Entidad de Certificación

THOMAS SIGNE

SOLUCIONES TECNOLÓGICAS GLOBALES

Política de Certificación
de Certificados de Agente Automatizado

THOMAS SIGNE
SOLUCIONES TECNOLÓGICAS GLOBALES

Firmado digitalmente por ALVARO HERNANDO GUTIERREZ VILLATE
Fecha: 2020.06.29 09:20:45 -05'00'

Información del documento

Nombre	PC de Certificados de Agente Automatizado
Realizado por	Thomas Signe Perú
País	Perú
Versión	2.1
Fecha	Junio del 2020
Tipo de documento	Público
Código	**THS-PE-AC-PC-COR-03**

Historial de versiones

Versión	Fecha	Descripción
1.0	02/10/2017	Elaboración de documento inicial.
2.0	27/05/2019	Se cambia el nombre del documento (antes "Política de Certificación de Certificados de Sello de Órgano"). Se cambia el código del documento (antes THS-PE-PC-SO-01). Se modifica la estructura del documento. Transcripción del documento de SIGNE "PC Certificados Corporativos de Sello Electrónico versión 1.3". Se añade la sección 0 con particularides de la EC Thomas Signe.
2.1	29/06/2020	Ajuste de la codificación del documento.

		Transcripción del documento de SIGNE "PC Certificados Corporativos de Sello Electrónico versión 1.4". En el proceso de emisión de certificados, se añade una excepción a la identificación presencial del Solicitante y del Custodio de Claves. Correcciones menores.

ÍNDICE

0 ENTIDAD DE CERTIFICACIÓN THOMAS SIGNE (EC THOMAS SIGNE)

0.1 PRESENTACIÓN

Signe S.A. (en adelante 'Signe') es una empresa con domicilio en España que brinda principalmente servicios consistentes en la edición e impresión de documentos de seguridad para empresas públicas y privadas. A partir del año 2010, Signe inicia su actividad como Prestador de Servicios de Certificación (PSC) que emite certificados reconocidos según la Ley 59/2003, de 19 de diciembre, de firma electrónica en España.

Desde hace más de 30 años, Signe se ha especializado en el diseño y desarrollo de soluciones de seguridad documental, produciendo y editando documentos -tanto en soporte papel como digital- protegidos contra posibles falsificaciones y modificaciones fraudulentas.

Hoy en día, gracias a una constante inversión en tecnología punta y la aplicación de estrictos controles de calidad, Signe se posiciona como un referente dentro del sector a nivel europeo y, cada vez más, también a nivel mundial.

En el año 2018, en una alianza comercial entre Signe y Thomas Greg & Sons de Perú, se ha creado la empresa Thomas Signe de Perú S.A. (en adelante 'Thomas Signe'), para actuar como Entidad de Certificación, Entidad de Registro, Software de Firma Digital y Servicios de Valor Añadido como Sistema de Intermediación Digital y Autoridad de Sellado de Tiempo (Timestamp); y así brindar dichos servicios en Perú y dar cumplimiento a la regulación peruana establecida por la Autoridad Administrativa Competente (AAC), INDECOPI.

Como Entidad de Certificación Digital - EC, Thomas Signe provee servicios de emisión, re-emisión, distribución y revocación de certificados digitales.

La infraestructura tecnológica y operativa de la EC de Thomas Signe es provista por Signe. Dicha infraestructura ha obtenido la cualificación eIDAS y es verificada anualmente por auditores autorizados.

Junto a los servicios de certificación digital, Thomas Signe brinda los servicios de registro o verificación de sus clientes, tanto en el caso de personas jurídicas como naturales, además de servicios de valor añadido de intermediación digital y sellado de tiempo.

