



SIGNE Autoridad de Certificación

Política de Certificación de Certificados de Titulado

Documento:	SIGNE-ES-AC-PC-PER-05
Versión:	3.2
Fecha:	18/10/2021
Tipo de documento:	PÚBLICO

Historial 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 DNle. 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
2.4	Ajuste de la codificación del documento. Correcciones menores.	19/03/2020
3.0	Añadido etiquetado del tipo de documento. Adaptación a la Ley 6/2020. Cambio del certificado de la Autoridad de Certificación Subordinada de SIGNE. Correcciones menores.	24/02/2021
3.1	Cambio del número de teléfono del servicio de revocación telefónico de SIGNE. Eliminación de que se podrá solicitar la revocación de un certificado telefónicamente o por correo electrónico a la RA en la que se tramitó la correspondiente solicitud de certificado.	21/06/2021

	Eliminación de que se atenderá la solicitud de revocación por correo electrónico en horario de oficina. Correcciones menores.	
3.2	Correcciones menores.	18/10/2021

Índice

1. Introducción	5
1.1. Descripción general	5
1.2. Nombre del documento e identificación	5
1.3. Definiciones y siglas	6
2. Entidades participantes	7
2.1. Autoridades de Certificación (CA)	7
2.2. Autoridad de Registro (RA)	7
2.3. Solicitante	7
2.4. Suscriptor/Firmante	8
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. Otros dispositivos	9
3.3. Uso particular de los certificados	9
3.3.1. Usos apropiados de los certificados	9
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 personales, que identifican a sus Suscriptores/Firmantes como poseedores de una determinada titulación académica.

Los certificados Corporativos de Persona Física son certificados cualificados de firma electrónica 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”) y conforme a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante, “Ley 6/2020”).

Los certificados de Titulado pueden ser utilizados para crear “firmas electrónicas avanzadas que se basan en un certificado cualificado de firma electrónica” únicamente por el propio Suscriptor/Firmante.

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 (PC) está subordinada al cumplimiento de la Declaración de Prácticas de Certificación (DPC) de SIGNE.

1.2. Nombre del documento e identificación

Nombre	PC de Certificados de Titulado
Código	SIGNE-ES-AC-PC-PER-05
Versión	3.2
Descripción	Política de Certificación de Certificados de Titulado
Fecha de emisión	18/10/2021
Tipo de documento	PÚBLICO
OID	1.3.6.1.4.1.36035.1.1.2 – Otros dispositivos ¹ - Nivel Medio
Localización	https://www.signe.es/signe-ac/dpc

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

1.3. Definiciones y siglas

Las definiciones y siglas se pueden encontrar especificadas en el documento “Declaración de Prácticas de Certificación” en <https://www.signe.es/signe-ac/dpc>

2. Entidades participantes

2.1. Autoridades de Certificación (CA)

Los certificados de Titulado son emitidos por “**SIGNE Autoridad de Certificación - 2020**”, 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 SIGNE o por entidades que actúen como Autoridades de Registro de 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, y en particular:

- Identificar y autenticar a los egresados que soliciten el certificado de Titulado, y obtener su consentimiento para la emisión del certificado, así como verificar de forma definitiva al egresado en el momento de entrega de las claves para la obtención del certificado.
- Verificar que la solicitud del 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, 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 las tareas asignadas a su rol en la RA 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 en el certificado por su nombre, apellidos y código identificativo (por ejemplo, DNI, NIE u otro tipo de NIF en España; N^o Pasaporte)², 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 electrónica asociados a cada certificado de Titulado será responsabilidad de la persona física Solicitante y a la vez Suscriptor/Firmante.

2.6. Tercero que confía en los certificados

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

² Conforme a lo establecido en el artículo 6.1.a) de la Ley 6/2020, el código identificativo del Suscriptor/Firmante que constará en el certificado será un DNI, un NIE u otro tipo de NIF español, excepto cuando el Suscriptor/Firmante carezca de él por causa lícita

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 dispositivos².

3.2.1. Otros dispositivos³

Las claves privadas de los certificados emitidos en Otros dispositivos no se generan en un dispositivo cualificado de creación de firma electrónica, en cumplimiento de los requisitos establecidos 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 privadas de los certificados emitidos en Otros dispositivos se pueden generar en los siguientes tipos de dispositivos:

- Dispositivo software

Las claves de certificados generadas en dispositivo software pueden ser copiadas a otros soportes, por lo tanto, es posible realizar copias de seguridad de las mismas.

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 en la DPC y en la legislación vigente al respecto.

Los certificados de Titulado se pueden utilizar para todas las relaciones telemáticas que se 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.

³ Otros dispositivos diferentes de Dispositivo Cualificado de Creación de Firma electrónica (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 Suscriptor/Firmante y su condición de titulado.

Se permite el uso de estos certificados en las relaciones personales del Suscriptor/Firmante con las Administraciones Públicas y en otros usos estrictamente personales.

3.3.2. Usos no autorizados de los certificados

No se autoriza su uso para la realización de transacciones comerciales o financieras por medio digital.

