

Sistemas Informáticos Abiertos, S.A.
Avenida de Europa, 2
Alcor Plaza Edificio B
Parque Oeste, Alcorcón 28922
Alcorcón - Madrid (España)
Telf: (34) 902 480 580 Fax: (34) 91 641 95 13

www.sia.es



PC - SIA

Política de Certificación

Certificados cualificados de Ciudadano – Nivel alto

OID: 1.3.6.1.4.1.39131.10.1.9 (QSCD portable)

OID: 1.3.6.1.4.1.39131.10.1.17 (QSCD centralizado)

Versión: 1.1





INDICE

1. INTRODUCCIÓN	8
1.1 Resumen.....	8
1.2 Nombre del documento e identificación.....	10
1.3 Entidades y personas intervinientes.....	11
1.3.1 Autoridad de Certificación / Prestador cualificado de Servicios de Confianza	11
1.3.2 Autoridades de Registro	11
1.3.3 Firmante	12
1.3.4 Suscriptor.....	12
1.3.5 Solicitante.....	12
1.3.6 Terceras Partes Aceptantes	12
1.4 Uso de los certificados.....	12
1.4.1 Usos apropiados / permitidos de los certificados	13
1.4.2 Limitaciones y restricciones en el uso de los certificados	13
1.5 Administración de Políticas	14
1.5.1 Organización responsable.....	14
2. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS.....	15
2.1 Nombres.....	15
2.1.1 Uso de seudónimos	15
2.2 Validación de la identidad inicial	15
2.2.1 Métodos para probar la posesión de la clave privada	15
2.2.2 Autenticación de la identidad de una persona física	15
2.2.3 Información no verificada sobre el solicitante	16
2.2.4 Comprobación de las facultades de representación.....	16
2.3 Identificación y autenticación para peticiones de renovación de claves.....	16
3. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS.....	17
3.1 Solicitud de certificados	17
3.2 Tramitación de las solicitudes de certificados	17
3.3 Emisión de certificados.....	17



3.3.1 Actuaciones de la AC durante la emisión de los certificados	18
3.3.2 Notificación al solicitante de la emisión por la AC del certificado.....	18
3.4 Aceptación del certificado	19
3.4.1 Forma en la que se acepta el certificado	19
3.4.2 Publicación del certificado por la AC.....	19
3.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades	19
3.5 Par de claves y uso del certificado.....	19
3.5.1 Uso de la clave privada del certificados por el titular	19
3.5.2 Uso de la clave pública y del certificado por los terceros aceptantes	20
3.6 Renovación de certificados sin cambio de claves	20
3.6.1 Circunstancias para la renovación de certificados sin cambio de claves.....	20
3.7 Renovación de certificados con cambio de claves.....	20
3.7.1 Circunstancias para una renovación con cambio de claves de un certificado.....	20
3.7.2 Quien puede pedir la renovación de un certificado.....	20
3.7.3 Tramitación de las peticiones de renovación con cambio de claves	21
3.7.4 Notificación de la emisión de nuevos certificados al titular.....	21
3.7.5 Forma de aceptación del certificado con nuevas claves	21
3.7.6 Publicación del certificado con las nuevas claves por la AC.....	21
3.7.7 Notificación de la emisión del certificado por la AC a otras Autoridades	21
3.8 Modificación de certificados	22
3.8.1 Causas para la modificación de un certificado.....	22
3.9 Revocación y suspensión de certificados	22
3.9.1 Causas para la revocación.....	22
3.9.2 Quien puede solicitar la revocación.....	22
3.9.3 Frecuencia de emisión de CRLs.....	23
3.9.4 Requisitos de comprobación en línea de la revocación	23
3.9.5 Otras formas de divulgación de información de revocación.....	23
3.9.6 Requisitos especiales de renovación de claves comprometidas	23
3.9.7 Circunstancias para la suspensión	24
3.10 Servicios de información del estado de certificados	24
3.10.1 Características operativas.....	24



3.10.2 Disponibilidad del servicio	24
3.11 Finalización de la suscripción	24
3.12 Custodia y recuperación de claves	24
3.12.1 Prácticas y políticas de custodia y recuperación de claves	24
4. CONTROLES DE SEGURIDAD TÉCNICA.....	26
4.1 Generación e instalación del par de claves	26
4.1.1 Generación del par de claves.....	26
4.1.2 Entrega de la clave privada al titular.....	26
4.1.3 Entrega de la clave pública al emisor del certificado	26
4.1.4 Tamaño de las claves	26
4.1.5 Parámetros de generación de la clave pública y verificación de la calidad	27
4.1.6 Usos admitidos de la clave (campo KeyUsage de X.509 v3).....	27
4.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos	27
4.2.1 Estándares para los módulos criptográficos	27
4.2.2 Control multi-persona (n de m) de la clave privada.....	28
4.2.3 Custodia de la clave privada	28
4.2.4 Copia de seguridad de la clave privada	28
4.2.5 Archivo de la clave privada	29
4.2.6 Transferencia de la clave privada a o desde el módulo criptográfico	29
4.2.7 Almacenamiento de la clave privada en un módulo criptográfico.....	29
4.2.8 Método de activación de la clave privada.....	29
4.2.9 Método de desactivación de la clave privada	30
4.2.10 Método de destrucción de la clave privada	30
4.3 Otros aspectos de la gestión del par de claves.....	30
4.3.1 Periodos operativos de los certificados y periodo de uso para el par de claves	30
4.4 Datos de activación	31
4.4.1 Generación e instalación de los datos de activación.....	31
4.4.2 Protección de los datos de activación.....	31
5. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP	32
5.1 Perfil de certificado	32
5.1.1 Número de versión	32



5.1.2 Extensiones del certificado	32
5.1.3 Identificadores de objeto (OID) de los algoritmos	35
5.1.4 Formatos de nombre	35
5.1.5 Restricciones de nombre	35
5.1.6 Identificador de objeto (OID) de la Política de Certificación	36
5.1.7 Uso de la extensión "PolicyConstraints"	36
5.1.8 Sintaxis y semántica de los "PolicyQualifier"	36
5.1.9 Tratamiento semántico para la extensión "Certificate Policy"	37
5.2 Perfil de Certificado cualificado de Ciudadano – Nivel alto	37
6. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD	43
6.1 Tarifas	43
6.1.1 Tarifas de emisión de certificado o renovación	43
6.1.2 Tarifas de acceso a los certificados	43
6.1.3 Tarifas de acceso a la información de estado o revocación	43
6.1.4 Tarifas de otros servicios tales como información de políticas	43
6.1.5 Política de reembolso	43



RELACION DE TABLAS

Tabla 1 – Datos identificación DPC.....	10
Tabla 2 – Organización responsable.....	14
Tabla 3 – Definición extensión SubjectAltName	34
Tabla 4 – OID políticas de certificación	36
Tabla 5 – Perfil certificado Firma	40
Tabla 6 – Perfil certificado Autenticación	42



1. INTRODUCCIÓN

1.1 Resumen

El presente documento recoge la Política de Certificación correspondiente a los certificados emitidos por la Autoridad de Certificación (en adelante AC) del prestador de servicios de confianza (TSP), Sistemas Informáticos Abiertos Sociedad Anónima (en adelante SIA), del tipo Certificado cualificado de ciudadano – Nivel alto, que define los mecanismos y procedimientos para la emisión, gestión, revocación, renovación y cualquier otro proceso que afecte al ciclo de vida de los certificados electrónicos emitidos por la AC de SIA. La Política de Certificación (en adelante PC) de SIA se ha estructurado conforme al documento RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC-3647. Cuando no se haya previsto nada en alguna sección o esta venga referida en la DPC, no se contemplará dicho apartado.

Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta estándares europeos, entre los que cabe destacar los siguientes:

- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Igualmente, se ha considerado como normativa básica aplicable a la materia:

- 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 (en adelante eIDAS) y por el que se deroga la Directiva 1999/93/CE.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (Texto consolidado, última modificación: 2 de Octubre de 2015).



- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal, como su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que en su Disposición final sexta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

La regulación aplicable en España, en la fecha de elaboración del presente documento de políticas de certificación, son la Ley 59/2003, de 19 de diciembre, de Firma Electrónica (Texto consolidado, última modificación: 2 de Octubre de 2015) y eIDAS.

En este contexto, los Certificados de ciudadano de nivel alto serán emitidos como **Certificados Cualificados** cumpliendo los requisitos establecidos en el anexo I y II de eIDAS, y desarrollado en Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Asimismo, se han tenido en cuenta los estándares en materia de certificados cualificados, en concreto:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile (reemplaza a TS 101 862).
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

La PC incluye todas las actividades encaminadas a la gestión de los certificados electrónicos en su ciclo de vida, y sirve de guía en la relación entre SIA y los usuarios de sus servicios telemáticos. En consecuencia, todas las partes involucradas tienen la obligación de conocer la PC y ajustar su actividad a lo dispuesto en la misma.



Los Certificados cualificados de ciudadano – Nivel alto solo pueden ser utilizados por el propio ciudadano. La emisión de estos certificados se realizará en un dispositivo cualificado de creación de firma electrónica.

En esta PC se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (DPC) del Prestador de Servicios de Confianza de SIA, conteniendo las reglas a las que se sujeta el uso de los certificados definidos en esta política, así como el ámbito de aplicación y las características técnicas de este tipo de certificados.

Esta PC asume que el lector conoce los conceptos básicos de PKI, certificado y firma electrónica, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

1.2 Nombre del documento e identificación

Nombre del documento	Política de Certificación de certificado cualificado de ciudadano – Nivel alto.
Versión del documento	1.1
Estado del documento	Vigente
Fecha de emisión	23/04/2018
Fecha de caducidad	No aplicable
OID	1.3.6.1.4.1.39131.10.1.9 (QSCD portable) 1.3.6.1.4.1.39131.10.1.17 (QSCD centralizado)
Ubicación de la PC	https://psc.sia.es/
DPC relacionada	Declaración de Prácticas de Certificación de la PKI de SIA OID 1.3.6.1.4.1.39131.10.1.1.1.0 Disponible en https://psc.sia.es/

Tabla 1 – Datos identificación DPC



1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

- SIA como órgano competente de la expedición y gestión de la Autoridad de Certificación / Prestador de Servicios de Confianza.
- Las Autoridades de Registro.
- Los Firmantes.
- Los Suscriptores.
- Las Terceras partes aceptantes de los certificados emitidos.
- Los solicitantes.

1.3.1 Autoridad de Certificación / Prestador cualificado de Servicios de Confianza

SIA actúa como Autoridad de Certificación (AC) relacionando una determinada clave pública con un sujeto o entidad concretos a través de la emisión de Certificados electrónicos.

Las Autoridades de Certificación que componen la PKI de SIA son:

- “AC raíz” Autoridad de Certificación de primer nivel. Esta AC solo emite certificados para sí misma y sus AC subordinadas, a excepción de la emisión del certificado de validación de OCSP y la emisión de la ARL. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.
- “AC subordinada”: Autoridad de Certificación subordinada de “AC raíz”. Su función es la emisión de certificados para terceros, en este caso, la emisión de Certificado cualificado de ciudadano – Nivel alto.

En este ámbito, SIA actúa como prestador de servicios de confianza, emitiendo los certificados electrónicos cualificados de firma y proveyendo servicios de firma electrónica cualificada basada en un certificado cualificado y creada mediante un dispositivo cualificado de creación de firma electrónica, conforme a lo establecido en eIDAS y en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

1.3.2 Autoridades de Registro

La gestión de las solicitudes y emisión de los certificados será realizada por las entidades que actúen como Autoridades de Registro (en adelante AR) de SIA, tal y como viene estipulado en la DPC.

Cada entidad que actúe como AR 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, cumpliendo con lo estipulado en la DPC, apartados 1.3.2 y 9.6.2.
- Los dispositivos de creación de firma a utilizar, que previamente SIA haya homologado.

1.3.3 Firmante

Se entienden por firmante de los certificados cualificados las personas físicas titulares identificadas en el certificado que hagan uso de los servicios de emisión y gestión de los certificados así como de los certificados mismos.

1.3.4 Suscriptor

En el caso de una vinculación entre el firmante y una entidad mediante una relación contractual. El suscriptor es la entidad con personalidad jurídica que suscribe un contrato con SIA, para la expedición de certificados cualificados a estos ciudadanos.

1.3.5 Solicitante

Los solicitantes de certificados cualificados de ciudadano – Nivel alto, son los propios usuarios vinculados a la propia entidad (bien sean corporaciones, empresas, entidades privadas o públicas).

1.3.6 Terceras Partes Aceptantes

Las terceras partes aceptantes, son las personas físicas o entidades diferentes al titular que deciden aceptar y confiar en un certificado emitido por SIA. Y como tales, les es de aplicación lo establecido por la presente Política de Certificación cuando deciden confiar efectivamente en tales certificados.

1.4 Uso de los certificados

Un certificado emitido por la AC de SIA sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en esta PC, por lo que existen ciertas limitaciones en el uso de los certificados de SIA.



1.4.1 Usos apropiados / permitidos de los certificados

Un certificado emitido por la AC de SIA sólo puede ser utilizado para los propósitos explícitamente permitidos e indicados en esta PC y en la correspondiente Declaración de Prácticas de Certificación.

Los certificados deben emplearse únicamente con la legislación que les sea aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación en materia criptográfica existentes en cada momento.

1.4.2 Limitaciones y restricciones en el uso de los certificados

De forma general según lo establecido en la Declaración de Prácticas de Certificación de SIA, y tras aceptar sus condiciones de uso.

De forma específica, cabe reseñar que este certificado será utilizado por los firmantes en las relaciones que mantengan con terceros que confían, de acuerdo con lo usos autorizados en las extensiones “Key Usage” y “Extended Key Usage” del certificado y en conformidad con las limitaciones que consten en el certificado.

El reglamento eIDAS establece que los Certificados Cualificados de Firma Electrónica cumplirán los requisitos establecidos en el anexo I y II. Por otro lado, la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de firma electrónica donde se presumirá el cumplimiento de los requisitos establecidos en dicho anexo cuando un certificado cualificado de firma electrónica se ajuste a dichas normas.

Los certificados de firma son certificados cualificados de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones EN 319 412-5.

El uso del certificado de firma proporciona las siguientes garantías:

- **No repudio de origen**
Asegura que el documento proviene de la persona física de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del Certificado de Firma. El receptor de un mensaje firmado electrónicamente podrá verificar el certificado empleado para esa firma utilizando cualquiera de los Prestadores de Servicios de Validación. De esta forma garantiza que el documento proviene de un determinado titular.