0.2 TRANSCRIPCIÓN DE DOCUMENTO DE SIGNE

El presente documento es una transcripción realizada por Thomas Signe del documento original de Signe "PC Certificados Corporativos de Sello Electrónico" vigente publicado en https://www.signe.es/signe-ac/dpc, en la que se han realizado los siguientes cambios:

- Se ha modificado la estructura del documento para ser conforme al Sistema de Gestión de Documentación de Thomas Signe.
- Se ha añadido una sección 0 donde se describen las particularidades de Thomas Signe como Entidad de Certificación (EC Thomas Signe) conforme al marco legal de firmas y certificados digitales en Perú, cuyo contenido no entra en contradicción con el del resto del documento.

0.3 OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas que utiliza Thomas Signe para la administración de sus servicios como Entidad de Certificación Digital – EC, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI, en calidad de Autoridad Administrativa Competente de la Infraestructura Oficial de la Firma Electrónica del Perú.

0.4 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura de servicios de certificación digital brindados por Thomas Signe a través de Signe, la cual cuenta con la cualificación eIDAS.

Signe, como proveedor de infraestructura y responsable de la gestión de operaciones de los servicios de la EC de Thomas Signe, asume todos los aspectos de responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano y los servicios de certificación digital provistos por la EC de Thomas Signe.

0.5 DEFINICIONES Y ABREVIACIONES

La tabla siguiente muestra, para una serie de términos establecidos en el marco legal de firmas y certificados digitales en Perú, su nombre, abreviatura y definición en dicho marco legal, así como sus particularides en Thomas Signe como Entidad de Certificación (EC Thomas Signe) y el nombre, abreviatura y definición del término correspondiente indicado en el resto del documento (transcripción del documento de Signe indicado en el apartado 0.2).

Término Marco Legal Perú	**Definición Marco Legal Perú**	**Particularidades EC Thomas Signe**	**Término Documento (Signe)**
Entidad de Certificación - EC	Persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.	Thomas Signe, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital, de acuerdo con los términos y condiciones de los servicios establecidos y publicados en el presente documento y en la Declaración de Prácticas de Certificación. A Thomas Signe, como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante la ACC a fin de poder ingresar a la IOFE.	Autoridades de Certificación – CA *(ver definición en apartado 2.1)*
Entidad de Registro - ER	Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.	Thomas Signe, brinda también los servicios de Entidad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro, de acuerdo con los términos y condiciones de los servicios establecidos y publicados en el presente documento y en la Declaración de Prácticas de Certificación.	Autoridad de Registro – RA *(ver definición en apartado 2.2)*
Titular	Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.	Persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo, con conocimiento y	Suscriptor *(ver definición en apartado 2.4)*

	Dentro de la Infraestructura Oficial de Firma Electrónica, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado. Tratándose de personas naturales, éstas son titulares y suscriptores del certificado digital. En el caso de personas jurídicas, éstas son titulares del certificado digital.	plena aceptación de los derechos y deberes establecidos y publicados en el presente documento y en la Declaración de Prácticas de Certificación.	
Suscriptor	Persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.	Persona natural responsable de la generación y uso de la clave privada, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en el presente documento y en la Declaración de Prácticas de Certificación.	Custodio de claves *(ver definición en apartado 2.6)*
Solicitante	En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular y	Persona natural que solicita los servicios provistos por la EC, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en el presente documento y en la	Solicitante *(ver definición en apartado 2.3)*

	suscriptor del certificado digital. En el caso de personas jurídicas, la solicitud del certificado digital y el registro o verificación de su identidad deberán realizarse a través de un representante debidamente acreditado.	Declaración de Prácticas de Certificación.	
Tercero que confía o tercer usuario	Personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.	Persona natural, equipo, servicio o cualquier ente que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en el presente documento y en la Declaración de Prácticas de Certificación.	Tercero que confía en los certificados *(ver definición en apartado 2.7)*

0.6 TIPO DE CERTIFICADOS

El tipo de certificados emitidos por Thomas Signe "Certificados de Agente Automatizado" se corresponde con el tipo de certificados emitidos por Signe "Certificados Corporativos de Sello Electrónico" indicado en el resto del documento (transcripción del documento de Signe indicado en el apartado 0.2).

