



SIGNE Autoridad de Certificación

Política de Certificación de Certificados Corporativos de Persona Física

Documento:	SIGNE-ES-AC-PC-COR-03
Versión:	3.4
Fecha:	31/05/2023
Tipo de documento:	PÚBLICO

Historial de versiones

Versión	Cambios	Fecha
1.0	Creación del documento	02/11/2010
1.3	Cambios en el formato	24/03/2015
1.4	Modificación documento. Inclusión definiciones y acrónimos. Actualización User Notice	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. Se cambia el período de validez de los certificados de 3 años a 1, 2 ó 3 años. Homogeneización con el resto de Políticas de Certificación en la generación de claves y entrega del certificado en soporte Otros dispositivos utilizando un dispositivo software. Eliminación del uso restringido del certificado emitido en servidor criptográfico a la firma de las copias electrónicas de los títulos. Aclaraciones en el método de activación de la clave privada en DCCF centralizado. Añadida la revocación por correo electrónico. Eliminación de campos E-mail y OID privado (NIF de la Organización) del DN. Cambios en formato del valor del campo Serial Number del DN. Inclusión de campo Organization Identifier en el DN. Correcciones menores.	22/03/2019
2.4	Ajuste de la codificación del documento. En el proceso de emisión de certificados, se añade una excepción a la identificación presencial del Solicitante y de los	19/03/2020

	Firmantes, conforme a lo establecido en la Ley 59/2003. Correcciones menores.	
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. Añadido que el Suscriptor (Corporación) pueda ser una entidad sin personalidad jurídica cuyos datos constan en el certificado. Añadidos en el soporte Otros dispositivos los tipos dispositivo criptográfico portable y dispositivo criptográfico centralizado. 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. Eliminación de que se atenderá la solicitud de revocación por correo electrónico en horario de oficina. Correcciones menores.	21/06/2021
3.2	Correcciones menores.	18/10/2021
3.3	Incluida la revocación online y se eliminar la revocación por email Se indica la validación del certificado antes del uso de la clave privada Unificación del "Contrato de Prestación de Servicio de Certificación" y "Regímenes Obligatorios de Uso del Certificado" en el documento de "Solicitud y Aceptación de Servicio"	03/06/2022
3.4	Cambios menores.	31/05/2023

Índice

1. Introducción	5
1.1. Descripción General	5
1.2. Nombre del documento e identificación	6
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	7
2.5. Firmante	8
2.6. Custodio de claves	8
2.7. 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. Dispositivo Cualificado de Creación de Firma electrónica (DCCF)	9
3.2.2. Otros dispositivos	10
3.3. Uso particular de los certificados	10
3.3.1. Usos apropiados de los certificados	10
3.3.2. Usos no autorizados de los certificados	11
3.4. Tarifas	11
4. Procedimientos operativos	12
4.1. Proceso de emisión de certificados	12
4.2. Revocación de certificados	14
4.3. Renovación de certificados	14
5. Perfil de los certificados	15
5.1. Nombre distinguido (DN)	15
5.2. Extensiones comunes de los certificados	16
5.3. Extensiones de los certificados en Otros dispositivos	17
5.4. Extensiones de los certificados en DCCF	17

1. Introducción

1.1. Descripción General

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”), que identifican al Suscriptor como Corporación (empresa, entidad privada o pública) y al Firmante como vinculado a esa Corporación, ya sea como empleado, asociado, colaborador, cliente o proveedor.

Los certificados Corporativos de Persona Física pueden ser utilizados para crear firmas electrónicas avanzadas y cualificadas únicamente por el propio Firmante.

La solicitud y emisión de los certificados Corporativos de Persona Física se puede realizar a través de SIGNE o de las propias organizaciones a las que se vincula cada certificado, actuando éstas como Autoridades de Registro de SIGNE. No obstante, también se pueden utilizar otras entidades no vinculadas con el Firmante que sean 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.

El presente documento es una adaptación de la Política de Certificación “Certificados de firma electrónica - Certificados Corporativos de Persona Física” (OID 1.3.6.1.4.1.13177.10.1.2.D) 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	Política de Certificación de Certificados Corporativos de Persona Física
Código	SIGNE-ES-AC-PC-COR-03
Versión	3.4
Descripción	Política de Certificación de Certificados Corporativos de Persona Física
Fecha de emisión	31/05/2023
Tipo de documento	PÚBLICO
OID	1.3.6.1.4.1.36035.1.2
Localización	https://www.signe.es/signe-ac/dpc

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 Corporativos de Persona Física 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 y la emisión de los certificados Corporativos de Persona Física será realizada por SIGNE o por entidades que actúen como intermediarios de SIGNE.