Dado que en el sistema de firma con dispositivos cualificados de creación de firma electrónica se garantiza que las claves de firma permanecen, con un alto nivel de confianza, bajo el exclusivo control del titular, la firma es la prueba efectiva del contenido y del autor del documento (garantía de “no repudio”). Siendo equivalente esta firma electrónica a una firma manuscrita.

- Integridad

El certificado cualificado de ciudadano, en dispositivo cualificado de creación de firma electrónica, permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma electrónica. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de dicho resumen.

1.5 Administración de Políticas

1.5.1 Organización responsable

Esta PC es propiedad de SIA.

Nombre	SIA
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580

Tabla 2 – Organización responsable



2. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS

2.1 Nombres

2.1.1 Uso de seudónimos

No se permite la utilización de seudónimos en ningún caso.

2.2 Validación de la identidad inicial

2.2.1 Métodos para probar la posesión de la clave privada

El par de claves de los Certificados cualificados de ciudadanos – Nivel alto los genera el solicitante, una vez se ha personado, ha sido validado por la Autoridad de Registro y ha firmado el documento de conformidad con la emisión del certificado cualificado de ciudadano, en el dispositivo cualificado de creación de firma electrónica.

Cuando el solicitante acceda al servicio de generación, el sistema informará al titular de que se le va a emitir su certificado de ciudadano y generará en ese momento su correspondiente clave privada y la almacenará en el dispositivo de forma protegida, estableciendo el titular su propia contraseña que únicamente el conocerá, de modo que se garantice el control exclusivo por su parte.

La generación del certificado deberá hacerse acorde con los requisitos que la LFE marca con respecto a los plazos máximos permitidos desde que la persona física realizó el registro presencial.

2.2.2 Autenticación de la identidad de una persona física

La autenticación de la identidad de la persona física identificada en el certificado se realiza mediante su personación ante el operador del punto de registro, acreditándose mediante presentación del Documento Nacional de Identidad (DNI), pasaporte válido o el Número de Identificación de Extranjeros (NIE) del solicitante u otro medio admitido en derecho que lo identifique y se seguirá un proceso integrado con el registro llevado a cabo por la Autoridad de Registro.

Este proceso debe ser presencial, ya que el titular debe personarse en una oficina de registro para identificarse y firmar personalmente un documento de comparecencia y conformidad con las condiciones de emisión del certificado.



2.2.3 Información no verificada sobre el solicitante

Toda la información recabada en el apartado anterior ha de ser verificada por la Autoridad de Registro.

2.2.4 Comprobación de las facultades de representación

No estipulado al no estar contemplada la emisión de certificados para personas jurídicas ni personas físicas representantes.

2.3 Identificación y autenticación para peticiones de renovación de claves

En el supuesto de renovación de la clave, SIA informará previamente al firmante sobre los cambios que se hayan producido en los términos y condiciones respecto a la emisión anterior.

El proceso de renovación de un nuevo certificado, para el firmante es como si de una nueva emisión de certificados se tratase.

En el ámbito de emisión de certificados en dispositivos cualificados de creación de firma electrónica, la renovación del certificado se podrá llevar a cabo de forma que se cumplan los requisitos que la Ley marca con respecto a los plazos máximos permitidos desde que la persona física realizó el registro presencial. En caso contrario, para renovar su certificado, tendrá que personarse en la oficina de registro siguiendo los procedimientos de comprobación de la identidad de persona física desarrollados a tal efecto.



3. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

3.1 Solicitud de certificados

SIA solo admite solicitudes de emisión de certificado tramitados por una persona física mayor de edad, con capacidad plena de obrar y con capacidad jurídica suficiente.

El solicitante deberá cumplimentar el formulario de solicitud del certificado asumiendo la responsabilidad de la veracidad de la información reseñada, y tramitarlo ante SIA por medio de la Autoridad de Registro Reconocida presencialmente, donde procederá a verificar y firmar el documento de conformidad con la emisión del certificado cualificado de persona física vinculada a empresa de los datos de la solicitud. Con este hecho, acepta los requisitos establecidos en la DPC y en esta PC.

3.2 Tramitación de las solicitudes de certificados

Compete a la Autoridad de Registro la comprobación de la identidad del solicitante, la verificación de la documentación aportada y la constatación de que el solicitante ha firmado el documento de conformidad. Una vez completa la solicitud, la Autoridad de Registro, la remitirá al Prestador de Servicios de confianza para su tramitación.

3.3 Emisión de certificados

Previo a la generación de claves y certificados, es necesaria la validación y aprobación por la AR de la solicitud de certificado, y dados de alta los datos dentro del sistema del TSP.

Las claves para los certificados de ciudadano - Nivel alto se generan en el dispositivo cualificado de creación de firma electrónica (en adelante QSCD).

La AR verificará la identidad del solicitante, su vinculación con la entidad a la que representa y los datos que se incluyan en el certificado, siendo estos registrados en el sistema como un nuevo titular. El sistema generará los códigos de emisión de un solo uso, necesarios para el proceso de emisión del certificado.

El titular siguiendo la guía de emisión del certificado, hará uso de los códigos para iniciar el proceso de generación y emisión del certificado.



La AC verificará que el dispositivo en el que se han generado el par de claves es un dispositivo cualificado de creación de firma electrónica, procederá a la emisión del certificado y habilitará el acceso al mismo.

La AR notificará al solicitante la finalización satisfactoria del proceso de emisión.

SIA evitará generar certificados que caduquen con posterioridad a los certificados de la AC que los emitió.

3.3.1 Actuaciones de la AC durante la emisión de los certificados

Los procedimientos establecidos en esta sección también se aplicarán en caso de renovación de certificados cualificados en dispositivos cualificados de creación de firma, ya que ésta implica la emisión de nuevos certificados.

En la emisión de los certificados la AC:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada;
- Protege la confidencialidad e integridad de los datos de registro;
- Incluye en el certificado las informaciones establecidas en el artículo 11.2 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

En el ámbito de los dispositivos cualificados de creación de firma, una vez que el usuario se ha registrado en el sistema con nivel avanzado de garantía de registro y ha solicitado expresamente la emisión de sus certificados, dicha emisión se llevará a cabo la primera vez que el solicitante acceda al procedimiento de generación.

El sistema informará al solicitante de que se le va a emitir su certificado en un dispositivo cualificado de creación de firma y generará en ese momento su clave privada, la cual permanecerá almacenada en el dispositivo de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

La generación de los certificados deberá hacerse acorde con los requisitos que la Ley marca con respecto a los plazos máximos permitidos desde que el titular realizó el registro presencial.

3.3.2 Notificación al solicitante de la emisión por la AC del certificado

En la finalización del proceso de emisión del Certificado en un dispositivo cualificado de creación de firma, se informa al titular que se encuentra disponible dicho certificado para su uso, pudiendo ser usado a partir de ese mismo momento para los procesos de firma electrónica.



3.4 Aceptación del certificado

3.4.1 Forma en la que se acepta el certificado

La aceptación del certificado es la acción mediante la cual su titular da inicio a sus obligaciones respecto al TSP SIA. El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el firmante y SIA haya sido firmado y el certificado este en posesión del firmante.