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

SIGNE podrá establecer las tarifas que considere oportunas a los Suscriptores/Firmantes, 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 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 y el Régimen Obligatorio de Uso del Certificado, que se quedarán 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 generación de certificados.

Para poder acceder a la aplicación online de generación de certificados será necesario que el Solicitante proporcione el código de autenticación recibido.

Una vez autenticado, el Solicitante procederá a la generación del certificado (incluye la generación de las claves, la emisión del certificado y la descarga de ambos en formato PKCS #12 protegido con una contraseña que él mismo habrá establecido).

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 generación del certificado.

4.2. Revocación de certificados

El Suscriptor/Firmante 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/Firmante puede:

a) Solicitar la revocación online

El Suscriptor/Firmante deberá:

- Acceder en la web de SIGNE al apartado correspondiente a revocación, y seleccionar el enlace correspondiente a revocación online.
- Introducir correctamente su código identificativo.
- Introducir el código de revocación proporcionado durante el proceso de emisión del certificado.
- Aceptar explícitamente la tramitación de la solicitud de revocación y las consecuencias de ésta.

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

b) Solicitar la revocación telefónicamente

El Suscriptor/Firmante deberá llamar al servicio de revocación telefónico de SIGNE (horario de oficina⁴): **+34 918 06 10 08**

⁴ Días laborables en Madrid de lunes a viernes, de 8:30 a 18:30

c) Solicitar la revocación por correo electrónico

El Suscriptor/Firmante deberá enviar un correo electrónico a SIGNE: **signe-ac@signe.com**

En el apartado correspondiente de la DPC se encuentra toda la información complementaria referente a la revocación de certificados.

4.3. Renovación de certificados

SIGNE Autoridad de Certificación enviará una notificación de recordatorio de caducidad del certificado por correo electrónico al Suscriptor/Firmante 45 días, 30 días y 15 días antes de la fecha de caducidad del certificado.

El certificado de Titulado podrá ser renovado de forma online o de forma presencial ante la RA.

a) Proceso de renovación online:

El Suscriptor/Firmante podrá renovar de forma online su certificado sólo en el plazo de los 45 días anteriores a la fecha de caducidad de su certificado actual, y únicamente si éste no ha sido revocado y se ha emitido con identificación presencial ante un operador de la RA.

Para ello, el Suscriptor/Firmante deberá:

- Acceder a la web del portal del Titulado de SIGNE.
- Acceder a la opción de renovación del certificado y autenticarse con su certificado de Titulado a renovar.
- Firmar electrónicamente con su certificado de Titulado a renovar el Contrato de Prestación de Servicios de Certificación y el Régimen Obligatorio de Uso del Certificado correspondientes a su nuevo certificado.
- Realizar lo indicado en el punto d) del proceso de emisión de certificados.

El nuevo certificado tendrá nuevas claves y los mismos datos del Suscriptor/Firmante que el anterior certificado.

b) Proceso de renovación presencial ante la RA

En el caso de que el Suscriptor/Firmante no pueda renovar de forma online su certificado, podrá dirigirse a la RA para formalizar la renovación de su certificado, la cual se efectuará del mismo modo que la emisión de un certificado.

El nuevo certificado tendrá nuevas claves, con posibles cambios en los datos del Suscriptor/Firmante con respecto al anterior certificado.

5. Perfil de los certificados

5.1. Nombre distinguido (DN)

El DN de los certificados de Titulado contendrá los atributos que se indican a continuación. Todos los valores serán verificados por la Autoridad de Registro.

Atributo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre y apellidos del Suscriptor/Firmante
SN, Surname	Apellido	Primer apellido del Suscriptor/Firmante
G, Given Name	Nombre de pila	Nombre de pila del Suscriptor/Firmante
C, Country Name	País	Código de dos letras según ISO 3166-1 del país emisor del código identificativo del Firmante
Serial Number	Número de serie	Código identificativo del Suscriptor/Firmante, codificado según ETSI EN 319 412-1 con uno de los tipos siguientes: IDC (national identity card number, por ejemplo, DNI en España), PNO (national personal number, por ejemplo, NIE u otro NIF distinto de DNI en España), PAS (passport number, N ^o Pasaporte) ⁵ 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>

⁵ Conforme a lo establecido en el artículo 6.1.a) de la Ley 6/2020, el código identificativo del Suscriptor/Firmante será un DNI, un NIE u otro tipo de NIF español, excepto cuando el Suscriptor/Firmante carezca de él por causa lícita

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: <i>email del Suscriptor/Firmante</i> directoryName: 1.3.6.1.4.1.13177.0.1: <i>Nombre de pila del Suscriptor/Firmante</i> 1.3.6.1.4.1.13177.0.2: <i>Primer apellido del Suscriptor/Firmante</i> 1.3.6.1.4.1.13177.0.3: <i>Segundo apellido del Suscriptor/Firmante (este campo puede estar vacío)</i>
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-calssuers 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).

