An Indra company

PC - SIA

Política de Certificación
Certificados cualificados de Sello Electrónico

OID: 1.3.6.1.4.1.39131.10.1.12	(Nivel medio)
OID: 1.3.6.1.4.1.39131.10.1.12.1	(AAPP – Nivel medio)
OID: 1.3.6.1.4.1.39131.10.1.12.2	(PSD2 – Nivel medio)
OID: 1.3.6.1.4.1.39131.10.1.13	(Nivel alto)
OID: 1.3.6.1.4.1.39131.10.1.13.1	(AAPP – Nivel alto)
OID: 1.3.6.1.4.1.39131.10.1.13.2	(PSD2 – Nivel alto)

Versión: 1.9

SIA | PC

Certificado cualificado de Sello Electrónico

Fecha: 23 de junio de 2025

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

Revisión	Fecha	Autor	Descripción
1.0	12 de junio de 2017	SIA	Primera versión del documento
1.1	23 de abril de 2018	SIA	Corrección de erratas en la definición del certificado cualificado de Sello Electrónico para el caso de las entidades de carácter no público.
1.2	11 de Junio de 2019	SIA	Corrección sobre los puntos de distribución de CRLs. Se añade uso de autenticación de cliente y protección de correo.
1.3	22 de Junio 2020	SIA	Inclusión de certificados de sello electrónico PSD2.
1.4	17 de noviembre de 2020	SIA	Adecuación a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
1.5	18 de mayo de 2021	SIA	Revisión normativa y tiempo máximo de los certificados de 5 años. Se añaden certificados de nivel alto en QSCD.
1.6	01/04/2022	SIA	Se realizan modificaciones en el OID de los certificados para indicar un OID distinto por cada perfil de certificado de sello.
1.7	16 de enero de 2023	SIA	Cambio de plantilla, actualización de domicilio social y corrección de erratas.
1.8	16 de abril de 2023	SIA	Revisión de nuevas versiones ETSI y mayor detalle en atributos opcionales de *"Subject Alternative Name"*.
1.9	23 de junio de 2025	SIA	Adecuación a eIDAS-2 y revisión general de redacción.

INDICE

RELACION DE TABLAS

1. Introducción

1.1 Resumen

El presente documento recoge la Política de Certificación correspondiente a los certificado 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”, “Certificado cualificado de Sello Electrónico PSD2 – Nivel medio”, “Certificado cualificado de Sello Electrónico – Nivel alto” y “Certificado cualificado de Sello Electrónico PSD2 – Nivel alto”, que define los mecanismos y procedimientos para la emisión, gestión, revocación, renovación y cualquier otro proceso que afecte al ciclo de vida de los certificados electrónicos emitidos por la AC de SIA.

La Política de Certificación (en adelante PC) de SIA se ha estructurado conforme al documento RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC-3647. Cuando no se haya previsto nada en alguna sección o esta venga referida en la DPC, no se contemplará dicho apartado.

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

- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- 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.
- ETSI TS 119 495: Electronic Signatures and Trust Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.

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 y por el que se deroga la Directiva 1999/93/CE.

- Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) nº 910/2014 en lo que respecta al establecimiento del Marco Europeo de Identidad Digital (eIDAS2).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
- Reglamento de Ejecución (UE) 2024/2690 de la Comisión de 17 de octubre de 2024 por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad. (Actos de Implementación NIS2).
- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados (modificada por la Orden ETD/743/2022, de 26 de julio).
- Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (modificado por el Reglamento de Ejecución (UE) 2022/960 de la Comisión, de 20 de junio de 2022).
- 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.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Resolución de 29 de noviembre de 2012 de la Secretaría de Estado de Administraciones Públicas, por la que 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.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- DIRECTIVA (UE) 2017/1564 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de septiembre de 2017 sobre ciertos usos permitidos de determinadas obras y otras prestaciones protegidas por derechos de autor y derechos afines en favor de personas ciegas, con discapacidad visual o con otras dificultades para acceder a textos impresos, y por la que se modifica la Directiva 2001/29/CE relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE. (PSD2)
- Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros. (RTS on SCA & CSC)
- Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, por el que se transpone al ordenamiento jurídico español la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, relativa a los servicios de pago en el mercado interior (PSD2).

La regulación aplicable en España, en la fecha de elaboración del presente documento de políticas de certificación, son la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el reglamento eIDAS.

En este contexto, los Certificados de Sello Electrónico de nivel medio y alto serán emitidos como **Certificados Cualificados de Sello Electrónico** cumpliendo los requisitos establecidos en el anexo III de eIDAS, y desarrollado en Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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.

Tanto los Certificados cualificados de Sello Electrónico – Nivel medio y alto como los Certificados cualificados de Sello Electrónico PSD2 – Nivel medio y alto, sólo pueden ser utilizados por el propio titular para el procesamiento automático. La emisión de estos certificados se realizará en Módulos de Seguridad Hardware (HSM) QSCD (Qualified Seal Creation Device) , de acuerdo con lo establecido en el Reglamento europeo eIDAS u opcionalmente en software para los de nivel medio.

