**SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA**
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

psc.sia.es

# PC - SIA

## Política de Certificación

## Certificados reconocidos de Empleado Público

## OID: 1.3.6.1.4.1.39131.10.1.4

**Versión: 1.0**

## HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

| Revisión | Fecha | Autor | Descripción |
|---|---|---|---|
| 1.0 | 22 de octubre de 2015 | SIA | Primera versión del documento |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# INDICE

# RELACION DE TABLAS

# 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 certificación, Sistemas Informáticos Abiertos Sociedad Anónima (en adelante SIA), del tipo Certificado reconocido de Empleado Público - 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.

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 de Empleado Público - Nivel medio, son certificados reconocidos de persona física según la Ley 59/2003 de firma electrónica que identifican los empleados públicos (en cualquiera de sus categorías: funcionario, laboral fijo, etc) así como su vinculación a una concreta Entidad Pública en virtud del cargo que ocupa en la misma, según los requisitos establecidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y alineado con La Disposición derogatoria única segunda de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas informa que queda derogada expresamente, entre otras, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y en la Disposición final séptima se añade que, la presente Ley entrará en vigor al año de su publicación en el «Boletín Oficial del Estado.

Los Certificados de Empleado Público - Nivel medio serán emitidos como Certificados Electrónicos Reconocidos cumpliendo los requisitos del anexo I de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, así como lo dispuesto a tal efecto en la Ley 59/2003, de 19 de diciembre, de firma electrónica. El prestador de servicios de certificación, SIA, cumplirá los requisitos expresados en el anexo II de la directiva indicada anteriormente, y desarrollado en Ley 59/2003, de 19 de diciembre, de firma electrónica.

Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta estándares en materia de certificados reconocidos, en concreto:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile

- 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.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

Los Certificados reconocidos de Empleado Público - Nivel medio sólo pueden ser utilizados por el propio empleado público. La emisión de estos certificados se realizará en un dispositivo de creación de firma.

En esta PC se detalla y completa lo estipulado en la Declaración de Prácticas de Certificación (en adelante DPC) del Prestador de Servicios de Certificación 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 Empleado Público - Nivel medio |
|---|---|
| **Versión del documento** | 1.0 |
| **Estado del documento** | Vigente |
| **Fecha de emisión** | 27/07/2015 |
| **Fecha de caducidad** | No aplicable |
| **OID** | 1.3.6.1.4.1.39131.10.1.4 |
| **Ubicación de la PC** | https://psc.sia.es/ |

| | |
|---|---|
| **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 https://psc.sia.es/ |

Tabla 1 – Datos identificación PC

## 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.
- Las Autoridades de Registro.
- Los Firmantes.
- Los Suscriptores.
- Las Terceras partes aceptantes de los certificados emitidos.
- Los solicitantes.

### 1.3.1 Autoridad de Certificación

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. 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 finales, en este caso, la emisión de Certificados reconocidos de Empleado Público - Nivel medio.

### 1.3.2 Autoridades de Registro

La gestión de las solicitudes y la gestión de la 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.

Principalmente, la propia entidad pública (Administración, Órgano o Entidad de derecho público) es quien actuará como Autoridad de Registro de SIA para la gestión de las solicitudes y la gestión de la emisión de certificados a aquellas personas físicas con las que tenga vinculación directa como empleados públicos, en cualquiera de sus categorías (funcionario, laboral fijo, etc) . La propia entidad pública podrá ser el Suscriptor de todos estos certificados emitidos.

Cada entidad pública 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 el empleado público, en cualquiera de sus categorías (funcionario, laboral fijo, etc), como la persona física titular identificada en el certificado y que haga uso del mismo. .

### 1.3.4 Suscriptor

En el caso de una vinculación entre el firmante y una entidad pública mediante una relación laboral o contractual. El suscriptor es la entidad pública con personalidad jurídica (Administración, Órgano o Entidad de derecho público) que suscribe un contrato con SIA para la expedición de certificados reconocidos a sus empleados públicos, en cualquiera de sus categorías (funcionario, laboral fijo, etc).

