

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 Sello

Electrónico – Nivel medio

OID: 1.3.6.1.4.1.39131.10.1.12

Versión: 1.0



SI-0013/2006



STI-01/2008



ISO/IEC 15504



ISO 22301

ISO 9001  
ISO 14001  
BUREAU VERITAS  
Certification





### HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

| Revisión | Fecha               | Autor | Descripción                   |
|----------|---------------------|-------|-------------------------------|
| 1.0      | 12 de junio de 2017 | SIA   | Primera versión del documento |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |
|          |                     |       |                               |



# INDICE

|  |           |
|--|-----------|
| <b>1. INTRODUCCIÓN .....</b>   | <b>8</b>  |
| 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.....   | 13        |
| 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        |
| <b>2. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS.....</b>           | <b>16</b> |
| 2.1 Nombres.....   | 16        |
| 2.1.1 Uso de seudónimos .....  | 16        |
| 2.2 Validación de la identidad inicial .....   | 16        |
| 2.2.1 Métodos para probar la posesión de la clave privada .....                          | 16        |
| 2.2.2 Autenticación de la identidad de una persona física .....                          | 16        |
| 2.2.3 Información no verificada sobre el solicitante .....                               | 17        |
| 2.2.4 Comprobación de las facultades de representación.....                              | 17        |
| 2.3 Identificación y autenticación para peticiones de renovación de claves.....          | 17        |
| <b>3. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS.....</b>        | <b>18</b> |
| 3.1 Solicitud de certificados .....  | 18        |
| 3.2 Tramitación de las solicitudes de certificados .....                                 | 18        |
| 3.3 Emisión de certificados.....   | 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        |
| <b>4. CONTROLES DE SEGURIDAD TÉCNICA.....</b>  | <b>25</b> |
| 4.1 Generación e instalación del par de claves .....   | 25        |
| 4.1.1 Generación del par de claves.....  | 25        |
| 4.1.2 Entrega de la clave privada al titular.....  | 25        |
| 4.1.3 Entrega de la clave pública al emisor del certificado .....                                | 25        |
| 4.1.4 Tamaño de las claves .....   | 25        |
| 4.1.5 Parámetros de generación de la clave pública y verificación de la calidad .....            | 25        |
| 4.1.6 Usos admitidos de la clave (campo KeyUsage de X.509 v3).....                               | 26        |
| 4.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos ..... | 26        |
| 4.2.1 Estándares para los módulos criptográficos .....   | 26        |
| 4.2.2 Control multi-persona (n de m) de la clave privada.....                                    | 26        |
| 4.2.3 Custodia de la clave privada .....   | 27        |
| 4.2.4 Copia de seguridad de la clave privada.....  | 27        |
| 4.2.5 Archivo de la clave privada .....  | 27        |
| 4.2.6 Transferencia de la clave privada a o desde el módulo criptográfico .....                  | 27        |
| 4.2.7 Almacenamiento de la clave privada en un módulo criptográfico.....                         | 27        |
| 4.2.8 Método de activación de la clave privada.....  | 28        |
| 4.2.9 Método de desactivación de la clave privada .....  | 28        |
| 4.2.10 Método de destrucción de la clave privada .....   | 28        |
| 4.3 Otros aspectos de la gestión del par de claves.....  | 28        |
| 4.3.1 Periodos operativos de los certificados y periodo de uso para el par de claves .....       | 28        |
| 4.4 Datos de activación .....  | 29        |
| 4.4.1 Generación e instalación de los datos de activación.....                                   | 29        |
| 4.4.2 Protección de los datos de activación.....   | 29        |
| <b>5. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP .....</b>   | <b>30</b> |
| 5.1 Perfil de certificado .....  | 30        |
| 5.1.1 Número de versión .....  | 30        |
| 5.1.2 Extensiones del certificado .....  | 30        |
| 5.1.3 Identificadores de objeto (OID) de los algoritmos .....                                    | 33        |



|  |           |
|--|-----------|
| 5.1.4 Formatos de nombre .....   | 33        |
| 5.1.5 Restricciones de nombre .....  | 33        |
| 5.1.6 Identificador de objeto (OID) de la Política de Certificación .....  | 33        |
| 5.1.7 Uso de la extensión "PolicyConstraints" .....                        | 34        |
| 5.1.8 Sintaxis y semántica de los "PolicyQualifier" .....                  | 34        |
| 5.1.9 Tratamiento semántico para la extensión "Certificate Policy" .....   | 34        |
| 5.2 Perfil de Certificado de Sello Electrónico .....                       | 34        |
| <b>6. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD .....</b>                    | <b>38</b> |
| 6.1 Tarifas .....  | 38        |
| 6.1.1 Tarifas de emisión de certificado o renovación .....                 | 38        |
| 6.1.2 Tarifas de acceso a los certificados .....                           | 38        |
| 6.1.3 Tarifas de acceso a la información de estado o revocación .....      | 38        |
| 6.1.4 Tarifas de otros servicios tales como información de políticas ..... | 38        |
| 6.1.5 Política de reembolso .....  | 38        |