Como evidencia de la aceptación deberá quedar firmado el documento de conformidad por ambas partes. El certificado se considera válido a partir de la fecha en que se firmó el documento de conformidad con la emisión del Certificado cualificado de ciudadano – Nivel alto.

3.4.2 Publicación del certificado por la AC

Los certificados no se publicarán en ningún repositorio de acceso libre.

3.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades

No se efectúan notificaciones a terceros.

3.5 Par de claves y uso del certificado

3.5.1 Uso de la clave privada del certificados por el titular

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta PC y de acuerdo con lo establecido en las extensiones “Key Usage” y “Extended Key Usage” del certificado.

Del mismo modo, el firmante solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en la DPC y PC y solo para lo que éstas establezcan.

Tras la expiración o revocación del certificado, el firmante dejará de usar la clave privada.

Los certificados cualificados de ciudadano – Nivel alto regulados en esta PC sólo pueden ser utilizados para la relación telemática segura con las administraciones públicas y entidades que acepten el certificado. Asimismo, permite al ciudadano aplicar firma electrónica cualificada a documentos electrónicos.



3.5.2 Uso de la clave pública y del certificado por los terceros aceptantes

Los terceros aceptantes sólo pueden depositar su confianza en los certificados para aquello que establece esta PC y de acuerdo con lo establecido en las extensiones “Key Usage” y “Extended Key Usage” del certificado.

Los terceros aceptantes han de realizar las operaciones de clave pública de manera satisfactoria para confiar en el certificado, así como asumir la responsabilidad de verificar el estado del certificado utilizando los medios que se establecen en la DPC y en esta PC. Asimismo, se obligan a las condiciones de uso establecidas en estos documentos.

3.6 Renovación de certificados sin cambio de claves

3.6.1 Circunstancias para la renovación de certificados sin cambio de claves

Todas las renovaciones de certificados realizadas en el ámbito de esta PC se realizarán con cambio de claves. En consecuencia, no se recogen el resto de puntos del apartado 4.6 que establece la RFC 3647, lo que implica, a efectos de esta PC su no estipulación.

3.7 Renovación de certificados con cambio de claves

3.7.1 Circunstancias para una renovación con cambio de claves de un certificado

Un certificado cualificado puede ser renovado, entre otros, por los siguientes motivos:

- Expiración de la vigencia del certificado.
- Cambio de datos contenidos en el certificado.
- Claves comprometidas o pérdida de fiabilidad de las mismas.
- Olvido de la contraseña establecida en la emisión del certificado, lo cual implica una inicialización en el caso del eToken.
- Cambio de formato.

Todas las renovaciones, con independencia de su causa, se realizarán con cambio de claves.

3.7.2 Quien puede pedir la renovación de un certificado

La renovación del certificado cualificado, la debe de solicitar el firmante del certificado.



3.7.3 Tramitación de las peticiones de renovación con cambio de claves

De forma automatizada, la AC informará al firmante de que su certificado está próximo a expirar. Para la renovación del mismo, aparecen dos formas de proceder:

- Si ha pasado un periodo inferior a cinco (5) años desde que el firmante se personó en la AR, éste deberá efectuar el proceso de emisión de certificados sin la necesidad de la personación en la AR.
- Si ha pasado un periodo superior a cinco (5) años desde que el firmante se personó en la AR, éste deberá personarse nuevamente en la AR y efectuar el proceso de emisión de certificados, como si del proceso inicial se tratara.

Si alguna de las condiciones establecidas en la DPC como en esta PC han sido modificadas, se deberá asegurar que tal hecho es conocido por el titular del certificado y que éste está de acuerdo con las mismas.

3.7.4 Notificación de la emisión de nuevos certificados al titular

Al tratarse de una renovación de certificados con cambio de claves, siguiendo el proceso de emisión de certificados como si del proceso inicial se tratara, una vez generado éste satisfactoriamente, se le notificara al firmante.

3.7.5 Forma de aceptación del certificado con nuevas claves

El titular confirmará electrónicamente la aceptación del certificado.

3.7.6 Publicación del certificado con las nuevas claves por la AC

El certificado cualificado de ciudadano – Nivel alto no se publicará.

3.7.7 Notificación de la emisión del certificado por la AC a otras Autoridades

No se efectúan notificaciones a terceros.



3.8 Modificación de certificados

3.8.1 Causas para la modificación de un certificado

Todas las modificaciones de certificados realizadas en el ámbito de esta PC se tratarán por la AR como una revocación de certificados y la emisión de un nuevo certificado.

En consecuencia, no se recogen el resto de puntos del apartado 3.8 que establece la RFC 3647, lo que implica, a efectos de esta PC su no estipulación.

3.9 Revocación y suspensión de certificados

La revocación de un certificado supone la pérdida de validez del mismo, y es irreversible.

La suspensión supone la pérdida temporal de validez de un certificado, y es reversible.

Las revocaciones y suspensiones tienen efecto desde el momento en que aparecen publicadas en la CRL.

La revocación de un certificado inhabilita el uso legítimo del mismo por parte del titular.

3.9.1 Causas para la revocación

Un certificado podrá ser revocado según se especifica en la DPC de SIA.

3.9.2 Quien puede solicitar la revocación

En el ámbito de la AC de SIA pueden solicitar la revocación de un certificado:

- El titular a nombre del cual fue expedido el certificado.
- El suscriptor, que es la entidad con personalidad jurídica que suscribe un contrato con SIA para la expedición de certificados.
- La Entidad de Registro que intervino en la emisión.
- La propia AC de SIA cuando tenga conocimiento de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.



3.9.3 Frecuencia de emisión de CRLs

La AC SIA, generará una nueva CRL cada 24 horas como máximo, o en su defecto, en el momento en que se produzca una revocación de un certificado cualificado ciudadano – Nivel alto.

3.9.4 Requisitos de comprobación en línea de la revocación

Este tipo de certificado tiene previsto un servicio de validación de certificados mediante el protocolo OCSP. Este servicio será de acceso libre y debe considerar:

- Comprobar la dirección contenida en la extensión AIA (Authority Information Access) del certificado.
- Comprobar que la respuesta OCSP está firmada. El certificado de firma de respuestas OCSP emitidos por AC SIA son conformes a la norma: RFC 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”.

3.9.5 Otras formas de divulgación de información de revocación

Para el uso del servicio de CRLs, que es de acceso libre, deberá considerarse que:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión “CRL Distribution Point” o en esta misma PC como en la DPC.
- El usuario deberá comprobar adicionalmente las CRLs pendientes de la cadena de certificación de la jerarquía.
- El usuario deberá asegurarse que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.
- Los certificados revocados que expiren no serán retirados de la CRL.

3.9.6 Requisitos especiales de renovación de claves comprometidas

No hay ninguna variación en las cláusulas anteriores cuando la revocación sea debida al compromiso de la clave privada.



3.9.7 Circunstancias para la suspensión

En el ámbito de la AC de SIA, no se contempla la suspensión (revocación temporal) de certificados. En todos los casos en los que sea necesario suspender un certificado, éste se revocará de forma permanente.

3.10 Servicios de información del estado de certificados

3.10.1 Características operativas

SIA ofrece un servicio gratuito de publicación en la web de Listas de Certificados Revocados (CRL) sin restricciones de acceso. Al igual que ofrece el servicio mediante protocolo OCSP según lo establecido en las políticas de certificación.