### 1.3.5 Solicitante

Los solicitantes de certificados de Empleado Público son los propios empleados públicos vinculados a la Entidad Pública (Administración, organismo o entidad de derecho público).

### 1.3.6 Terceras Partes

Las terceras partes aceptantes, son las personas físicas o jurídicas 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 Practicas 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 Practicas 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.

## 1.5 Administración de Políticas

### 1.5.1 Organización responsable

Esta PC es propiedad de SIA.

| Nombre | SIA |
|---|---|
| **Dirección correo** | info@sia.es |
| **Dirección postal** | Avenida de Europa, 2<br>Alcor Plaza Edificio B<br>Parque Oeste Alcorcón<br>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 reconocidos de Empleado Público - 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 reconocido de Empleado Público.

El par de claves es generado por el empleado público de la entidad pública (Administración, Órgano o Entidad de derecho público) y la demostración de posesión de la clave privada consiste en la utilización del certificado. En el proceso de registro, el método para probar la posesión de la clave privada por el solicitante será la entrega de un PKCS#10 o una prueba equivalente.

### 2.2.2 Autenticación de la identidad de una persona física

La autentificación de la identidad de la persona física identificada en el certificado se realiza mediante su personación ante el operador de la Autoridad 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.

### 2.2.3 Información no verificada sobre el solicitante

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

### 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.

# 3. REQUISITOS OPREACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

## 3.1 Solicitud de certificados

SIA solo admite solicitudes de emisión de certificados expedidos a Empleados Públicos, personas físicas mayores 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 reconocido de Empleado Público 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 y circunstancias personales del solicitante, la verificación de la documentación aportada y la constatación de que el solicitante ha firmado el documento de conformidad con la emisión del certificado reconocido de Empleado Público. Una vez completa la solicitud, la Autoridad de Registro la remitirá al Prestador de Servicios de Certificación 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 PSC.

El proceso de emisión se realizara en los siguientes pasos:

1. La AR verificará la identidad del solicitante, su vinculación con la entidad pública suscriptora y los datos que se incluyan en el certificado.
2. Envío por parte de AR de un correo electrónico al firmante de forma segura, con los pasos a seguir para completar el proceso y un enlace.
3. El solicitante procede a generar el par de claves en un dispositivo de creación de firmas siguiendo las instrucciones enviadas por la AR.
4. La AR envía la petición de generación de certificado a la AC.

5. Generación del certificado asociado a las claves generadas, y confirmación al solicitante de la generación de las mismas tras el proceso satisfactorio.
6. El solicitante descarga de forma segura el certificado en su ordenador.

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 PSC SIA. El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el firmante y SIA haya sido firmado y los medios que permitan hacer uso del certificado se encuentren 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 reconocido de Empleado Público.

### 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 reconocidos de Empleado Público - Nivel medio regulados en esta PC sólo pueden ser utilizados para autenticarse frente a los sistemas y ciudadanos y prestar los servicios de firma electrónica de documentos relacionados con la actividad ordinaria de la Entidad Pública y a los que se quiera dotar de control de identidad del firmante como empleado público, de integridad del documento firmado y no repudio del Empleado Público.

### 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 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 reconocido 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 reconocido, la debe de solicitar el firmante del certificado o el suscriptor.

### 3.7.3 Tramitación de las peticiones de renovación con cambio de claves

De forma automatizada, la AC informara al firmante 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.

### 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 reconocido de Empleado Público - Nivel medio no se publicará en ningún repositorio de acceso libre.

### 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 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.

### 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 (empleado público) a nombre del cual fue expedido el certificado.
- 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 reconocido de Empleado Público - Nivel medio.

### 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, este se revocara 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 su Web de Listas de Certificados Revocados (CRL) sin restricciones de acceso.

### 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, este 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 PSC en ningún momento custodiará ni copiará la clave privada emitida a las personas físicas (empleados públicos) vinculadas a la entidad pública. Por lo tanto, el PSC 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 de creación de firma. Las claves privadas se generan en el dispositivo de creación de firma protegido por el firmante.