## RELACION DE TABLAS

|   |    |
|---|----|
| Tabla 1 – Datos identificación DPC.....                 | 10 |
| Tabla 2 – Organización responsable.....                 | 15 |
| Tabla 3 – Definición extensión SubjectAltName SIA ..... | 32 |
| Tabla 4 – Definición extensión SubjectAltName AAPP..... | 32 |
| Tabla 5 – OID políticas de certificación .....          | 34 |
| Tabla 6 – Perfil certificado.....                       | 37 |



# 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 Sello Electrónico – Nivel medio, 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 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal 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 el reglamento eIDAS.

En este contexto, los Certificados de Sello Electrónico de nivel medio serán emitidos como **Certificados Cualificados de Sello Electrónico** cumpliendo los requisitos establecidos en el anexo III 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 Sello Electrónico – Nivel medio solo pueden ser utilizados por el propio titular para el procesamiento automático. La emisión de estos certificados se realizará en soporte software o en Módulos de Seguridad Hardware (HSM).

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 Sello Electrónico.  |
| Versión del documento | 1.0   |
| Estado del documento  | Vigente   |
| Fecha de emisión      | 17/02/2017  |
| Fecha de caducidad    | No aplicable  |
| OID                   | 1.3.6.1.4.1.39131.10.1.12   |
| Ubicación de la PC    | <a href="https://psc.sia.es/">https://psc.sia.es/</a>   |
| DPC relacionada       | Declaración de Prácticas de Certificación de la PKI de SIA<br><br>OID 1.3.6.1.4.1.39131.10.1.1.1.0<br><br>Disponible en <a href="https://psc.sia.es/">https://psc.sia.es/</a> |

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 Sello Electrónico – Nivel medio.

En este ámbito, SIA actúa como prestador de servicios de confianza, emitiendo los certificados electrónicos cualificados de firma y proveyendo servicios de firma electrónica basada en un certificado cualificado para la creación de firmas electrónicas automatizadas, 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, apartados 1.3.2 y 9.6.2.

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.
- 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 jurídicas 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 este caso es la entidad, ya sean corporaciones, entidades privadas, públicas o de derecho público, representadas por una persona física, el titular. Los datos de la entidad que representa, serán incluidos en el certificado, de forma opcional podrán ser incluidos los de la persona física, el cual será el responsable de la custodia de las claves privadas de dicho certificado.

El suscriptor también recibe el nombre de firmante, según se define en el artículo 6 de la Ley 59/2003 de Firma Electrónica y en el artículo 3 del reglamento eIDAS.

### 1.3.5 Solicitante

Los solicitantes de certificados cualificados de Sello Electrónico – Nivel medio, son los propios usuarios con poderes de representación de 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 y a la entidad a la que representa 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.

Los certificados emitidos bajo los criterios de esta política están indicados para soportar sello electrónico avanzado con certificados cualificados, tal y como está definido en los artículos 36 y 37 de eIDAS, garantizando lo siguiente para todos los sellos:

- a) estar vinculado al creador del sello de manera única;
- b) permitir la identificación del creador del sello;
- c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo y
- d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

### 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 III. 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 sello electrónico 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 sello proporciona las siguientes garantías:

- No repudio de origen

Asegura que el documento proviene de la entidad de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del sello electrónico. 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 una determinada entidad, es decir la firma es la prueba efectiva del contenido y de la autoría del documento (garantía de “no repudio”).

- Integridad

El certificado cualificado de Sello Electrónico, 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<br>Alcor Plaza Edificio B<br>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 Sello Electrónico – Nivel medio 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 Sello Electrónico, en soporte software o en Módulos de Seguridad Hardware (HSM).