3.10.2 Disponibilidad del servicio

Los servicios de descarga de Listas de Certificados Revocados de SIA funcionarán 24 horas al día, 7 días a la semana y todos los días del año. SIA dispone de un CPD (Centro de Proceso de Datos) replicado, donde en caso de caída del nodo principal, éste asumirá dicho servicio.

3.11 Finalización de la suscripción

La extinción de la validez de un certificado se produce en los siguientes casos:

- Revocación del certificado por cualquiera de las causas recogidas en el apartado 4.9.1 de la DPC.
- Expiración del período de validez que figura en el certificado.

Si no se solicita la renovación del certificado la extinción de su validez supondrá la extinción de la relación entre el titular y la AC.

3.12 Custodia y recuperación de claves

3.12.1 Prácticas y políticas de custodia y recuperación de claves

El TSP en ningún momento podrá recuperar la clave de los usuarios. En caso de pérdida de la misma se deberá revocar el certificado y emitir uno nuevo.



En el ámbito del Certificado cualificado de ciudadano – Nivel Alto, la clave privada que se genera en SIAVAL SafeCert Server Signing System quedará custodiada por el TSP, teniendo en cuenta que el acceso a esta clave será realizada por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del firmante.

En este sentido, el acceso a dicha clave sólo puede ser efectuado por el titular de la misma mediante una aplicación al efecto donde el titular deberá estar debidamente autenticado. Posteriormente para la firma, deberá introducir el PIN de protección de su certificado tan sólo conocido por el titular y no almacenada en los sistemas, más un segundo factor de autenticación.

Sólo prestadores de servicios de certificación que expidan certificados cualificados podrán gestionar los datos de creación de firma electrónica en nombre del firmante. Para ello, podrán efectuar una copia de seguridad de los datos de creación de firma siempre que la seguridad de los datos duplicados sea del mismo nivel que la de los datos originales y que el número de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio. No se podrán duplicar los datos de creación de firma para ninguna otra finalidad.

La autoridad competente realiza copias de seguridad de las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.

En línea con la mención anterior, en el apartado cuarto del anexo II eIDAS se establece que, sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante, podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos cumpliendo lo anteriormente descrito en referencia a la duplicidad de datos.

En el caso de los dispositivos cualificados de creación de firma electrónica eToken, la autoridad ni custodiará, ni copiará la clave privada emitida bajo esta política. Por lo tanto, el TSP en ningún momento podrá recuperar la clave de los usuarios. En caso de pérdida de la misma se deberá revocar el certificado y emitir uno nuevo.



4. CONTROLES DE SEGURIDAD TÉCNICA

Los controles de seguridad técnica para los componentes internos de SIA, y concretamente para la AC raíz y AC subordinada en los procesos de emisión y firma de certificados, están descritos en la DPC de SIA.

En este apartado se recogen los controles de seguridad técnica para la emisión de certificados bajo esta PC.

4.1 Generación e instalación del par de claves

4.1.1 Generación del par de claves

Los pares de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan en un dispositivo cualificado de creación de firma electrónica o QSCD, que podrá ser un eToken, el cual cumple el nivel de seguridad FIPS 140-2 Nivel 3 y Common Criteria EAL4+ AVA_VAN 5, o SIAVAL SafeCert Server Signing System. Las claves son protegidas por el firmante con su PIN o contraseña.

4.1.2 Entrega de la clave privada al titular

La clave privada la genera el titular mediante el proceso de emisión provisto por el prestador, una vez ha sido personado y validado por la AR, por medio de un proceso seguro.

La clave privada se genera en un dispositivo cualificado de creación de firma electrónica bajo el control exclusivo del firmante y, por lo tanto, no existe ninguna entrega de la clave privada al titular.

4.1.3 Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada es generada junto a la clave privada sobre el dispositivo cualificado de creación de firma electrónica y es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10.

4.1.4 Tamaño de las claves

El tamaño de las claves de los certificados cualificados de ciudadano es de 2048 bits.



4.1.5 Parámetros de generación de la clave pública y verificación de la calidad

La clave pública de los certificados cualificados está codificada de acuerdo con RFC5280 y PKCS#1. El algoritmo de generación de claves es RSA.

4.1.6 Usos admitidos de la clave (campo KeyUsage de X.509 v3)

La clave definida por la presente política, y por consiguiente el certificado asociado, se utilizará para la firma electrónica de documentos electrónicos y la autenticación en servicios telemáticos.

A tal efecto, en el campo “key Usage” del certificado se ha incluido el siguiente uso:

Key Usage:

- nonRepudiation
- Digital Signature
- Key Encipherment

4.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos

En este punto se hace siempre referencia a las claves generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación. La información sobre las claves de las entidades que componen la Autoridad de Certificación se encuentra en la Declaración de Prácticas de Certificación (DPC) de SIA.

Los dispositivos empleados para la creación de claves utilizadas por los certificados cualificados de ciudadano - Nivel alto, son dispositivos cualificados de creación de firma electrónica o QSCD, los cuales pueden ser dispositivos eToken o dispositivo SIAVAL SafeCert Server Signing System.

4.2.1 Estándares para los módulos criptográficos

Los dispositivos cualificados de creación de firma electrónica basados en eToken, cumplen el nivel de seguridad FIPS 140-2 Nivel 3 y Common Criteria EAL4+ AVA_VAN 5.



El dispositivo cualificado de creación de firma electrónica SIAVAL SafeCert Server Signing System tiene su seguridad certificada conforme a la Declaración de Seguridad – ACO, versión 1.3, de enero de 2018, para el nivel de evaluación CAP-C.

4.2.2 Control multi-persona (n de m) de la clave privada

Las claves privadas generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran, bajo el control exclusivo de los firmantes. No está estipulado que exista control multi-persona para las claves privadas asociadas a los certificados de esta política.

4.2.3 Custodia de la clave privada

En el caso del dispositivo cualificado de creación de firma electrónica eToken no se custodian las claves privadas de los firmantes de los certificados definidos por la presente política.

En el caso del dispositivo cualificado de creación de firma electrónica SIAVAL SafeCert Server Signing System, la custodia de la clave privada la realiza la autoridad competente siendo únicamente los titulares de las mismas los que pueden acceder a dicha clave, introducir un identificador de usuario (DNI/NIE/Pasaporte), una contraseña tan sólo conocida por el titular y no almacenada en los sistemas de SIA, y un segundo factor de autenticación.

En todo momento el titular podrá modificar la contraseña personal de acceso a través de la consola del usuario.

4.2.4 Copia de seguridad de la clave privada

En el caso del dispositivo cualificado de creación de firma electrónica eToken, SIA no copiará las claves privadas de firma de los firmantes de los certificados definidos por la presente política. Es responsabilidad del firmante la conservación de sus datos de creación de firma y asegurar su confidencialidad y la protección de todo acceso o revelación.

En el caso del dispositivo cualificado de creación de firma electrónica SIAVAL SafeCert Server Signing System, la autoridad competente realiza copias de seguridad de las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.



4.2.5 Archivo de la clave privada

En el caso del dispositivo cualificado de creación de firma electrónica eToken, las claves privadas de los certificados cualificados de los firmantes definidos por la presente política nunca serán archivadas por la AC.