### 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 ajustado a la Ley.

La clave privada se genera en un dispositivo de creación de firma 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 de generación y custodia 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 reconocidos de Empleado Público - Nivel medio 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 reconocidos 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 relacionados con la entidad pública suscriptora.

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

**Key Usage:** Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos.

## 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 de creación de firma. 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.

### 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

Bajo ningún caso, se custodian las claves privadas de firma de los firmantes de los certificados definidos por la presente política.

### 4.2.4 Copia de seguridad de la clave privada

Bajo ningún concepto, SIA 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.

### 4.2.5 Archivo de la clave privada

Las claves privadas de los certificados reconocidos 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 ligadas al certificado reconocido de Empleado Público - Nivel medio se realiza en el propio dispositivo de creación de firma, el cual no permite la exportación de la clave privada.

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

Las claves privadas se generan en un dispositivo de creación de firma. Las claves no pueden ser exportadas, y es responsabilidad del firmante el aseguramiento y confidencialidad del acceso a las mismas.

### 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.

### 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.

### 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 de creación de firma.

## 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.

## 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.

### 4.4.2 Protección de los datos de activación

El propio firmante generará el par de claves en el dispositivo de creación de firma. Por lo tanto, el firmante es el responsable de la protección de los datos de activación de su clave privada. SIA recomienda una contraseña o PIN para el acceso a la clave privada y requerida para el proceso de firma, junto a segundo mecanismo de segundo factor de autenticación.

# 5. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

## 5.1 Perfil de certificado

Se ha tenido en cuenta los siguientes estándares y normas europeas en la definición de los certificados emitidos por los sistemas de SIA:

- 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 Electrónicos para la Administración General del Estado según Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Los perfiles están definidos en el Anexo II de la Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- 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 Empleado Público - Nivel medio, vinculan la identidad de una persona física, empleado público, (Nombre, Apellidos y número de Documento Nacional de Identidad) a una determinada clave pública, sin incluir ningún tipo de atributos en el mismo. Para garantizar la autenticidad y no repudio, toda esta información estará firmada electrónicamente por el prestador de servicios de certificación encargado de la emisión.

Los campos singulares para identificar al certificado de Empleado Público son:

- Descripción del tipo de certificado.
- Datos de identificación personal de titular del certificado
    - Nombre y apellidos.
    - Número de Documento Nacional de Identidad (DNI) o Número de Identificación del Extranjero (NIE).

- Nombre de la entidad en la que está suscrito el empleado.
- Número de Identificación Fiscal (NIF) de la entidad.
- Número de identificación de personal.
- Correo electrónico.
- Unidad Organizativa.
- Puesto o cargo.

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 reconocidos incorporan adicionalmente el identificador de objeto (OID) definido por ETSI EN 319 412-5, sobre perfiles de certificados reconocidos: 0.4.0.1862.1.1.

Los certificados que son expedidos con la calificación de reconocidos 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 “QcStatement”, conforme a las normas vigentes. En concreto, los certificados reconocidos de Empleado Público - Nivel medio incluye las siguientes declaraciones:

- QcCompliance, establece la calificación con la que se ha realizado la emisión del “Certificado reconocido”.
- 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.

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 sobre el firmante en la extensión SubjectAltName. En esta extensión se utilizarán los sub-campos: Nombre RFC822, que contiene la dirección de correo electrónico asociado al empelado público, y DirectoryName incluyendo este último atributos con la información del firmante con objeto de proporcionar una forma sencilla de obtener los datos personales del firmante y el suscriptor.

