



Signe - Autoridad de Certificación

Política de certificación

Certification policy

Certificados Corporativos de Titulado

Versión: 2.1
Fecha: 11/04/2018

Versión	Cambios	Fecha
1.0	Creación del documento	02/11/2010
1.1	Cambios en el formato	24/03/2015
1.2	Modificación documento. Inclusión definiciones y acrónimos.	06/06/2016
2.0	Adaptación eIDAS	28/02/2018
2.1	<ul style="list-style-type: none">● Corrección en la extensión Key Usage para quitar el bit de cifrado● Corrección en el procedimiento de emisión	11/04/2018

Índice

1. Introducción	5
1.1. Descripción general	5
1.2. Nombre del documento e identificación	6
1.3. Definiciones y acrónimos	6
2. Entidades participantes	6
2.1. Autoridades de certificación (AC)	6
2.2. Autoridad de registro (AR)	6
2.3. Solicitante	7
2.4. Suscriptor/Firmante	7
2.5. Custodio de claves	8
2.6. Tercero que confía en los certificados	8
3. Características de los certificados	9
3.1. Periodo de validez de los certificados	9
3.2. Tipos de soporte	9
3.2.1. Soporte en software	9
3.3. Uso particular de los certificados de Titulado	10
3.3.1. Usos apropiados de los certificados	10
3.3.2. Usos no autorizados de los certificados	10
3.4. Tarifas	10
4. Procedimientos operativos	11
4.1. Proceso de emisión de certificados	11
4.2. Revocación de certificados	12
4.3. Renovación de certificados	13

5. Perfil de los certificados	14
5.1. Nombre distinguido (DN)	14
5.1.1. Información relativa a la titulación	15
5.2. Extensiones de los certificados	16

1. Introducción

1.1. Descripción general

Los Certificados de Titulado son certificados digitales personales que permiten identificar telemáticamente a sus Suscriptores/Firmantes como poseedores de una determinada titulación académica.

Estos certificados pueden ser emitidos en los siguientes tipos de soporte:

En software (nivel medio), a través de una aplicación, obteniendo un certificado para la firma y la autenticación.

Los Certificados de Titulado son certificados digitales reconocidos de conformidad con la Ley 59/2003 de 19 de diciembre de firma electrónica, y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Son certificados cualificados porque cumplen los requisitos establecidos en el anexo I del Reglamento UE 910/2014.

Los Certificados de Titulado garantizan la identidad del Suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica avanzada que se basa en un certificado reconocido".

La solicitud de los Certificados de Titulado se puede realizar a través de las propias organizaciones a las que se vincula cada estudiante, actuando como Autoridades de Registro de SIGNE.

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

1.2. Nombre del documento e identificación

Nombre:	PC -Certificados de Titulado
Versión:	2.1
Descripción:	Política de Certificación para Certificados de Titulado
Fecha de Emisión:	11/04/2018
OIDs	1.3.6.1.4.1.36035.1.1.2 - Otros dispositivos ¹
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)” URL <https://www.signe.es/signe-ac/dpc>

2. Entidades participantes

2.1. Autoridades de certificación (AC)

Los Certificados de Titulado son emitidos exclusivamente por SIGNE Autoridad de Certificación, autoridad de certificación subordinada de la AC Raíz de Firmaprofesional.

2.2. Autoridad de registro (AR)

La gestión de las solicitudes de los certificados será realizada por las entidades que actúen como Autoridades de Registro de SIGNE o por la misma SIGNE.

Cada entidad que actúe como AR de SIGNE podrá cursar la solicitud de certificados de titulado a aquellas personas físicas que hayan finalizado sus estudios y solicitado su título.

¹ Otros dispositivos diferentes de Dispositivo Cualificado de Creación de Firma (DCCF)

Cada AR deberá colaborar con SIGNE en la solicitud, verificación de los datos necesarios, y entrega del certificado electrónico; y en particular:

- Identificar a los egresados que soliciten el certificado electrónico de titulado, y obtener su consentimiento para la emisión del certificado, así como a verificar de forma definitiva al egresado en el momento de entrega de las claves para la obtención del certificado electrónico de titulado.
- Verificar que la solicitud de servicio es íntegra y, los datos veraces, en particular el código de entidad y código de estudio y, en el caso de las solicitudes incompletas, completarlas o corregirlas.
- Tramitar la formalización del contrato de prestación de servicios de certificación electrónica, y validar los datos con el titulado en los términos y condiciones que se establezcan.
- Custodiar toda la información y documentación gestionada relativa a cada certificado reconocido tramitado, empleando siempre la máxima diligencia en la verificación de la exactitud y veracidad de los datos y documentos custodiados.
- Conceder acceso a SIGNE a los datos académicos de los egresados estrictamente necesarios para la prestación de los servicios, actuando SIGNE como encargado del tratamiento de dichos datos por cuenta de la AR.
- Emplear personal que tenga los conocimientos, la experiencia y las cualificaciones necesarias para la realización de los servicios de identificación que le correspondan.