0.7 SERVICIOS DE CERTIFICACIÓN DIGITAL

Thomas Signe brinda los servicios de emisión, re-emisión, revocación y distribución de los certificados digitales.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritos en la Declaración de Prácticas y las Políticas de Certificación de Thomas Signe publicadas en la página web:

www.thomas-signe.pe

0.8 TARIFAS

0.8.1 TARIFAS DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

Las tarifas relativas a los servicios de certificación digital de Thomas Signe se indican directamente con los clientes mediante correo electrónico o por vía telefónica.

0.8.2 TARIFAS DE ACCESO A LA INFORMACIÓN DE ESTADO

El acceso a la consulta del estado de los certificados emitidos, es libre y gratuito y, por tanto, no aplica una tarifa.

0.8.3 TARIFAS DE REVOCACIÓN

No se establece ninguna tarifa para la revocación de certificados.

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL

Los Certificados Corporativos de Sello Electrónico son certificados reconocidos, en los términos de la Ley 59/2003, 19 de diciembre, de firma electrónica (en adelante, "Ley 59/2003") y cualificados de sello electrónico, según el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, "Reglamento eIDAS"), que identifican al Suscriptor y Creador del sello como una Corporación con personalidad jurídica.

La finalidad de estos certificados es poder firmar en nombre de la organización documentos electrónicos de manera automática. Estos certificados tienen como objetivo cumplir las mismas funciones que realizan los "Sellos de Empresa" en los documentos en papel.

Estos certificados se ajustan a los requisitos que impone la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público y han sido autorizados para su utilización en facturación electrónica y digitalización certificada por la Agencia Tributaria.

En el presente documento se exponen las Condiciones Particulares referentes a este tipo de certificado. Esta Política de Certificación está subordinada al cumplimiento de la Declaración de Prácticas de Certificación (DPC) de SIGNE.

El presente documento es una adaptación de la Política de Certificación "PC Sello Empresarial" (OID 1.3.6.1.4.1.13177.10.1.10.2) de Firmaprofesional para SIGNE Autoridad de Certificación. Ambas políticas comparten aspectos como las características de los certificados, procedimientos y perfiles, y se diferencian en el alcance (siendo la presente más limitada) y en qué Autoridad de Certificación emite los certificados.

1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre	PC Certificados Corporativos de Sello Electrónico
Código	SIGNE-ES-AC-PC-COR-04
Versión	1.4
Descripción	Política de Certificación de Certificados Corporativos de Sello Electrónico
Fecha de emisión	19/03/2020
OIDs	1.3.6.1.4.1.36035.1.5.1 – Dispositivo Cualificado de Creación de Sello portable (DCCS portable) - Nivel Alto 1.3.6.1.4.1.36035.1.5.3 – Dispositivo Cualificado de Creación de Sello centralizado (DCCS centralizado) - Nivel Alto 1.3.6.1.4.1.36035.1.5.2 – Otros dispositivos - Nivel Medio
Localización	https://www.signe.es/signe-ac/dpc

1.3 DEFINICIONES Y ACRÓNIMOS

Las definiciones y acrónimos se pueden encontrar especificadas en el documento "Declaración de Prácticas de Certificación (DPC)" en https://www.signe.es/signe-ac/dpc/

2 ENTIDADES PARTICIPANTES

2.1 AUTORIDADES DE CERTIFICACIÓN (CA)

Los Certificados Corporativos de Sello Electrónico son emitidos por "SIGNE Autoridad de Certificación", CA Subordinada de la CA Raíz de Firmaprofesional.

2.2 AUTORIDAD DE REGISTRO (RA)

La gestión de las solicitudes y emisiones de los certificados será realizada por SIGNE o por entidades que actúen como Intermediarios de SIGNE.