Una vez que el solicitante ha firmado el documento de aceptación y se ha completado el proceso de registro e identificación, nos remitirá su csr (PKCS#10) correspondiente clave privada, que el mismo almacenará en su sistema de forma protegida, de modo que garantice el control exclusivo por su parte. Finalmente, si todo el proceso ha sido satisfactorio, se le entregara un certificado x.509 (PKCS#11) que dicho solicitante tendrá que cargar en su sistema.

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 solicitante del certificado se realiza mediante su personación ante el operador del punto de registro, acreditándose mediante presentación del Documento Nacional de Identidad (DNI), pasaporte español 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, así como el documento acreditativo de la representación que ejerce.

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

La AR verificará con sus propias fuentes de información el resto de datos y atributos a incluir en el certificado (subject), debiendo guardar la documentación acreditativa de la validez de aquellos datos no verificables por dichas fuentes.

## 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 cualificados, 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 Sello Electrónico de los datos de la solicitud, aportando además la documentación que acredite su representación. 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, la constatación de que el solicitante ha firmado el documento de conformidad y que la vinculación con la entidad para la que se solicita el sello electrónico es válida, por los medios de los que dispone el TSP. 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 Sello Electrónico - Nivel medio se generan en soporte software o en Módulos de Seguridad Hardware (HSM).

El proceso de emisión se realizará en los siguientes pasos:

1. 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.
2. El solicitante enviara por correo un CSR, que previamente habrá generado en su sistema.



3. La AC emitirá el certificado x.509 de la clave pública asociado a su clave privada, y se le entrega al solicitante.

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

## 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 una hoja de aceptación firmada por el firmante. El certificado se considera válido a partir de la fecha en que se firmó la hoja de aceptación.

### 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 Sello Electrónico – Nivel medio 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 titular aplicar de forma automatizada firma electrónica avanzada 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 3.6 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.
- 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. Comprobando que los restantes datos de representación del suscriptor continúan siendo válidos.

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 y siguiendo el proceso de emisión de certificados como si del proceso inicial se tratara, el sistema informará al titular de que se ha procedido a la renovación telemática de su certificado y le informará del nuevo periodo de validez del mismo, informando también de que el anterior certificado ha sido revocado y que el certificado quedará sin efecto.

### 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 Sello Electrónico 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 el cual solicito la expedición el certificado tras la comprobación de su relación ante la entidad.
- El suscriptor, que es la entidad con personalidad jurídica que suscribe un contrato con SIA para la expedición del certificado.
- Otra persona física con nivel de apoderamiento sobre la entidad a la que el suscriptor estaba representando.
- 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 la 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 de Sello Electrónico.

### 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
- 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

Para este tipo de certificados, el TSP en ningún momento custodiará ni copiará la clave privada emitida por los suscriptores. Por lo tanto el TSP en ningún momento podrá recuperar la clave de los firmantes. 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 privada y pública para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan en soporte software, o en Módulos de Seguridad Hardware (HSM).

#### 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.

#### 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 de generación de claves 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 sello electrónico 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.

### 4.2.1 Estándares para los módulos criptográficos

El módulo criptográfico empleado en la emisión de los certificados adscritos a esta Política de Certificación es un dispositivo software. Si el firmante utiliza un navegador Internet Explorer o Chrome en un entorno Microsoft Windows, el equipo utilizará CSP (Cryptographic Service Provider). En Unix/Linux y navegadores Mozilla Firefox, se emplea PKCS#11. También cabe la posibilidad de que la entidad suscrita emplee el uso de Módulos de Seguridad Hardware (HSM).

### 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

Se pueden dar dos casos de custodia de claves:

- En Software, las claves son almacenadas por el aplicativo que hace uso del sello electrónico.
- El HSM, las claves con almacenadas en un módulo criptográfico que cumple con la certificación FIPS 140-2 nivel 3.

### 4.2.4 Copia de seguridad de la clave privada

En cualquier caso, 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. Tanto si las claves son custodiadas en software como en HSM, si se realizan copias de seguridad de las mismas, ha de ser manteniendo los mismos niveles de seguridad, como mínimo.

### 4.2.5 Archivo de la clave privada

Las claves privadas de los certificados cualificados de los firmantes nunca serán archivadas por la AC.

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

La generación de las claves vinculadas al certificado cualificado de Sello Electrónico se realiza en el propio dispositivo software del sistema. Se puede utilizar un fichero en formato PKCS#12 para transferir la clave privada a otro sistema, pero la responsabilidad de proteger este fichero y esta operación es del propio usuario.