Los OIDs en el sub-campo DirectoryName de la extensión SubjectAltName se describen en el cuadro siguiente.

| OID | Concepto | Descripción |
|---|---|---|
| 2.16.724.1.3.5.3.2.1 | Tipo de certificado | Tipo de certificado. |
| 2.16.724.1.3.5.3.2.2 | Entidad Suscriptora | Nombre de la Entidad Publica |
| 2.16.724.1.3.5.3.2.3 | NIF Entidad Suscriptora | Numero único de identificación de la Entidad Pública |
| 2.16.724.1.3.5.3.2.4 | DNI/NIE | DNI/NIE del Empleado Público |
| 2.16.724.1.3.5.3.2.5 | Número de Identificación Personal | Número identificativo del Empleado Público |
| 2.16.724.1.3.5.3.2.6 | Nombre | Nombre de pila del Empleado Público |
| 2.16.724.1.3.5.3.2.7 | Apellido 1 | Primer apellido del Empleado Público |
| 2.16.724.1.3.5.3.2.8 | Apellido 2 | Segundo apellido del Empleado Público |
| 2.16.724.1.3.5.3.2.9 | Email | Correo electrónico del Empleado Público |
| 2.16.724.1.3.5.3.2.10 | Unidad Organizativa | Unidad dentro de la Administración, en la que está incluido el Empleado Público |
| 2.16.724.1.3.5.3.2.11 | Puesto o cargo | Puesto desempeñado por el Empleado Público |
| 1.3.6.1.4.1.39131.10.2.8 | Colegio profesional | Nombre del colegio profesional al que pertenece el titular |
| 1.3.6.1.4.1.39131.10.2.9 | ID Colegio / ID Entidad | ID Colegio / ID Entidad al que pertenece el titular |
| 1.3.6.1.4.1.39131.10.2.10 | ID Colegiado | Número de identificacion de la colegiatura del Titular |

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 los nombres

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 Empleado Público – nivel medio, estará compuesto de los siguientes elementos:

- CN, T, SN, SerialNumber, G, OU, O, C

Los atributos CN (Common Name), G (Givename), SN (Surname) y serialNumber del DN serán los que distingan a los DN entre sí.

La sintaxis de estos atributos es la siguiente:

- CN = Nombre Apellido1 Apellido2 – <DNI> NNNNNNNNA
- T = Cargo o Puesto
- SN = Apellidos
- SerialNumber = DNI/NIE en formato NNNNNNNNA
- G = Nombre
- OU = Definición del tipo del certificado
- O = Entidad a la que está vinculado el empleado público.
- C = País. 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 1.3.6.1.4.1.39131.10.1.4.

Los identificadores de los certificados expedidos bajo la presenta Política de Certificación son los siguientes:

| | |
|---|---|
| Política de Certificados de Empleado Público - Nivel medio | 1.3.6.1.4.1.39131.10.1.4 |

Tabla 4 – OID política 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.

### 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 Certificado de Empleado Público - Nivel medio

| ***Certificado de Empleado Público - Nivel medio*** | | |
|---|---|---|
| **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)** | <Código de país de dos letras> | País |
| **Organization (O)** | <Razón social de la Entidad Pública> | Razón social de la organización |
| **Organizational Unit (OU)** | Certificado electrónico de empleado público | Tipo de certificado |
| **Given Name (G)** | <Nombre> | Nombre de pila |
| **Serial Number (serialNumber)** | <DNI/NIE> | DNI/NIE del empleado público |
| **Surname (SN)** | <Apellido1> <Apellido2> | Primer y segundo apellido |
| **Title (T)** | Cargo ejercido en la entidad pública por parte del titular | Cargo |
| **Common Name (CN)** | <Nombre> <Apellido1> <Apellido2> – DNI <DNI/NIE> | Nombre, apellidos y DNI/NIE del empleado público |
| **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)** | **1 (seleccionado)** | |
| **Key Encipherment** | **1 (seleccionado)** | |
| **Data Encipherment** | **1 (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) | |
| **ExtendedKeyUsage** | | |
| **Autenticación del cliente** | OID: 1.3.6.1.5.5.7.3.2 | |
| **Correo seguro** | OID: 1.3.6.1.5.5.7.3.4 | |
| **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-calssuers | |
| **Access Method** | https://psc.sia.es/ac_sub01.crt | |
| **Access Method** | Id-ad-ocsp | |
| **Access Location** | https://psc.sia.es/ocsp | |
| **Qualified Certificate Statements** | | |
| **QcCompliance** | OID 0.4.0.1862.1.1 | Certificado reconocido |
| **QcEuRetentionPeriod** | 15 años | Duración custodia |
| **Certificate Policies** | | |
| **Policy Identifier** | 1.3.6.1.4.1.39131.10.1.4 | |
| **Policy Qualifier ID** | Especificación de la DPC | |
| **CPS Pointer** | https://psc.sia.es | |
| **User Notice** | “Certificado reconocido de Empleado Público - Nivel medio. Consulte las condiciones de uso en https://psc.sia.es. Contacto: Avda. de Europa, 2 Alcor Plaza. Edificio B - Parque Oeste Alcorcón - 28922 Alcorcón - Madrid” | |
| **Subject Alternative Name** | | |
| **Nombre RFC822** | < correo electrónico de la persona responsable del certificado > | Correo electrónico de la persona |