En el caso del dispositivo cualificado de creación de firma electrónica SIAVAL SafeCert Server Signing System, la autoridad competente mantiene, según la legislación vigente, las copias de seguridad con las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.

4.2.6 Transferencia de la clave privada a o desde el módulo criptográfico

En el caso del dispositivo cualificado de creación de firma electrónica eToken, la generación de las claves ligadas al certificado cualificado de Ciudadano- Nivel alto que se realizan en el propio dispositivo, no permite la exportación de la clave privada.

En el caso del dispositivo cualificado de creación de firma electrónica SIAVAL SafeCert Server Signing System, la autoridad competente mantiene, según la legislación vigente, las copias de seguridad con las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.

4.2.7 Almacenamiento de la clave privada en un módulo criptográfico

En el caso del dispositivo cualificado de creación de firma electrónica eToken, la generación de las claves ligadas al certificado cualificado de Ciudadano- Nivel alto que se realizan en el propio dispositivo, no permite la exportación de la clave privada.

En el caso del dispositivo cualificado de creación de firma electrónica SIAVAL SafeCert Server Signing System, la autoridad competente mantiene, según la legislación vigente, las copias de seguridad con las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.

4.2.8 Método de activación de la clave privada

La activación de la clave privada asociada a los certificados de esta PC, requiere la utilización de los programas o sistemas informáticos que sirvan para aplicar los datos de creación de firma. SIA requiere del uso de un dato de activación o contraseña para la utilización de la clave privada.



La activación de la clave privada requiere autenticación del titular en el sistema, siendo necesario introducir un identificador de usuario (DNI/NIE/Pasaporte), una contraseña tan sólo conocida por el titular y no almacenada en los sistemas, más un segundo factor de autenticación.

4.2.9 Método de desactivación de la clave privada

La desactivación se realizará cuando el firmante cierre la aplicación software de creación de firma o el módulo criptográfico asociado.

Si un titular autenticado en el sistema se equivoca repetidas veces en su contraseña de firma, tanto su clave como el certificado de firma se bloquearán automáticamente de manera temporal, pudiendo ser implementado una prueba de Turing (Captcha) en el caso del dispositivo SIAVAL SafeCert Server Signing System.

4.2.10 Método de destrucción de la clave privada

En términos generales, la destrucción siempre debe ser precedida por una revocación del certificado asociado a la clave, si éste estuviese todavía vigente.

La destrucción de la clave privada del firmante consiste en borrar la clave privada y el certificado asociado al usuario del dispositivo cualificado de creación de firma electrónica.

4.3 Otros aspectos de la gestión del par de claves

4.3.1 Periodos operativos de los certificados y periodo de uso para el par de claves

Los certificados emitidos al amparo de la presente política tienen una validez de tres (3) años. El par de claves utilizado para la emisión de los certificados se crea para cada emisión y por tanto también tiene una validez de tres (3) años.

En el caso que haya transcurrido más de 5 años desde la identificación inicial de la persona física, en cumplimiento del artículo 13 de la Ley de Firma Electrónica (*“La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará ...”*) la renovación deberá tramitarse ante SIA por medio de la Autoridad de Registro Reconocida presencialmente.

La caducidad deja automáticamente sin validez a los Certificados de Ciudadano, originando el cese permanente de su operatividad conforme a los usos que le son propios.

La caducidad de un Certificado de Ciudadano inhabilita el uso legítimo por parte del firmante.



4.4 Datos de activación

4.4.1 Generación e instalación de los datos de activación

Los datos de activación de la clave privada, consisten en la creación de la contraseña que custodiará las claves y la generación de las mismas, en el dispositivo cualificado de creación de firma electrónica.

4.4.2 Protección de los datos de activación

El propio firmante generará el par de claves en el dispositivo cualificado de creación de firma electrónica. Por lo tanto, el firmante es el responsable de la protección de los datos de activación de su clave privada. SIA requiere una contraseña o PIN para el acceso a la clave privada y requerida también para el proceso de firma, junto a un mecanismo de segundo factor de autenticación en el caso del dispositivo SIAVAL SafeCert Server Signing System.

La contraseña de acceso a la clave privada del certificado es confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados en los servicios ofrecidos a través de una red de comunicaciones; por lo tanto, deben tenerse en cuenta unas normas de seguridad para su custodia y uso:

- Memorícelas y procure no anotarlas en ningún documento físico ni electrónico que el Titular conserve.
- No envíe ni comunique a nadie ni por ningún medio, ya sea vía telefónica, correo electrónico, etc.
- Recuerde que son personales e intransferibles. Si cree que esta información puede ser conocida por otra persona, debe cambiarla. El uso de las mismas por persona distinta del Titular presupone grave negligencia por parte del mismo y permite la activación de las claves privadas para poder realizar operaciones de firma electrónica en su nombre. Es obligación del titular notificar la pérdida de control sobre su clave privada, a causa del compromiso de las mismas, ya que es motivo de revocación del certificado asociado a dichas claves.
- Como medida adicional, deberá abstenerse de escoger un número relacionado con sus datos personales, así como cualquier otro código que pueda resultar fácilmente predecible por terceras personas (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones de la misma cifra, secuencias de cifras que ya forman parte de su número de DNI, etc.)
- Se recomienda cambiarlo periódicamente.



5. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

5.1 Perfil de certificado

Los certificados emitidos por los sistemas de SIA, serán conformes con lo dispuesto en las siguientes normas y especificaciones técnicas:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile
- RFC 5280 “Internet X.509 Public Key Infrastructure. Certificate and CRL Profile”.
- RFC 3739 “Internet x509 Public Key Infrastructure. Qualified Certificates Profile”.
- Perfiles de Certificados derivados del Real Decreto 1671/2009 y está adaptado a las disposiciones de la Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, la Ley40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Publico (LRJ) y al Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS).
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

5.1.1 Número de versión

Los certificados siguen el estándar definido X.509 versión 3.

5.1.2 Extensiones del certificado

Los certificados emitidos por SIA de ciudadano – Nivel alto, vinculan la identidad de una persona física (Nombre, Apellidos y número de Documento Nacional de Identidad) a una determinada clave pública, sin incluir ningún tipo de atributos al mismo. Para garantizar la autenticidad y no repudio, toda esta información estará firmada electrónicamente por el prestador de servicios de confianza encargada de la emisión.

Los datos personales del ciudadano, incluidos en el certificado son:

- Nombre y apellidos.
- Número de Documento Nacional de Identidad.
- Clave pública asociada al ciudadano.



Las extensiones utilizadas en los certificados son:

- Authority Key Identifier.
- Subject Key Identifier.
- KeyUsage. Calificada como crítica.
- ExtKeyUsage.
- CRL Distribution Point.
- Authority Information Access.
- Qualified Certificate Statements.
- CertificatePolicies.
- Subject Alternative Name.

Los certificados emitidos con la consideración de cualificados incorporan adicionalmente el identificador de objeto (OID) definido por el ETSI EN 319 412-5, sobre perfiles de certificados cualificados: 0.4.0.1862.1.1.