Adicionalmente, la propia Corporación (empresa, entidad privada o públicas) podrá actuar como Autoridad de Registro de SIGNE para la gestión de las solicitudes y emisiones de los certificados. La propia Corporación será el Suscriptor de todos estos certificados emitidos.

Cada Corporación que actúe como RA establecerá:

- Qué criterios se deben cumplir para solicitar un certificado, sin entrar en contradicción con lo estipulado en la DPC y la presente PC.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del Custodio de claves, cumpliendo con lo estipulado en la DPC.
- Los dispositivos de creación de sello a utilizar, que previamente SIGNE haya homologado.

2.3 SOLICITANTE

El Solicitante es el representante legal o voluntario (apoderado general) de la Corporación (empresa, entidad privada o pública) que adquiere los certificados.

2.4 SUSCRIPTOR

El suscriptor de este tipo de certificados es la persona jurídica que consta en el certificado.

2.5 CREADOR DEL SELLO

El Creador del sello es la persona jurídica que consta en el certificado.

De acuerdo con el Reglamento eIDAS, el Creador del sello es la persona jurídica que crea el sello electrónico.

2.6 CUSTODIO DE CLAVES

La custodia de los datos de creación de sello asociados a cada certificado corporativo de Sello Electrónico será responsabilidad de la persona física Solicitante o de otra persona física autorizada por el Solicitante.

La identidad del custodio de claves es verificada de forma indubitada por la Autoridad de Registro, que conserva la documentación acreditativa correspondiente, a disposición de los órganos judiciales, cuando actúen en el ejercicio de las funciones que tienen atribuidas y de las autoridades competentes en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal, cuando así se requiera.

2.7 TERCERO QUE CONFÍA EN LOS CERTIFICADOS

Estos certificados son certificados reconocidos/cualificados que cumplen los requisitos que establecen la Ley 59/2003 y el Reglamento eIDAS.

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso, tanto cuantitativas como cualitativas, que se contienen en la DPC y en la presente PC.

3 CARACTERÍSTICAS DE LOS CERTIFICADOS

3.1 PERIODO DE VALIDEZ DE LOS CERTIFICADOS

Los certificados Corporativos de Sello Electrónico tendrán un periodo de validez de 1, 2 ó 3 años.

3.2 TIPOS DE SOPORTE

Los Certificados Corporativos de Sello Electrónico se emitirán en dos tipos de soporte en función de dónde se cree y resida el par de claves, dando lugar a dos niveles de aseguramiento:

- Dispositivo Cualificado de Creación de Sello (DCCS): Nivel Alto
- Otros dispositivos: Nivel Medio

La Corporación decidirá el tipo de soporte en el que emite sus certificados.

3.2.1 DISPOSITIVO CUALIFICADO DE CREACIÓN DE SELLO (DCCS)

Las claves privadas de los certificados emitidos en DCCS se generan y almacenan en un dispositivo cualificado de creación de sello (DCCS) como una tarjeta o un dispositivo criptográfico que ofrece, al menos, las garantías indicadas en el artículo 24 de la Ley 59/2003, y en el Anexo II del Reglamento eIDAS mutatis mutandis a los requisitos de los dispositivos cualificados de creación de sello electrónico.

Esta condición se indicará en el propio certificado mediante los siguientes campos:

Para DCCS portable:

- Extensión “Certificate Policies” con valor OID “1.3.6.1.4.1.36035.1.5.1”

Para DCCS centralizado:

- Extensión “Certificate Policies” con valor OID “1.3.6.1.4.1.36035.1.5.3”

En todo caso:

- Extensión QcStatements con valor “id-etsi-qcs-QcSSCD” habilitado

Las claves de certificados generadas en DCCS portable generalmente no pueden ser copiadas de ninguna manera, por lo que si se pierde o se estropea el dispositivo, será necesario realizar un nuevo proceso de emisión de certificado.