Adicionalmente, la propia Corporación (empresa, entidad privada o pública) podrá actuar como Autoridad de Registro de SIGNE para la gestión de las solicitudes y la emisión de los certificados Corporativos de Persona Física a aquellas personas físicas con las que tenga una vinculación, ya sea como empleados, asociados, colaboradores, clientes o proveedores. La propia Corporación será el Suscriptor de todos estos certificados emitidos.

Cada entidad o 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 Firmante, del Solicitante y del Suscriptor, cumpliendo con lo estipulado en la DPC y la presente PC.
- Los dispositivos de creación de firma electrónica a utilizar, que previamente SIGNE haya homologado.

2.3. Solicitante

El Solicitante es el representante legal o voluntario (apoderado) de la Corporación que adquiere los certificados para los empleados o personas vinculadas con la Corporación.

Los profesionales autónomos o empresarios individuales, al no ser representantes legales o voluntarios de una Corporación, podrán solicitar certificados Corporativos de Persona Física en los que el código identificativo del Suscriptor será igual a su propio código identificativo (por ejemplo, su NIF en España).

2.4. Suscriptor

La Corporación es el Suscriptor de los certificados y por lo tanto el propietario de los certificados emitidos.

El Suscriptor podrá ser una persona jurídica, una entidad sin personalidad jurídica, o un autónomo o empresario individual, cuyos datos constan en el certificado.

2.5. Firmante

El Firmante será 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; DNI o N^o Carné de Extranjería en Perú; N^o Pasaporte)¹, que tenga una vinculación (empleado, asociado, colaborador, cliente o proveedor) con el Suscriptor.

De acuerdo con el Reglamento eIDAS, el Firmante es la persona física que crea la firma electrónica.

2.6. Custodio de claves

La custodia de los datos de creación de firma electrónica, o de los datos de acceso a los mismos, asociados a cada certificado Corporativo de Persona Física será responsabilidad de la persona física Firmante.

2.7. Tercero que confía en los certificados

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

¹ Conforme a lo establecido en el artículo 6.1.a) de la Ley 6/2020, el código identificativo del Firmante que constará en el certificado será un DNI, un NIE u otro tipo de NIF español, excepto cuando el Firmante carezca de él por causa lícita

3. Características de los certificados

3.1. Periodo de validez de los certificados

Los certificados Corporativos de Persona Física tendrán un periodo de validez de hasta 3 años.

3.2. Tipos de soporte

Los certificados Corporativos de Persona Física 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 Firma electrónica (DCCF): Nivel Alto
- Otros dispositivos: Nivel Medio

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

3.2.1. Dispositivo Cualificado de Creación de Firma electrónica (DCCF)

Las claves privadas de los certificados emitidos en DCCF se generan y almacenan en un dispositivo cualificado de creación de firma electrónica que ofrece, al menos, las garantías indicadas en el Anexo II del Reglamento eIDAS. Esta condición se indicará en el propio certificado mediante los siguientes campos:

Para DCCF portable:

- Extensión Certificate Policies con valor OID 1.3.6.1.4.1.36035.1.2.1

Para DCCF centralizado:

- Extensión Certificate Policies con valor OID 1.3.6.1.4.1.36035.1.2.3

En todo caso:

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

Las claves de certificados generadas en DCCF portable 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.

Las claves de certificados generadas en DCCF centralizado pueden ser copiadas protegidas por un dispositivo criptográfico hardware (HSM) y por los datos de activación de las mismas bajo custodia del Firmante, por lo tanto, es posible realizar copias de seguridad de las mismas.

3.2.2. Otros dispositivos²

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 1.3.6.1.4.1.36035.1.2.2
- 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 criptográfico portable
- Dispositivo criptográfico centralizado
- Dispositivo software

Las claves de certificados generadas en dispositivo criptográfico portable 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.

Las claves de certificados generadas en dispositivo criptográfico centralizado pueden ser copiadas protegidas por un dispositivo criptográfico hardware (HSM) y por los datos de activación de las mismas bajo custodia del Firmante, por lo tanto, es posible realizar copias de seguridad de las mismas.

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.

Si el certificado se emite en Dispositivo criptográfico centralizado se asegura que el sistema verifica que el certificado es válido en el momento del uso de la clave privada.