En el caso de que las claves privadas se generen directamente en un módulo criptográfico de seguridad (HSM), estas claves se generarán dentro del propio dispositivo y no pueden ser exportadas.

### 4.2.7 Almacenamiento de la clave privada en un módulo criptográfico

Las claves privadas se generan en un dispositivo software. Las claves pueden ser exportadas mediante un fichero con el formato PKCS#12 que permite almacenar las claves privadas con sus certificados protegiéndolo con un cifrado con clave simétrica. Es responsabilidad del firmante el aseguramiento y confidencialidad de este fichero.



Los firmantes, también pueden disponer de Módulos de Seguridad Hardware (HSM), los cuales incrementan el nivel de protección de dichas claves.

#### 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 no controla ni define el control de acceso lógico a la clave privada de estos dispositivos de creación de firma, pero recomienda el uso de un dato de activación o contraseña para la utilización de la clave privada.

En el caso en que las claves se generen dentro de un HSM, hay que tener en cuenta que los mecanismos de seguridad empleados son superiores, teniendo que activar y emplear las medidas de seguridad que estos proporcionan.

#### 4.2.9 Método de desactivación de la clave privada

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

#### 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 software.

### 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.



La caducidad deja automáticamente sin validez a los Certificados Cualificados de Sello Electrónico, originando el cese permanente de su operatividad conforme a los usos que le son propios e 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 cuando estas sean generadas en un soporte Software. En el caso en que se emplee un HSM, el proceso de activación de la clave privada constara de un mayor nivel de complejidad.

### 4.4.2 Protección de los datos de activación

Si las claves son generadas en software, se recomienda proteger los datos de activación de la clave privada, por medio de una contraseña. En el caso de emplear módulos criptográficos de seguridad, que se apliquen las medidas de seguridad que estos ofrecen activadas.



## 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.
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal 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 Sello Electrónico, vinculan la identidad de una entidad a una determinada clave pública, sin la necesidad de incluir ningún tipo de atributos de la persona física 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 de la entidad del sello electrónico, incluidos en el certificado son:

- Nombre de la entidad u Organización.



- Número de Identificación Fiscal (NIF) de la entidad u Organización según norma técnica.
- País

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 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 persona física representante de persona jurídica 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, indicativo del tipo de certificado, firma, sello o web.
- QcSyntax-V2, habilitado indicando el OID. 0.4.0.194121.1.2.
- QcPDS, indica URL de la PDS, un resumen de la DPC en inglés del servicio prestado.

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 1.3.6.1.4.1.39131.10.2.

Por otro lado, el certificado contiene más información en la extensión SubjectAltName. En esta extensión se utilizará el sub-campo DirectoryName 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 responsable del sello           |
| 1.3.6.1.4.1.39131.10.2.3 | Apellido1           | Primer apellido del responsable del sello  |
| 1.3.6.1.4.1.39131.10.2.4 | Apellido2           | Segundo apellido del responsable del sello |
| 1.3.6.1.4.1.39131.10.2.5 | DNI                 | DNI del responsable del sello              |

Tabla 3 – Definición extensión SubjectAltName SIA

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

| OID                  | Concepto                   | Descripción  |
|----------------------|----------------------------|--|
| 2.16.724.1.3.5.6.2.1 | Tipo de certificado        | Tipo de certificado.                               |
| 2.16.724.1.3.5.6.2.2 | Entidad Suscriptora        | Nombre de la Entidad suscriptora                   |
| 2.16.724.1.3.5.6.2.3 | NIF Entidad Suscriptora    | Número de identificación de la Entidad suscriptora |
| 2.16.724.1.3.5.6.2.4 | DNI/NIE                    | DNI/NIE del responsable del sello                  |
| 2.16.724.1.3.5.6.2.5 | Descripción del componente | Descripción del componente que posee el sello      |
| 2.16.724.1.3.5.6.2.6 | Nombre                     | Nombre de pila del responsable del sello           |
| 2.16.724.1.3.5.6.2.7 | Apellido 1                 | Primer apellido del responsable del sello          |
| 2.16.724.1.3.5.6.2.8 | Apellido 2                 | Segundo apellido del responsable del sello         |
| 2.16.724.1.3.5.6.2.9 | Email                      | Correo electrónico del responsable del sello       |

Tabla 4 – Definición extensión SubjectAltName AAPP





### 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 de Persona Física Representante de Persona Jurídica, estará compuesto de los siguientes elementos:

- CN, O, OI, OU y C

Los atributos CN (Common Name), O (Organization), OI (Organization Identifier) y OU (Organization Unit) del DN serán los que distinguan a los DN entre sí. La sintaxis de estos atributos es la siguiente:

- CN = Denominación del sistema
- O = Organización del creador del sello
- OI = NIF de la entidad en formato VATES – NIF entidad, según norma ETSI EN 319 412-1
- OU = Naturaleza del certificado
- C = País del titular. En este caso, España. El atributo “C” (country) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en PrintableString.