3.2.2 OTROS DISPOSITIVOS

Las claves privadas de los certificados emitidos en Otros dispositivos no se generan en un dispositivo cualificado.

Por lo anterior, SIGNE no puede garantizar que las claves criptográficas han sido creadas en un Dispositivo Cualificado de Creación de Sello (DCCS), en cumplimiento de los requisitos establecidos en el artículo 24 de la Ley 59/2003 y en el Anexo II del Reglamento eIDAS mutatis mutandis a los requisitos de los dispositivos cualificados de creación de sello electrónico. Esta condición se indicará en el propio certificado mediante los siguientes campos:

- Extensión “Certificate Policies” con valor OID “1.3.6.1.4.1.36035.1.5.2”
- Extensión QcStatements con valor “id-etsi-qcs-QcSSCD” deshabilitado

Las claves de certificados generadas en Otros dispositivos generalmente pueden ser copiadas a otros soportes, por lo tanto es posible realizar copias de seguridad de los mismos.

3.3 USO PARTICULAR DE LOS CERTIFICADOS

3.3.1 USOS APROPIADOS DE LOS CERTIFICADOS

Los certificados emitidos por SIGNE podrán usarse en los términos establecidos por la normativa vigente aplicable a la firma electrónica, con las condiciones adicionales que se establecen en la DPC, y en esta PC.

Estos certificados pueden ser utilizados para autenticarse en sistemas de comunicaciones seguras, para la remisión de comunicaciones comerciales, para publicar informaciones en el web de la empresa, etc.

Estos certificados son válidos para su utilización para la firma automatizada de documentos, para la facturación electrónica y digitalización certificada y se ajustan a los requisitos que impone la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

3.3.2 USOS NO AUTORIZADOS DE LOS CERTIFICADOS

No se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta PC y en la DPC.

Dado que los certificados no se han diseñado para el cifrado de información, SIGNE no recomienda su uso para tal cometido.

3.4 TARIFAS

El precio de los certificados de Sello Electrónico y las condiciones de pago de este tipo de certificados será necesario consultarlas telefónicamente o por mail con SIGNE.

4 PROCEDIMIENTOS OPERATIVOS

4.1 PROCESO DE EMISIÓN DE CERTIFICADOS

La RA se encargará de tramitar las solicitudes y proceder a la emisión de los certificados cumpliendo siempre con los términos generales descritos en la DPC.

Los pasos a seguir para la obtención del certificado son los siguientes:

a) Solicitud

Si la Corporación no tuviera firmado el contrato de prestación de servicios de certificación con SIGNE, éste deberá ser firmado por el representante legal en el momento de solicitar un certificado.

El Solicitante deberá haberse personado ante SIGNE o un agente comercial de ésta para identificarse como representante de la organización a la que pertenece. Esta identificación presencial deberá ser realizada en el momento la solicitud, excepto, conforme a lo establecido en la Ley 59/2003, cuando la identidad del Solicitante constara ya a SIGNE en virtud de una relación preexistente, en la que se hubiera identificado presencialmente al interesado y el período de tiempo transcurrido desde dicha identificación es menor de cinco años.

En el momento de la solicitud, el Solicitante deberá presentar una autorización firmada (Hoja de solicitud) con los datos del Custodio de claves (la persona autorizada a obtener un certificado corporativo de Sello Electrónico).

Los datos de esta autorización deben incluir: Nombre, Número de documento de identificación que será presentado (por ejemplo, NIF o NIE para España, CUI o Nº Carné de Extranjería para Perú), Cargo en la organización y Dirección de correo electrónico de la persona autorizada y la confirmación de lectura del Régimen obligatorio del uso del certificado, documento que quedará bajo custodia de la RA y de la que el Custodio de claves podrá obtener una copia.