Los certificados que son expedidos con la calificación de cualificados están identificados en la extensión QcStatements con OID 1.3.6.1.5.5.7.1.3, que indica la existencia de una lista de declaraciones “QcStatements” codificadas en formato ASN.1, conforme a las normas vigentes, concretamente los certificados cualificados de ciudadano – Nivel alto incluyen las siguientes declaraciones:

- QcCompliance, establece la calificación con la que se ha realizado la emisión del “Certificado cualificado”.
- QcEuRetentionPeriod, determina el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este. En el caso de SIA, es de quince (15) años.
- QcType, detalla el tipo de certificado emitido, firma, sello o web.
- QcSyntax-v2, habilitado indicando el OID. 0.4.0.194121.1.1.
- QcPDS, indica URL de la PDS, un resumen de la DPC en inglés del servicio prestado.
- QcSSCD, indica el uso de dispositivo cualificado de creación de firma electrónica.

QcSSCD, indica el uso de dispositivo cualificado de creación de firma electrónica. SIA tiene definida una política de asignación de OIDs dentro de su rango privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados de SIA comienza por el prefijo 1.3.6.1.4.1.39131.10.3.

Por otro lado, el certificado contiene más información sobre el firmante en la extensión SubjectAltName. En esta extensión se utilizará el sub-campo DirectoryName que incluye atributos definidos por SIA con la información del firmante con objeto de proporcionar una forma sencilla de obtener los datos personales del firmante.



Los OIDs de los atributos definidos por SIA en el sub-campo DirectoryName de la extensión SubjectAltName se describen en el cuadro siguiente.

OID	Concepto	Descripción
1.3.6.1.4.1.39131.10.2.1	Tipo de certificado	Tipo de certificado
1.3.6.1.4.1.39131.10.2.2	Nombre	Nombre del usuario
1.3.6.1.4.1.39131.10.2.3	Apellido1	Primer apellido del usuario
1.3.6.1.4.1.39131.10.2.4	Apellido2	Segundo apellido del usuario
1.3.6.1.4.1.39131.10.2.5	DNI/NIE/Pasaporte	DNI/NIE/Pasaporte del usuario
1.3.6.1.4.1.39131.10.2.8	Nombre Colegio	Nombre del colegio profesional
1.3.6.1.4.1.39131.10.2.9	Número de Colegio	Identificados del colegio profesional
1.3.6.1.4.1.39131.10.2.10	Número de Colegiado	Número o Identificador del colegiado
1.3.6.1.4.1.39131.10.2.11	Comunidad	Comunidad de la Oficina
1.3.6.1.4.1.39131.10.2.12	Provincia	Provincia de la Oficina
1.3.6.1.4.1.39131.10.2.13	Localidad	Localidad de la Oficina
1.3.6.1.4.1.39131.10.2.14	Numero de Oficina	Número o Identificador de la Oficina
1.3.6.1.4.1.39131.10.2.15	Tipo de Oficina	Tipo de la Oficina

Tabla 3 – Definición extensión SubjectAltName



5.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador del algoritmo criptográfico con Objeto (OID): SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

5.1.4 Formatos de nombre

Los certificados emitidos por SIA contienen el “distinguished name X.500” del emisor y del titular del certificado en los campos “issuer” y “subject” respectivamente.

5.1.5 Restricciones de nombre

No se emplean restricciones de nombres, aunque los nombres contenidos en los certificados se ajustan a “Distinguished Names” X.500, que son únicos y no ambiguos.

El DN para los certificados ciudadano – Nivel alto, estará compuesto de los siguientes elementos:

- CN, GN, SN, serialNumber, C

Los atributos CN (Common Name), GN (Givenname), SN (Surname) y serialNumber del DN serán los que distingan a los DN entre sí. La sintaxis de estos atributos es la siguiente:

- CN, dependiendo del documento con el que se realice la identificación del titular, del tipo de certificado (FIRMA o AUTH) y de la información que se muestre en el CN, las opciones son las siguientes:
 - DNI, CN = Apellido1 Apellido2 Nombre – DNI NNNNNNNNA FIRMA|AUTH
 - NIE, CN = Apellido1 Apellido2 Nombre – NIE ANNNNNNNNA FIRMA|AUTH
 - Pasaporte, CN = Apellido1 Apellido2 Nombre – PAS AAAAAAAAAA FIRMA|AUTH
 - No se muestra nada, independientemente del documento aportado, CN = Apellido1 Apellido2 Nombre FIRMA|AUTH
- GN = Nombre
- SN = Apellido1
- serialNumber = Si es certificado de firma, codificado según las normas ETSI EN 319 412-1 y RFC 3739 apartado 3.2.6.1, relativo a la codificación de la información semántica. Las opciones en función del documento de identidad serían las siguientes:
 - DNI sería IDCES-NNNNNNNNNA
 - NIE sería IDCES-ANNNNNNNNNA
 - Pasaporte sería PASES-AAAAAAAAA

Si es de autenticación, la codificación del campo sería:



- DNI sería NNNNNNNNA
- NIE sería ANNNNNNNNA
- Pasaporte sería XXXXXXXXX

- C = País del ciudadano. En este caso, España. El atributo “C” (country) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en PrintableString.

Se incluirá un literal (AUTH o FIRMA) que identifique la tipología del certificado al final del CN, tal y como se indica en el punto del CN, en este apartado.

5.1.6 Identificador de objeto (OID) de la Política de Certificación

El OID de la presente PC es 1.3.6.1.4.1.39131.10.1.9. Los identificadores de los certificados expedidos bajo la presente Política de Certificación son los siguientes:

Política de Certificados cualificados de Ciudadano – Nivel alto	1.3.6.1.4.1.39131.10.1.9 (QSCD portable) 1.3.6.1.4.1.39131.10.1.17 (QSCD centralizado)
QCP-n-qscd	0.4.0.194112.1.2

Tabla 4 – OID políticas de certificación

5.1.7 Uso de la extensión “PolicyConstraints”

No estipulado.

5.1.8 Sintaxis y semántica de los “PolicyQualifier”

La extensión “Certificate Policies” contiene los siguientes “Policy Qualifiers”:

- URL DPC: contiene la URL donde puede obtener la última versión de la DPC y de las Políticas de Certificación asociadas.



- Notice Reference: Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

Y el siguiente “Policy Identifier”:

- QCP-n-qscd: indicación de certificado cualificado de firma en SSCD, acorde a eIDAS. Sólo para certificado de firma.
- NCP+: Indicación de certificado acorde a una política normalizada, en dispositivo seguro acorde al Reglamento eIDAS. Solo para certificado de autenticación.

5.1.9 Tratamiento semántico para la extensión “Certificate Policy”

La extensión “Certificate Policy” permite identificar la política y el tipo de certificado asociado al certificado.