2.3. Solicitante

El Solicitante es el egresado, estudiante que ha completado sus estudios y se encuentra en situación de obtener el título que acredite la consecución de los mismos.

Cada entidad actuando como RA de SIGNE es responsable de determinar qué grupos de usuarios pueden solicitar el certificado de Titulado.

2.4. Suscriptor/Firmante

El Suscriptor/Firmante es la persona física identificada por su nombre, apellidos y NIF, al que se le ha expedido un certificado de Titulado.

De acuerdo con el Reglamento RD 910/2014, el firmante es la persona física que crea la firma electrónica.

2.5. Custodio de claves

La custodia de los datos de creación de firma asociados a cada certificado electrónico de titulado será responsabilidad de la persona física Solicitante, cuya identificación se incluirá en el certificado electrónico.

2.6. Tercero que confía en los certificados

Los terceros que confíen en estos certificados deben tener presente las limitaciones en su uso.

3. Características de los certificados

3.1. Periodo de validez de los certificados

Los certificados de Titulado tendrán un periodo de validez de 3 años.

3.2. Tipos de soporte

Los Certificados de Titulado se generarán en soporte software.

3.2.1. Soporte en software

Las claves privadas de los certificados emitidos en soporte software se generan y almacenan en un navegador de Internet, como por ejemplo Microsoft Internet Explorer.

Al tratarse de certificados en software, SIGNE no puede garantizar que las claves criptográficas del firmante han sido creadas en un Dispositivo Cualificado de Creación de Firma (DCCF), en cumplimiento de los requisitos establecidos en el artículo 24 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y en el Anexo II del Reglamento UE 910/2014. Esta condición se indicará en el propio certificado mediante los siguientes campos:

- Extensión “Certificate Policies” con valor OID “1.3.6.1.4.1.36035.1.1.2”
- Extensión QcStatement con valor “id-etsi-qcs-QcSSCD” deshabilitado

Los Certificados de Titulado en software pueden ser copiados a otros soportes, por lo tanto es posible realizar copias de seguridad de los mismos.

Los Certificados de Titulado en software están identificados mediante el OID 1.3.6.1.4.1.36035.1.1.2 en la extensión “X509v3 Certificate Policies”.

3.3. Uso particular de los certificados de Titulado

3.3.1. Usos apropiados de los certificados

Los certificados emitidos por SIGNE podrán usarse en los términos establecidos por la DPC, y lo establecido en la legislación vigente al respecto.

Dichos certificados se utilizan para todas las relaciones telemáticas que puedan llegar a establecer entre el titulado y los diversos ámbitos en los que se requiera constatar la categoría de titulado, sin que en ningún caso el atributo que se contiene en el certificado constituya una declaración oficial de titulado, sino exclusivamente una manifestación del organismo docente refiriendo que un determinado sujeto es titulado.

Los Certificados de Titulado pueden ser utilizados con los siguientes propósitos:

- Proporcionar integridad a un documento firmado electrónicamente.
- No repudio de origen.
- Identificación del Firmante y su condición de titulado.

3.3.2. 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.

Tampoco se permite el uso del certificado para la realización de transacciones comerciales, económicas y financieras, en medio digital.

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

3.4. Tarifas

SIGNE podrá establecer las tarifas que considere oportunas a los Suscriptores, así como establecer los medios de pago que considere más adecuado en cada caso. Para más detalles sobre el precio y condiciones de pago de este tipo de certificados será necesario consultar con el Departamento Comercial de Signe.

4. Procedimientos operativos

4.1. Proceso de emisión de certificados

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

a) Solicitud:

La petición del certificado deberá ser realizada por el Solicitante, cumpliendo con lo descrito en la DPC y con lo siguiente:

- El Solicitante deberá estar autorizado a solicitar el certificado, esto es, deberá haber completado sus estudios y encontrarse en situación de obtener el título que acredite la consecución de los mismos.
- El Solicitante deberá entregar la documentación requerida a la RA para tramitar la solicitud.
- En el momento de la solicitud, el Solicitante deberá proporcionar una dirección de correo electrónico válida, a la que únicamente él tenga acceso.