La RA verificará presencialmente la identidad del Custodio de claves con su documento de identificación presentado (por ejemplo, DNI o NIE en España, DNI o Carné de Extranjería en Perú). Esta identificación presencial deberá ser realizada en el momento la solicitud, excepto, conforme a lo establecido en la Ley 59/2003, cuando la identidad del Custodio de Claves constara ya a SIGNE en virtud de una relación preexistente, en la que se hubiera identificado presencialmente al interesado y el período de tiempo transcurrido desde dicha identificación es menor de cinco años.

b) Aceptación de la solicitud

La RA verificará la identidad del Solicitante, su vinculación con la Corporación (su condición de representante o apoderado), la existencia de ésta, y los datos a incluir en el certificado.

La RA podrá verificar los datos anteriores según uno de los siguientes procedimientos:

- Al Solicitante con su documento de identificación presentado (por ejemplo, DNI o NIE en España, DNI o Carné de Extranjería en Perú).
- A la relación que vincula el Solicitante como representante legal o voluntario de la Corporación:

  - Mediante conexión telemática con los correspondientes registros públicos o especiales (por ejemplo, con un acceso en línea al Registro de Universidades o al Registro Mercantil).
  - Mediante la solicitud de las escrituras públicas, contratos, estatutos, pactos o cualesquiera otros documentos que puedan acreditar la constitución de la entidad, su vigencia e identificación de los miembros que las integran.

c) Tramitación

Una vez aceptada, la RA tramitará la solicitud del certificado, en función del soporte que se utilice.

d) Generación de claves

El primer paso de la tramitación será la generación de claves según el soporte que se utilice:

En Otros dispositivos:

En el caso de que el soporte utilizado sea un dispositivo software:

- El Custodio de claves recibirá por correo electrónico la confirmación de la solicitud, juntamente con un código de autenticación a la aplicación online de emisión de certificados.
- Para poder acceder a la aplicación online de emisión de certificados será necesario que el Custodio de claves proporcione el código de autenticación recibido. Una vez autenticado, el Custodio de claves procederá a la descarga del certificado electrónico (incluye la generación de las claves, la emisión del certificado y la descarga de ambos protegidos con una contraseña que él mismo establecerá).

En Dispositivos Cualificados de Creación de Sello (DCCS)

Se procederá a la activación del dispositivo y seguidamente se generará el par de claves.

Las claves serán generadas por el Custodio de claves o por la RA en los sistemas indicados por el Solicitante, utilizando aplicaciones compatibles con los estándares de PKI, haciendo entrega a la RA de una petición de certificado en formato PKCS#10.

e) Emisión del certificado

Una vez las claves generadas, la RA procederá a la emisión del certificado, firmando la petición de generación de certificado y enviándola a la CA.

f) Entrega

Finalmente, la RA hará entrega del certificado al Custodio de claves según el soporte que se utilice:

En Otros dispositivos:

En el caso de que el soporte utilizado sea un dispositivo software:

- El Custodio de claves procederá a la descarga del certificado electrónico (incluye la generación de las claves, la emisión del certificado y la descarga de ambos protegidos con una contraseña que él mismo establecerá).
- El Custodio de claves podrá instalar las claves y el certificado en su sistema informático introduciendo la contraseña que él mismo estableció en el momento de la descarga.

En Dispositivos Cualificados de Creación de Sello (DCCS)

Portable: La RA cargará el certificado en el dispositivo en el que se hayan generado previamente el par de claves. El código de activación del dispositivo de creación de sello será entregado únicamente al Custodio de claves (en el caso de que éste no aporte su propio dispositivo).

Centralizado: La RA cargará el certificado en el dispositivo en el que se hayan generado previamente el par de claves. Para la activación de los datos de creación de sello en el módulo de seguridad, el sistema informático configurado por el Custodio de claves deberá utilizar una contraseña definida por él mismo.

4.2 REVOCACIÓN DE CERTIFICADOS

El Suscriptor deberá solicitar la revocación de su certificado en caso de pérdida, compromiso de claves u otras causas descritas en la DPC.