5.2 Perfil de Certificado cualificado de Ciudadano – Nivel alto

Certificado cualificado de ciudadano – Nivel alto FIRMA		
Nombre atributo	Valor	Observaciones
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada emisora	
Signature Algorithm	SHA-256 con RSA-2048	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Serial Number (serialNumber)	A82733262	
Common Name (CN)	SIA SUB01	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 3 años	



Subject (Asunto)		
Country (C)	ES	España
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	Razón social de SIA
Organizational Unit (OU)	<Código de entidad suscriptor>	
Serial Number (serialNumber)	IDCES-<DNI> IDCES-<NIE> PASES-<Pasaporte>	DNI/NIE/Pasaporte de usuario según ETSI EN 319 412-1
Surname	<Apellido1>	Primer apellido
Given Name	<Nombre>	Nombre de pila
Common Name (CN)	<Apellido1> <Apellido2> <Nombre>[– DNI <DNI> NIE <NIE> PAS <Pasaporte>] FIRMA	Nombre, apellidos y DNI/NIE/Pasaporte del ciudadano
Subject Public Key Info	Clave pública (RSA-2048 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage		Marcado como crítica
Digital Signature	0 (no seleccionado)	
Content Commitment (nonRepudiation)	1 (seleccionado)	
Key Encipherment	0 (no seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	0 (no seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
Extended Key Usage		
Email Protection	0 (no seleccionado)	
Client Authentication	0 (no seleccionado)	
CRL Distribution Point		
Distribution Point 1	https://psc.sia.es/ac_sub01.crl	
Distribution Point 2	http://psc.sia.es/ac_sub01.crl	
Authority Info Access		



Access Method	Id-ad-ocsp	
Access Location	https://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Method	https://psc.sia.es/ac_sub01.crt	
Qualified Certificate Statements (Codificado en formato ASN.1)		
QcCompliance	OID 0.4.0.1862.1.1	Certificado cualificado
QcEuRetentionPeriod	15 años	Duración custodia
QcSSCD	OID 0.4.0.1862.1.4	Uso de dispositivo cualificado de creación de firma electrónica
QcType	OID 0.4.0.1862.1.6	
id-etsi-qct-esign	OID 0.4.0.1862.1.6.1	
QCSyntax-v2	OID 1.3.6.1.5.5.7.11.2	
id-etsi-qcs-semanticId-Natural	OID 0.4.0.194121.1.1	
QcPDS	OID 0.4.0.1862.1.5	
PdsLocation	https://psc.sia.es/en (en)	
Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.9 1.3.6.1.4.1.39131.10.1.17	QSCD portable o QSCD centralizado
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	“Certificado cualificado de firma electrónica de Ciudadano de nivel alto. Condiciones de uso y vías de contacto en: https://psc.sia.es”	
Policy Identifier	QCP-n-qscd	
Subject Alternative Name		
Tipo del certificado	OID: 1.3.6.1.4.1.39131.10.2.1: CIUDADANO	
Nombre	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del usuario
Primer apellido	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido1>	Primer apellido del usuario
Segundo apellido	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido2>	Segundo apellido del usuario
DNI	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI> <NIE> <Pasaporte>	DNI NIE Pasaporte del usuario
Nombre Colegio	OID: 1.3.6.1.4.1.39131.10.2.8: <Nombre Colegio>	Nombre del colegio profesional



Número de Colegio	OID: 1.3.6.1.4.1.39131.10.2.9: <Nº de Colegio>	Identificados del colegio profesional
Número de Colegiado	OID: 1.3.6.1.4.1.39131.10.2.10: <Nº de Colegiado>	Número o Identificador del colegiado
Comunidad	OID: 1.3.6.1.4.1.39131.10.2.11: <Comunidad>	Comunidad de la Oficina
Provincia	OID: 1.3.6.1.4.1.39131.10.2.12: <Provincia>	Provincia de la Oficina
Localidad	OID: 1.3.6.1.4.1.39131.10.2.13: <Localidad>	Localidad de la Oficina
Numero de Oficina	OID: 1.3.6.1.4.1.39131.10.2.14: <Nº Oficina>	Número o Identificador de la Oficina
Tipo de Oficina	OID: 1.3.6.1.4.1.39131.10.2.15: <Tipo Oficina>	Tipo de la Oficina

Tabla 5 – Perfil certificado Firma

Certificado cualificado de ciudadano – Nivel alto AUTH		
Nombre atributo	Valor	Observaciones
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada emisora	
Signature Algorithm	SHA-256 con RSA-2048	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Serial Number (serialNumber)	A82733262	
Common Name (CN)	SIA SUB01	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 3 años	
Subject (Asunto)		
Country (C)	ES	España
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	Razón social de SIA
Organizational Unit (OU)	<Código de entidad suscriptora>	



Serial Number (serialNumber)	<DNI> <NIE> <Pasaporte>	DNI/NIE/Pasaporte del usuario
Surname	<Apellido1>	Primer apellido
Given Name	<Nombre>	Nombre de pila
Common Name (CN)	<Apellido1> <Apellido2> <Nombre>[– DNI <DNI> NIE <NIE> PAS <Pasaporte>] AUTH	Nombre, apellidos y DNI/NIE/Pasaporte del ciudadano
Subject Public Key Info	Clave pública (RSA-2048 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage		Marcado como crítica
Digital Signature	1 (seleccionado)	
Content Commitment (nonRepudiation)	0 (no seleccionado)	
Key Encipherment	1 (seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	0 (no seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
Extended Key Usage		
Email Protection	0 (no seleccionado)	
Client Authentication	1 (seleccionado)	
CRL Distribution Point		
Distribution Point 1	https://psc.sia.es/ac_sub01.crl	
Distribution Point 2	http://psc.sia.es/ac_sub01.crl	
Authority Info Access		
Access Method	Id-ad-ocsp	
Access Location	https://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Method	https://psc.sia.es/ac_sub01.crt	



Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.9 1.3.6.1.4.1.39131.10.1.17	QSCD portable o QSCD centralizado
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	“Certificado de Ciudadano de nivel alto, autenticación. Condiciones de uso y vías de contacto en: https://psc.sia.es/ ”	
Policy Identifier	NCP+	
Subject Alternative Name		
Tipo del certificado	OID: 1.3.6.1.4.1.39131.10.2.1: CIUDADANO	
Nombre	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del usuario
Primer apellido	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido1>	Primer apellido del usuario
Segundo apellido	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido2>	Segundo apellido del usuario
DNI	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI> <NIE> <Pasaporte>	DNI NIE Pasaporte del usuario
Nombre Colegio	OID: 1.3.6.1.4.1.39131.10.2.8: <Nombre Colegio>	Nombre del colegio profesional
Número de Colegio	OID: 1.3.6.1.4.1.39131.10.2.9: <Nº de Colegio>	Identificados del colegio profesional
Número de Colegiado	OID: 1.3.6.1.4.1.39131.10.2.10: <Nº de Colegiado>	Número o Identificador del colegiado
Comunidad	OID: 1.3.6.1.4.1.39131.10.2.11: <Comunidad>	Comunidad de la Oficina
Provincia	OID: 1.3.6.1.4.1.39131.10.2.12: <Provincia>	Provincia de la Oficina
Localidad	OID: 1.3.6.1.4.1.39131.10.2.13: <Localidad>	Localidad de la Oficina
Numero de Oficina	OID: 1.3.6.1.4.1.39131.10.2.14: <Nº Oficina>	Número o Identificador de la Oficina
Tipo de Oficina	OID: 1.3.6.1.4.1.39131.10.2.15: <Tipo Oficina>	Tipo de la Oficina

Tabla 6 – Perfil certificado Autenticación



6. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

6.1 Tarifas

6.1.1 Tarifas de emisión de certificado o renovación

Las tarifas a aplicar se establecerán en la página web del prestador SIA.

6.1.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos bajo esta Política es gratuito y por tanto no hay ninguna tarifa de aplicación sobre el mismo.

6.1.3 Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicara ninguna tarifa.

6.1.4 Tarifas de otros servicios tales como información de políticas

No se aplicara ninguna tarifa por el servicio de información sobre esta política ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

6.1.5 Política de reembolso

La política de reembolso se detallará en la página web del prestador SIA.