Signe - Autoridad de Certificación

Política de certificación

Certification policy

Certificados de Titulado

Documento:	SIGNE-POL-PER-AC-05
Versión:	2.3
Fecha:	22/03/2019

Registro de Versiones

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	Corrección en la extensión *Key Usage* para quitar el bit de cifrado Corrección en el procedimiento de emisión	11/04/2018
2.2	Homogeneización de la terminología sobre los distintos soportes de los certificados.	31/07/2018
2.3	Cambios en el formato. Eliminación de revocación online mediante DNIe. Añadida la revocación por correo electrónico. Eliminación de campo E-mail del DN. Cambios en formato del valor del campo *Serial Number* del DN. Correcciones menores.	22/03/2019

Índice

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.

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.

Los certificados de Titulado son certificados cualificados de firma electrónica porque cumplen los requisitos establecidos en el anexo I del 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").

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/cualificado".

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	2.3
Descripción	Política de Certificación de Certificados de Titulado
Fecha de emisión	22/03/2019
OIDs	1.3.6.1.4.1.36035.1.1.2 - Otros dispositivos[1] - 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)" URL https://www.signe.es/signe-ac/dpc

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

2. Entidades participantes

2.1. Autoridades de Certificación (CA)

Los Certificados de Titulado 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 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 RA de SIGNE podrá cursar la solicitud de certificados de titulado a aquellas personas físicas que hayan finalizado sus estudios y solicitado su título.

Cada RA 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 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 RA.
- 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 número de documento de identificación presentado (NIF o NIE para España, CUI o Nº Carné de Extranjería para Perú, Nº Pasaporte para cualquier país), al que se le ha expedido un certificado de Titulado.

El Suscriptor/Firmante y el Solicitante serán la misma persona física.

De acuerdo con el Reglamento eIDAS, 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 emitirán en Otros dispositivos[2].

3.2.1. Otros dispositivos[2]

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 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 eIDAS. 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 QcStatements con valor "id-etsi-qcs-QcSSCD" deshabilitado

Las claves de los Certificados de Titulado en Otros dispositivos 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 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.

[2] Otros dispositivos diferentes de Dispositivo Cualificado de Creación de Firma (DCCF)

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 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 RA.

d) Generación de claves, emisión y entrega del certificado

El Solicitante 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 Solicitante proporcione el código de autenticación recibido. Una vez autenticado, el Solicitante 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 Solicitante podrá instalar las claves y el certificado en su ordenador o sistema informático 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 DPC.

Para solicitar la revocación del certificado el Suscriptor puede:

a) Solicitar la revocación online

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 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.

c) Solicitar la revocación por correo electrónico

Enviar un correo electrónico a SIGNE: **signe-ac@signe.com**

La revocación del certificado se realizará en horario de oficina.

Para toda información complementaria referente a la revocación de los certificados, referirse al

apartado correspondiente de la DPC.

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 de forma online o de forma presencial ante la RA.

Proceso de renovación online:

- El Suscriptor recibirá por correo electrónico una notificación de la RA 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 DNIe 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 de foma online 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 RA.
- Descargarse el certificado en su ordenador (incluye la generación de las claves, la emisión del certificado y la descarga de ambos protegidos con una contraseña que él mismo establecerá) 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, Given Name	Nombre de Pila	*Nombre del Firmante*
C, Country	País	*Código de país de dos dígitos según ISO 3166-1, indicando el país emisor del documento de identificación presentado*
Serial Number	Número de Serie	*Identificador de la persona natural, codificado según la Norma Europea ETSI EN 319 412-1, con los posibles tipos siguientes: IDC (DNI en España o Perú), PNO (NIE en España, Carnet de Extranjería en Perú) o PAS (Pasaporte)* *El formato sería: "3 caracteres del tipo de identificador (IDC, PNO o PAS)" + "2 caracteres del código de país según ISO 3166-1" + "-" + "identificador de la persona natural (NIF o NIE para España, CUI o Nº Carné de Extranjería para Perú, Nº Pasaporte para cualquier país)".* *Ejemplo:* IDCES-00000000G
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 Subject Alternative Name	-	rfc822Name: *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)*
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	-	*<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>
X509v3 Certificate Policies	-	OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.1.2 (Otros dispositivos - Nivel Medio) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice: Este es un certificado cualificado de titulado OID de la política de certificación europea: 0.4.0.194112.1.0 (corresponde a la política para certificados EU cualificados emitidos a personas físicas sin uso de un DCCF "QCP-n")
QcStatements	-	id-etsi-qcs-QcCompliance (indica que el certificado es cualificado) id-etsi-qcs-QcEuRetentionPeriod: 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-etsi-qct-esign (indica que es un certificado para crear firmas electrónicas).

Una compañía de GRUPO signe

www.signe.es

Avda. de la Industria, 18
28760 Tres Cantos (Madrid)
España

Tel.: + 34 918 06 00 99
comercial@signe.es