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 Corporativos de Persona Física deben ser, en general, utilizados dentro del marco de la relación jurídica o vinculante entre el Firmante y la Corporación (empresa, entidad privada o pública). En concreto, pueden ser utilizados con los siguientes propósitos:

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

- a) Integridad del documento firmado.
- b) No repudio de origen.
- c) Identificación del Firmante y su vinculación con la Corporación.

Se permite el uso de estos certificados en las relaciones personales del Firmante con las Administraciones Públicas y en otros usos estrictamente personales siempre y cuando no exista una prohibición del Suscriptor (empresa, entidad privada o pública).

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 o la RA podrán establecer las tarifas que considere oportunas a los Suscriptores, así como establecer los medios de pago que consideren más adecuados 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 o de la RA.

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

El documento de Solicitud y Aceptación del Servicio, deberá ser firmado por el representante legal o voluntario de la Corporación, o, en su caso, por el autónomo o empresario individual en el momento de solicitar un certificado.

El Solicitante deberá incluir en el documento de Solicitud y Aceptación una autorización firmada con los datos del Firmante (las personas autorizadas a obtener un certificado Corporativo de Persona Física).

Los datos de esta autorización deben incluir: Nombre y apellidos, Código identificativo que constará en el certificado (por ejemplo, DNI, NIE u otro tipo de NIF en España; DNI o N° Carné de Extranjería en Perú; N° Pasaporte)³, Cargo, título o rol en la organización y Dirección de correo electrónico de cada persona autorizada.

Además, el Solicitante y el Firmante deberán firmar el documento de Solicitud y Aceptación del Servicio, documento que habrá sido entregado al Solicitante, quedando una copia bajo custodia de la RA

b) Aceptación de la solicitud

La RA realizará la identificación y autenticación del Suscriptor, del Solicitante y del Firmante según lo especificado en la DPC en los apartados de validación inicial de la identidad relativos a la autenticación de la identidad de una persona física y, dependiendo del tipo de Suscriptor, de una persona jurídica, de una entidad sin personalidad jurídica, o de una condición de autónomo o empresario individual.

c) Tramitación

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

³ Conforme a lo establecido en el artículo 6.1.a) de la Ley 6/2020, el código identificativo del Firmante que constará en el certificado será un DNI, un NIE u otro tipo de NIF español, excepto cuando el Firmante carezca de él por causa lícita

d) Generación de claves

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

DCCF portable o centralizado, Otros dispositivos de los tipos dispositivo criptográfico portable o centralizado

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

Portable: las claves serán generadas por un Operador de RA en el dispositivo, haciendo entrega a la RA de una petición de certificado en formato PKCS #10.

Centralizado: las claves serán generadas por el Firmante en el dispositivo, haciendo entrega a la RA de una petición de certificado en formato PKCS #10.

Otros dispositivos del tipo dispositivo software

- El Firmante 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 Firmante proporcione el código de autenticación recibido.
- Una vez autenticado, el Firmante 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).

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 Firmante según el soporte que se utilice:

DCCF portable o centralizado, Otros dispositivos de los tipos dispositivo criptográfico portable o centralizado

Portable: la RA cargará el certificado en el dispositivo en el que se hayan generado previamente las claves. El código de activación del dispositivo será entregado únicamente al Firmante (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 las claves. Para la activación de los datos de creación de firma electrónica en el dispositivo, el Firmante deberá utilizar:

- **DCCF centralizado:** dos factores de autenticación de categorías distintas, una contraseña definida por el Firmante, como factor de autenticación basado en el conocimiento, y una contraseña de un solo uso que el Firmante recibe en su teléfono móvil, como factor de autenticación basado en la posesión.
- **Dispositivo criptográfico centralizado:** un nombre de usuario, una contraseña de usuario definida por el Firmante y una contraseña del certificado definida por el Firmante.

Otros dispositivos del tipo dispositivo software

- La generación del certificado por el Firmante incluye la descarga conjunta de la clave privada y del certificado en formato PKCS #12 protegido con una contraseña que él mismo habrá establecido.
- El Firmante 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 o el Firmante deberá solicitar la revocación de su certificado en caso de pérdida, compromiso de claves, finalización de la vinculación del Firmante con la Corporación u otras causas descritas en la DPC.