El Solicitante (egresado) deberá dirigirse al servicio encargado de la tramitación de las titulaciones de la entidad en la que haya cursado sus estudios para solicitar la emisión de su certificado electrónico de titulado.

La entidad, a través del personal administrativo autorizado, se encargará de tramitar la solicitud con SIGNE.

b) Aceptación de la solicitud

La RA se encargará de verificar la información académica y completar los códigos de estudio y centro en caso de ser necesario antes de aceptar la solicitud y empezar con la tramitación del certificado.

c) Tramitación

Para proceder con la tramitación, el Solicitante deberá:

- Identificarse presencialmente ante la AR
- Verificar que la RA dispone de su dirección de correo electrónico.
- Leer, aceptar y firmar el Contrato de Prestación de Servicios de Certificación Electrónica, que se quedará en poder de la RA.

d) Generación de claves, emisión y entrega del certificado

El Suscriptor 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 de generación de claves será necesario que el Solicitante proporcione el código de autenticación recibido. Una vez autenticado, el Solicitante procederá a la descarga del certificado electrónico, protegido con una contraseña que él mismo establecerá, en su propio sistema informático.

El usuario podrá instalar el certificado en su ordenador introduciendo la contraseña que él mismo estableció en el momento de la descarga.

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 CPS.

Para solicitar la revocación del certificado el Suscriptor puede:

a) Solicitar la revocación online mediante el código de revocación

Para ello, el Suscriptor deberá:

- Acceder en la web de SIGNE al apartado correspondiente a revocación, y seleccionar el enlace correspondiente a revocación mediante código de revocación.
- En el formulario dispuesto, escribir correctamente los datos que le identifiquen.
- Introducir el Código de Revocación proporcionado durante el proceso de emisión del certificado.
- Aceptar explícitamente la tramitación de la solicitud y las consecuencias de ésta.

Una vez finalizado el proceso, el certificado será inmediatamente revocado.

b) Solicitar la revocación online mediante el DNle

Para ello, el Suscriptor deberá:

- Acceder a la web de SIGNE y autenticarse con su DNle.
- Solicitar la revocación de su certificado de titulado.
- Aceptar explícitamente la tramitación de la solicitud y las consecuencias de ésta.

Una vez finalizado el proceso, el certificado será inmediatamente revocado.

c) Solicitar la revocación telefónicamente

- Llamar al servicio de revocación telefónico de SIGNE en horario de oficina:
902 30 17 01

Una vez finalizado el proceso, el certificado será inmediatamente revocado.

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

4.3. Renovación de certificados

SIGNE Autoridad de Certificación enviará una notificación de renovación por correo electrónico al Suscriptor dos meses antes de la fecha de caducidad del certificado.

El certificado podrá ser renovado telemáticamente o personalmente ante la RA.

Proceso de renovación telemática:

- El Suscriptor recibirá por correo electrónico una notificación de la AR para iniciar la renovación a través de la página web de SIGNE.
- El Suscriptor deberá acceder a la web con su certificado antes de que caduque o con el DNle en el caso de que haya caducado.
- El Suscriptor deberá firmar electrónicamente la solicitud de renovación del certificado.

Proceso de renovación presencial ante la RA:

En el caso de que el Suscriptor no pueda renovar telemáticamente su certificado, podrá dirigirse a la RA para formalizar la renovación de su certificado. En este caso, se le generará un certificado nuevo, con un nuevo par de claves, pero con los mismos datos que el certificado a renovar.

Para ello deberá proceder según los puntos c) d) y e) del procedimiento de emisión de certificados, esto es:

- Identificarse presencialmente ante la RA.
- Verificar que la RA dispone de su dirección de correo electrónico.
- Leer, aceptar y firmar el Contrato de Prestación de Servicios de Certificación Electrónica, que se quedará en poder de la AR.
- Descargarse el certificado en su ordenador mediante el código de autenticación proporcionado, conectándose a la dirección proporcionada en el correo electrónico recibido.

5. Perfil de los certificados

5.1. Nombre distinguido (DN)

El DN de los certificados de Titulado contendrá como mínimo los elementos que se citan a continuación. Todos los valores de los componentes serán autenticados por la Autoridad de Registro:

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre y Apellidos del Firmante
SN, surName	Apellido	1er Apellido del Firmante
GN, givenName	Nombre de Pila	Nombre de pila del Firmante
E,E-mail	E-mail	Correo electrónico del Firmante
C, Country	País	Código de país de dos dígitos según ISO 3166-1, indicando la nacionalidad del titulado.
serialNumber	Número de Serie	NIF, NIE o código del documento identificativo presentado por el Firmante.
1.3.6.1.4.1.36035.3.1.X ₁ .1	Título	Nombre oficial de la X ₁ titulación obtenida
1.3.6.1.4.1.36035.3.1.X ₁ .2	Código Título	Código alfanumérico oficial de la titulación X ₁