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

El OID de la presente PC es 1.3.6.1.4.1.39131.10.1.12. Los identificadores de los certificados expedidos bajo la presenta Política de Certificación son los siguientes:

|  |                           |
|--|---------------------------|
| Política de Certificado Cualificado de Sello Electrónico | 1.3.6.1.4.1.39131.10.1.12 |
|--|---------------------------|



QCP-I

0.4.0.194112.1.1

Tabla 5 – 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-I: indicación de certificado cualificado de firma, acorde a eIDAS.
- OID del tipo de certificado, OID:2.16.724.1.3.5.6.2

### 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 de Sello Electrónico

| <b>Certificado Cualificado de Sello Electrónico – Nivel medio</b> |              |                      |
|---|--------------|----------------------|
| <b>Nombre atributo</b>  | <b>Valor</b> | <b>Observaciones</b> |
| <b>Campos x509 v1</b>   |              |                      |



|  |   |                            |
|--|---|----------------------------|
| <b>Versión</b>                             | V3  |                            |
| <b>Serial Number</b>                       | Número secuencial único, asignado automáticamente por la AC subordinada emisora     |                            |
| <b>Signature Algorithm</b>                 | SHA-256 con RSA-2048  |                            |
| <b>Issuer Distinguished Name (Emisor)</b>  |   |                            |
| <b>Country (C)</b>                         | ES  |                            |
| <b>Organization (O)</b>                    | SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA                                     |                            |
| <b>Organizational Unit (OU)</b>            | QUALIFIED CA  |                            |
| <b>Serial Number (serialNumber)</b>        | A82733262   |                            |
| <b>Common Name (CN)</b>                    | SIA SUB01   |                            |
| <b>Validity</b>                            |   |                            |
| <b>Not Before</b>                          | Fecha de emisión del certificado  |                            |
| <b>Not After</b>                           | Fecha de emisión + 3 años   |                            |
| <b>Subject (Asunto)</b>                    |   |                            |
| <b>Country (C)</b>                         | ES  | España                     |
| <b>Organization (O)</b>                    | <NOMBRE DE LA ENTIDAD>  | Nombre de la Organización  |
| <b>Organization Identifier (OI)</b>        | VATES-<NIF de la ENTIDAD>   |                            |
| <b>Organizational Unit (OU)</b>            | SELLO ELECTRÓNICO   | Naturaleza del certificado |
| <b>Common Name (CN)</b>                    | <Denominación del Sistema>  |                            |
| <b>Subject Public Key Info</b>             | Clave pública (RSA-2048 Bits), codificada de acuerdo con el algoritmo criptográfico |                            |
| <b>Extensiones x509 v3</b>                 |   |                            |
| <b>Authority Key Identifier</b>            | Identificador de la clave pública del emisor  |                            |
| <b>Subject Key Identifier</b>              | Identificador de la clave pública del firmante del certificado                      |                            |
| <b>KeyUsage</b>                            |   | Marcado como crítica       |
| <b>Digital Signature</b>                   | 1 (seleccionado)  |                            |
| <b>Content Commitment (nonRepudiation)</b> | 1 (seleccionado)  |                            |
| <b>Key Encipherment</b>                    | 1 (seleccionado)  |                            |
| <b>Data Encipherment</b>                   | 0 (no seleccionado)   |                            |
| <b>Key Agreement</b>                       | 0 (no seleccionado)   |                            |
| <b>Key Certificate Signature</b>           | 0 (no seleccionado)   |                            |
| <b>CRL Signature</b>                       | 0 (no seleccionado)   |                            |
| <b>EncipherOnly</b>                        | 0 (no seleccionado)   |                            |
| <b>DecipherOnly</b>                        | 0 (no seleccionado)   |                            |



