COMPLETA

Todos los Solicitantes, Suscriptores, 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.

9.16.3 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.

9.17 OTRAS ESTIPULACIONES

No se contemplan.

10 FORMATOS

THS-CO-AC-DPC-01-F01 Formulario de Solicitud de Certificado de Componente

THS-CO-AC-DPC-01-F08 Propuesta Comercial de Certificados Digitales - Componente

THS-CO-AC-DPC-01-F09 Contrato de Suscripción para Emisión de Certificados

THS-CO-AC-DPC-01-F10 Autorización Solicitud Certificado de Componente - Persona Natural

THS-CO-AC-DPC-01-F12 Autorización Solicitud Certificado de Componente - Otra Entidad

THS-CO-AC-DPC-01-F13 Autorización Solicitud Previa Certificado de Componente - Otra Entidad

THS-CO-AC-DPC-01-F14 Contrato de Prestación de Servicios para el Suministro de Certificados Digitales de Componente

THS-CO-AC-DPC-01-F15 Protocolo lectura videoconferencia verificación identidad

11 REGISTROS

IDENTIFICACIÓN	SOPORTE	RESPONSABLE	ARCHIVO	TIEMPO DE CONSERVACIÓN
Formularios completos de Solicitud de Certificado de Componente	Informático	Operador de Registro	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Propuestas comerciales firmadas de Certificados Digitales - Componente	Informático	Gerente Comercial	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Contratos firmados de Suscripción para Emisión de Certificados	Informático	Operador de Registro	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Autorizaciones firmadas Solicitud Certificado de Componente	Informático	Operador de Registro	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Contratos firmados de Prestación de Servicios para el Suministro de Certificados Digitales de Componente	Informático	Operador de Registro	Plataforma SAR	3 años o de acuerdo a normativa aplicable
Videoconferencias grabadas verificación identidad	Informático	Operador de Registro	Plataforma de la RA	3 años o de acuerdo a normativa aplicable

12 ANEXOS

12.1 ANEXO I: FORMULARIO DE SOLICITUD DE CERTIFICADO DE COMPONENTE

Datos del Administrador (Persona Natural)	
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*
Celular	*Completar el Número de celular del Administrador*
Correo electrónico	*Completar el Correo electrónico del Administrador*

Datos de la Entidad - Suscriptor (Persona Jurídica o Natural)	
Nombre descriptivo de la aplicación	*Completar la Denominación del sistema o proceso de firma*
Nombre o Razón social	*Completar el Nombre o Razón social de la Persona Jurídica o los Nombres y Apellidos de la Persona Natural*
NIT	*Completar el Número de Identificación Tributaria de la Entidad*
País	*Completar el País donde se localiza la Entidad*
Estado/Provincia	*Completar el Departamento donde se localiza la Entidad*
Localidad	*Completar el Municipio donde se localiza la Entidad*
Dirección	*Completar la Dirección exacta donde se localiza la Entidad*
Área	*Completar el Área de la Entidad en la que se encuentra el sistema o un texto libre*
Correo electrónico	*Completar un Correo electrónico corporativo de la Entidad*