Para solicitar la revocación del certificado, el Suscriptor o el Firmante pueden:

- Acceder a la web de Signe en el apartado de [obtención y revocación](#) y realizar la revocación online
- Llamar al servicio de revocación telefónico de SIGNE (horario de oficina⁴):
+34 918 06 10 08

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 Firmante 45 días, 30 días y 15 días antes de la fecha de caducidad del certificado.

El Suscriptor deberá ponerse en contacto con la RA, y solicitar la emisión de un nuevo certificado.

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

5. Perfil de los certificados

5.1. Nombre distinguido (DN)

El DN de los certificados Corporativos de Persona Física 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	<i>Nombre y apellidos del Firmante</i>
OI, Organization Identifier	Identificador de la organización	<i>Código identificativo del Suscriptor, codificado según ETSI EN 319 412-1 con el tipo VAT (national value added tax identification number, por ejemplo, NIF en España, N° RUC en Perú) Ejemplo: VATES-B0085974Z</i>
O, Organization Name	Organización	<i>Denominación o razón social del Suscriptor En caso de que el Suscriptor sea un autónomo o empresario individual, se incluirá su nombre y apellidos y/o el nombre comercial de su establecimiento y, opcionalmente, su código CNAE o IAE en España o un código equivalente en otro país</i>
OU, Organizational Unit Name	Unidad en la organización	<i>Contendrá uno de los siguientes valores: - Departamento del Firmante en la organización - Tipo de vinculación del Firmante con la organización</i>
T, Title	Título	<i>Cargo, título o rol del Firmante en la organización</i>
S, State or Province Name	Estado/Provincia	<i>Ámbito geográfico (por ejemplo, provincia en España y Perú) de vinculación del Firmante con la organización</i>
C, Country Name	País	<i>Código de dos letras según ISO 3166-1 del país emisor del código identificativo del Firmante</i>
Serial Number	Número de serie	<i>Código identificativo del Firmante, codificado según ETSI EN 319 412-1 con uno de los tipos siguientes: IDC (national identity card number, por ejemplo, DNI en España o Perú), PNO (national personal number, por ejemplo, NIE u otro NIF distinto de DNI en España, N° Carné de Extranjería en Perú), PAS (passport number, N° Pasaporte)⁵ Ejemplo: IDCES-00000000G</i>
SN, Surname	Apellidos	<i>Apellidos del Firmante</i>
G, Given Name	Nombre de pila	<i>Nombre de pila del Firmante</i>

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

5.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	<p>rfc822Name: <i>email del Firmante</i></p> <p>directoryName: 1.3.6.1.4.1.13177.0.1: <i>Nombre de pila del Firmante</i> 1.3.6.1.4.1.13177.0.2: <i>Primer apellido del Firmante</i> 1.3.6.1.4.1.13177.0.3: <i>Segundo apellido del Firmante (este campo puede estar vacío)</i></p>
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	-	<p>Access Method: id-ad-ocsp Access Location: <URI de acceso al servicio OCSP></p> <p>Access Method: id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora></p>
X509v3 CRL Distribution Points	-	<URI de la CRL>
QcStatements	-	<p>id-etsi-qcs-QcCompliance (indica que el certificado es cualificado)</p> <p>id-etsi-qcs-QcRetentionPeriod: 15 (años de retención de la documentación del certificado)</p> <p>id-etsi-qcs-QcPDS: https://www.signe.es/signe-ac/dpc/pds_en.pdf (URI de la PDS en lengua inglesa)</p> <p>id-etsi-qcs-QcType: id-qct-esign (indica que es un certificado para crear firmas electrónicas)</p>

5.3. Extensiones de los certificados en Otros dispositivos

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<p>OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.2.2 (Otros dispositivos - Nivel Medio) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice: Certificado de Persona Física cualificado</p> <p>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")</p>

5.4. Extensiones de los certificados en DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<p>OID de la política de certificación correspondiente al certificado: 1.3.6.1.4.1.36035.1.2.1 (DCCF portable - Nivel Alto) o 1.3.6.1.4.1.36035.1.2.3 (DCCF centralizado - Nivel Alto) URI de la DPC: http://www.signe.es/signe-ac/dpc User Notice: Certificado de Persona Física cualificado en DCCF</p> <p>OID de la política de certificación europea: 0.4.0.194112.1.2 (corresponde a la política para certificados EU cualificados emitidos a personas físicas con uso de un DCCF "QCP-n-qscd")</p>
QcStatements	-	id-etsi-qcs-QcSSCD (indica que la clave privada se custodia en un DCCF)