|   |   |                         |
|---|---|-------------------------|
| <b>Extended Key Usage</b>   |   |                         |
| <b>Email Protection</b>   | 0 (no seleccionado)   |                         |
| <b>Client Authentication</b>  | 0 (no seleccionado)   |                         |
| <b>CRL Distribution Point</b>   |   |                         |
| <b>Distribution Point 1</b>   | <a href="https://psc.sia.es/ac_sub01.crl">https://psc.sia.es/ac_sub01.crl</a>   |                         |
| <b>Distribution Point 2</b>   | <a href="http://psc.sia.es/ac_sub01.crl">http://psc.sia.es/ac_sub01.crl</a>   |                         |
| <b>Authority Info Access</b>  |   |                         |
| <b>Access Method</b>  | id-ad-ocsp  |                         |
| <b>Access Location</b>  | <a href="https://psc.sia.es/ocsp">https://psc.sia.es/ocsp</a>   |                         |
| <b>Access Method</b>  | id-ad-calssuers   |                         |
| <b>Access Method</b>  | <a href="https://psc.sia.es/ac_sub01.crt">https://psc.sia.es/ac_sub01.crt</a>   |                         |
| <b>Qualified Certificate Statements (Codificado en formato ASN.1)</b> |   |                         |
| <b>QcCompliance</b>   | OID 0.4.0.1862.1.1  | Certificado cualificado |
| <b>QcEuRetentionPeriod</b>  | 15 años   | Duración custodia       |
| <b>QcType</b>   | OID 0.4.0.1862.1.6.   |                         |
| <b>id-etsi-qct-eseal</b>  | OID 0.4.0.1862.1.6.2  | Certificado de sello    |
| <b>QCSyntax-v2</b>  | OID 1.3.6.1.5.5.7.11.2  |                         |
| <b>id-etsi-qcs-SemanticsId-Legal</b>                                  | OID 0.4.0.194121.1.2  |                         |
| <b>QcPDS</b>  | OID 0.4.0.1862.1.5  |                         |
| <b>PdsLocation</b>  | <a href="https://psc.sia.es/en">https://psc.sia.es/en</a> (en)  |                         |
| <b>Certificate Policies</b>   |   |                         |
| <b>Policy Identifier</b>  | 1.3.6.1.4.1.39131.10.1.12   |                         |
| <b>Policy Qualifier ID</b>  | Especificación de la DPC  |                         |
| <b>CPS Pointer</b>  | <a href="https://psc.sia.es/">https://psc.sia.es/</a>   |                         |
| <b>User Notice</b>  | “Certificado cualificado de sello electrónico de nivel medio. Condiciones de uso y vías de contacto en: <a href="https://psc.sia.es">https://psc.sia.es</a> ” |                         |
| <b>Policy Identifier</b>  | QCP-I   |                         |
| <b>Policy Identifier</b>  | 2.16.724.1.3.5.6.2  |                         |
| <b>Subject Alternative Name</b>                                       |   |                         |
| <b>Tipo del certificado</b>   | OID: 2.16.724.1.3.5.6.2.1: SELLO ELECTRONICO DE NIVEL MEDIO   |                         |



|                                   |  |  |
|-----------------------------------|--|--|
| <b>Nombre entidad suscriptora</b> | OID: 2.16.724.1.3.5.6.2.2: <Entidad Suscriptora>     | Entidad suscriptora                          |
| <b>NIF entidad suscriptora</b>    | OID: 2.16.724.1.3.5.6.2.3: <NIF entidad suscriptora> | NIF Entidad suscriptora                      |
| <b>DNI/NIE del responsable</b>    | OID: 2.16.724.1.3.5.6.2.4: <DNI / NIE>               | DNI / NIE del responsable del sello          |
| <b>Descripción del componente</b> | OID: 2.16.724.1.3.5.6.2.5: <Descripción Componente>  | Descripción del componente                   |
| <b>Nombre del responsable</b>     | OID: 2.16.724.1.3.5.6.2.6: <Nombre>                  | Nombre del responsable del sello             |
| <b>Apellido 1 del responsable</b> | OID: 2.16.724.1.3.5.6.2.7: <Apellido 1>              | Apellido 1 del responsable del sello         |
| <b>Apellido 2 del responsable</b> | OID: 2.16.724.1.3.5.6.2.8: <Apellido 2>              | Apellido 2 del responsable del sello         |
| <b>Email del responsable</b>      | OID: 2.16.724.1.3.5.6.2.9: <Email>                   | Correo electrónico del responsable del sello |

Tabla 6 – Perfil certificado



## 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.