1.3.6.1.4.1.36035.3.1.X ₁ .3	Organismo	Organismo que ha expedido la titulación X ₁ según el formato: <Código 3 cifras>-<Nombre organismo>
1.3.6.1.4.1.36035.3.1.X ₂ .1	Título	Nombre oficial de la X ₂ titulación obtenida
1.3.6.1.4.1.36035.3.1.X ₂ .2	Código Título	Código alfanumérico oficial de la titulación X ₂
1.3.6.1.4.1.36035.3.1.X ₂ .3	Organismo	Organismo que ha expedido la titulación X ₂ según el formato: <Código 3 cifras>-<Nombre organismo>
1.3.6.1.4.1.36035.3.1.X ₃ .1	Título	Nombre oficial de la X ₃ titulación obtenida
1.3.6.1.4.1.36035.3.1.X ₃ .2	Código Título	Código alfanumérico oficial de la titulación X ₃
1.3.6.1.4.1.36035.3.1.X ₃ .3	Organismo	Organismo que ha expedido la titulación X ₃ según el formato: <Código 3 cifras>-<Nombre organismo>
1.3.6.1.4.1.36035.3.1.X ₄ .1	Título	Nombre oficial de la X ₄ titulación obtenida
1.3.6.1.4.1.36035.3.1.X ₄ .2	Código Título	Código alfanumérico oficial de la titulación X ₄
1.3.6.1.4.1.36035.3.1.X ₄ .3	Organismo	Organismo que ha expedido la titulación X ₄ según el formato: <Código 3 cifras>-<Nombre organismo>
1.3.6.1.4.1.36035.3.1.X ₅ .1	Título	Nombre oficial de la X ₅ titulación obtenida
1.3.6.1.4.1.36035.3.1.X ₅ .2	Código Título	Código alfanumérico oficial de la titulación X ₅
1.3.6.1.4.1.36035.3.1.X ₅ .3	Organismo	Organismo que ha expedido la titulación X ₅ según el formato: <Código 3 cifras>-<Nombre organismo>

5.1.1. Información relativa a la titulación

La información de la titulación viene identificada y clasificada mediante el OID siguiente: 1.3.6.1.4.1.36035.3.1.<#TITULO>.<N>

Dónde:

1.3.6.1.4.1	Prefijo que indica que el OID pertenece a una empresa privada
36035	Corresponde con el código de la empresa SIGNE
3	Identificador para extensiones o campos del DN
1	Identificador de campo con información relativa la titulación
<#TITULO>	Número que identifica y agrupa la información correspondiente a una misma titulación
<N>	3 posibles valores: N=1 : Indica campo que contiene el nombre oficial de la titulación N=2 : Indica campo que contiene el código oficial de la titulación N=3 : Indica campo que indica el organismo que ha expedido la titulación

5.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 SubjectAlternativeName	-	<i>(Opcional) RFC822:<email del firmante> directoryName: 1.3.6.1.4.1.13177.0.1: Nombre de pila de la persona física tal y como aparece en su documento de identidad. 1.3.6.1.4.1.13177.0.2: Primer apellido de la persona física tal y como aparece en su documento de identidad 1.3.6.1.4.1.13177.0.3: Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)</i>
X509v3 IssuerAlternativeName	-	URL:http://www.signe.es/signe-ac
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	<i><id de la clave pública del certificado, obtenido a partir del hash de la misma></i>
X509v3 Authority Key Identifier	-	<i><id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma></i>
X509v3 AuthorityInformation Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP>
X509v3 CRL DistributionPoints	-	<URI de la CRL>
X509v3 CertificatePolicies	-	<i><OID de la política de certificación correspondiente al certificado> <URI de la DPC> User Notice: "Este es un certificado reconocido de titulado. Consulte las condiciones de uso en" + <URI de la DPC> <OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU</i>

		<p>cualificados emitidos a personas físicas “QCP-n”, sin uso de un DCCF)</p>
QcStatements	-	<p>Id-etsi-qcs-QcCompliance (indicando que el certificado es reconocido) id-etsi-qcs-QcEuRetentionPeriod = 15 (15 años de custodia de los datos del certificado) Id-etsi-qcs-QcPDS²: 0.4.0.1862.1.5 (URI:https://www.signe.es/signe-ac/dpc/pds_en.pdf) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).</p>

² Obligatoria en lengua inglesa. Pueden incluirse otros QcPDS en otras lenguas.