Para solicitar la revocación del certificado el Suscriptor puede:

- Llamar al servicio de revocación en horario de oficina: **902 30 17 01**
- Enviar un correo electrónico (la revocación del certificado se realizará en horario de oficina): **signe-ac@signe.com**

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

4.3 RENOVACIÓN DE CERTIFICADOS

El Solicitante deberá ponerse en contacto con la RA y solicitar la generación de un certificado nuevo.

5 PERFIL DE LOS CERTIFICADOS

Los certificados de sello electrónico de SIGNE siguen las recomendaciones del Esquema de identificación y firma electrónica de las Administraciones públicas, Bloque I: Perfiles de certificados electrónicos, en su versión V1.7.3 del 18/11/2009.

5.1 NOMBRE DISTINGUIDO (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	*Contendrá el nombre comercial de la persona jurídica o la denominación del sistema o aplicación de firma automática*
SN, Serial Number	Identificación de la organización	*Identificador de la persona jurídica, tal como figura en los registros oficiales (por ejemplo, NIF para España, RUC para Perú)*
O, Organization	Organización	*Contendrá la denominación exacta de la persona jurídica según aparezca en el Registro mercantil*
OI, Organization Identifier	Identificador de la organización	*Identificador de la persona jurídica, tal como figura en los registros oficiales. Codificado según la Norma Europea ETSI EN 319 412-1, con único posible tipo VAT.* *El formato sería: "VAT" + "2 caracteres del código de país según ISO 3166-1" + "-" + "identificador de la persona jurídica (por ejemplo, NIF para España, RUC para Perú)".* *Ejemplo:* VATES-B0085974Z.
OU, Organizational Unit (Opcional)	Unidad en la organización	*Contendrá el Departamento o Unidad*
ST, State	Ubicación Geográfica	*Ámbito geográfico de vinculación del suscriptor*
C, Country	País	*Código de país de dos dígitos según ISO 3166-1 donde está registrada la organización*

5.2 EXTENSIONES COMUNES DE LOS CERTIFICADOS

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	rfc822Name: *email de contacto*
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	TLS Web Client Authentication Email Protection
X509v3 Subject Key Identifier	-	*<id de la clave pública del certificado, obtenido a partir del hash de la misma>*
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Authority Information Access	-	Access Method: id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: id-ad-caIssuers Access Location: <URI de acceso al certificado de la CA emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
QcStatements	-	id-etsi-qcs-QcCompliance (indica que el certificado es cualificado) id-etsi-qcs-QcRetentionPeriod: 15 (años de retención de la documentación del certificado) id-etsi-qcs-QcPDS: https://www.signe.es/signe-ac/dpc/pds_en.pdf (URI de la PDS en lengua inglesa) id-etsi-qcs-QcType: id-qct-eseal (indica que es un certificado para crear sellos electrónicos)

5.3 EXTENSIONES DE LOS CERTIFICADOS EN OTROS DISPOSITIVOS

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.5.2 (Otros dispositivos - Nivel Medio) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice : Este es un Certificado de Sello Electrónico cualificado OID de la política de certificación europea: 0.4.0.194112.1.1 (corresponde a la política para certificados EU cualificados emitidos a personas jurídicas sin uso de un DCCS "QCP-l")

5.4 EXTENSIONES DE LOS CERTIFICADOS CON DCCS

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.5.1 (DCCS portable - Nivel Alto) o 1.3.6.1.4.1.36035.1.5.3 (DCCS centralizado - Nivel Alto) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice : Este es un Certificado de Sello Electrónico cualificado en DCCS OID de la política de certificación europea: 0.4.0.194112.1.3 (corresponde a la política para certificados EU cualificados emitidos a personas jurídicas con uso de un DCCS "QCP-l-qscd")
QcStatements	-	id-etsi-qcs-QcSSCD (indica que la clave privada se custodia en un DCCS)