| | | |
|---|---|---|
| | | responsable del certificado |
| **Tipo de certificado** | OID: 2.16.724.1.3.5.3.2.1: Certificado electrónico de empleado público | |
| **Nombre** | OID: 2.16.724.1.3.5.3.2.6: <Nombre> | Nombre del responsable |
| **Primer apellido** | OID: 2.16.724.1.3.5.3.2.7: <Apellido1> | Primer apellido del responsable |
| **Segundo apellido** | OID: 2.16.724.1.3.5.3.2.8: <Apellido2> | Segundo apellido del responsable |
| **DNI/NIE** | OID: 2.16.724.1.3.5.3.2.4: <DNI/NIE> | DNI/NIE del responsable |
| **Entidad Pública Suscriptora** | OID: 2.16.724.1.3.5.3.2.2: <Razón social de la Entidad Pública suscriptora> | Entidad Pública suscriptora |
| **NIF** | OID: 2.16.724.1.3.5.3.2.3: <NIF de Entidad Pública suscriptora > | NIF de la Entidad Pública suscriptora |
| **Correo Electrónico** | OID: 2.16.724.1.3.5.3.2.9: <- correo electrónico de la persona responsable del certificado > | Correo electrónico de la persona responsable del certificado |
| **Puesto o Cargo** | OID: 2.16.724.1.3.5.3.2.11: <Puesto desempeñado> | Puesto desempeñado por el suscriptor del certificado dentro de la Entidad Pública |
| **Unidad** | OID: 2.16.724.1.3.5.3.2.10: <Unidad Organizativa> | Unidad, dentro de la Entidad Pública , en la que está incluida el suscriptor del certificado |
| **NIP** | OID: 2.16.724.1.3.5.3.2.5:<Número de Identificacion del suscriptor del certificado > | Número identificativo |
| **Colegio profesional** | OID.1.3.6.1.4.1.39131.10.2.8: <Colegio profesional> | Nombre del colegio profesional al que pertenece el titular. OPCIONAL. |
| **ID Colegio / ID Entidad** | OID.1.3.6.1.4.1.39131.10.2.9: <ID Colegio/ID Entidad> | ID Colegio / ID Entidad al que pertenece el titular. OPCIONAL. |
| **ID Colegiado** | OID.1.3.6.1.4.1.39131.10.2.10: <ID Colegiado> | Número de identificacion de la colegiatura del Titular. OPCIONAL. |

Tabla 5 – Perfil certificado

# 6. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

## 6.1 Tarifas

### 6.1.1 Tarifas de emisión de certificado o renovación

SIA aplicará a las Entidades Públicas o Privadas las tarifas aprobadas para la prestación de los servicios de certificación o, en su defecto, las tarifas acordadas en el convenio o encomienda de gestión formalizados para tal efecto.

### 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 vendrá detallada, como parte de las tarifas acordadas, en el convenio o encomienda de gestión formalizados para tal efecto.