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 Sello Electrónico
Versión del documento	1.9
Estado del documento	Vigente
Fecha de emisión	16/05/2025
Fecha de caducidad	No aplicable
OIDs	1.3.6.1.4.1.39131.10.1.12 (Nivel medio para entidades no públicas)
	1.3.6.1.4.1.39131.10.1.12.1 (Nivel medio para AAPP)
	1.3.6.1.4.1.39131.10.1.12.2 (Nivel medio PSD2)
	1.3.6.1.4.1.39131.10.1.13 (Nivel alto para entidades no públicas)
	1.3.6.1.4.1.39131.10.1.13.1 (Nivel alto para AAPP)
	1.3.6.1.4.1.39131.10.1.13.2 (Nivel alto PSD2)
Ubicación de la PC	https://psc.sia.es/AC_SIA_PC_SELLO_v1.9.pdf

DPC relacionada	Declaración de Prácticas de Certificación de la PKI de SIA OID 1.3.6.1.4.1.39131.10.1.1.1.0 Disponible en https://psc.sia.es/

Tabla 1 – Datos identificación DPC

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

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

1.3.1 Autoridad de Certificación / Prestador cualificado de Servicios de Confianza

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

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

- **"AC raíz"** (SIA ROOT y SIA ROOT 2025) - 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"** (SIA SUB01 y SIA SUB01 2025) - Autoridad de Certificación subordinada de "AC raíz". Su función es la emisión de certificados para terceros, en este caso, la emisión de Sellos Electrónicos detallados en esta PC.

En este ámbito, SIA actúa como prestador de servicios de confianza, emitiendo los certificados electrónicos cualificados de sello en software, HSM o QSCD y proveyendo servicios de sello electrónico basada en un certificado cualificado de sello de nivel medio para la creación de firmas electrónicas automatizadas, conforme a lo establecido en eIDAS y en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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:

- Los criterios que deben cumplirse para solicitar un certificado, sin contradecir lo estipulado en la DPC y en la presente PC.
- Los mecanismos y procedimientos necesarios para llevar a cabo la identificación y autenticación del firmante, de acuerdo con lo establecido en los apartados 1.3.2 y 9.6.2 de la DPC.
- Los dispositivos de creación de firma que se utilizarán, previamente homologados por SIA.

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, la entidad —ya sea una corporación u otra entidad privada o pública, incluida la de derecho público— es la titular, y está representada por una persona física. Los datos de la entidad que representa serán incluidos en el certificado. Opcionalmente, podrán incluirse también los datos de la persona física, quien será responsable de la custodia de las claves privadas asociadas a dicho certificado.

El suscriptor también recibe el nombre de firmante, según se define en el artículo 3 del reglamento eIDAS.

El suscriptor del certificado de sello electrónico PSD2 será el Proveedor del Servicio de Pago (PSP) debidamente autorizado e inscrito en el registro público de la Autoridad Nacional Competente. El suscriptor será siempre una persona jurídica comprendida, al menos, en una de las categorías siguientes:

- Gestor de cuenta (PSP_AS)
- Proveedor de servicios de iniciación de pagos (PSP_PI)
- Proveedor de información sobre cuentas (PSP_AI)
- Emisor de instrumentos de pago basados en tarjetas (PSP_IC)

1.3.5 Solicitante

Los solicitantes de certificados cualificados de Sello Electrónico, de nivel medio o alto, son los usuarios con poderes de representación de la entidad (ya sean corporaciones, empresas o entidades privadas o públicas).

Los solicitantes de certificados cualificados de Sello Electrónico PSD2 de nivel medio y alto, son los propios usuarios con poderes de representación de la propia entidad (bien sean corporaciones, empresas o entidades privadas).

1.3.6 Terceras Partes Aceptantes

Las terceras partes aceptantes son las personas físicas o entidades distintas del titular y de la entidad a la que este representa, que deciden aceptar y confiar en un certificado emitido por SIA. Como tales, les resulta aplicable lo establecido en la presente Política de Certificación (PC) cuando hacen uso de dichos 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 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.

El reglamento eIDAS establece que los Certificados Cualificados de Sello Electrónico 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 la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, 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** - Elcertificado cualificado de sello electrónico, emitido en un dispositivo cualificado de creación de sello, en HSM o, opcionalmente, en software, permite verificar que un documento no ha sido modificado por terceros. Para garantizar su integridad, se emplean funciones criptográficas de resumen, que generan una huella digital única del contenido. Esta se firma con la clave privada, de modo que cualquier alteración del documento implica una modificación detectable del resumen, asegurando así la autenticidad del mensaje desde su emisión hasta su recepción.

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.

Contacto	SIA
Entidad	SISTEMAS INFORMATICOS ABIERTOS, S.A.U.
C.I.F.	A82733262
Dirección postal	Avenida de Bruselas, 35 28108 Alcobendas - Madrid (España)
Dirección de correo electrónico	psc@sia.es
Dirección web	https://psc.sia.es
Teléfono	+34 91 307 79 97

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 y alto y Certificados cualificados de Sello Electrónico PSD2 – Nivel medio y alto, se generan a petición del 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) QSCD.

La posesión de la clave privada se probará mediante CSR (PKCS#10) que se proveerá en el momento de le emisión con el fin de generar el correspondiente certificado de clave pública, una vez validada la firma del CSR.

La generación del certificado deberá hacerse acorde con los requisitos que la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza 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 autentificación 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.

2.2.5 Autenticación de la identidad de un Prestador de Servicios de Pago

Para validar la identidad de un Prestador de Servicios de Pago, la AR comprobará:

- El número de autorización u otro identificador reconocido expedido por una Autoridad Nacional Competente que acredite que el Prestador de Servicios de Pago puede ejercer su función.
- El Rol o roles que desempeña el Prestador de Servicios de Pago relacionado con el número de autorización.
- El nombre de la Autoridad Nacional Competente.

Para la validación de los mismos se utilizará de la información publicada por las Autoridades Nacionales Competentes, ya sea a través de los registros nacionales públicos y/o de los registros e instituciones de la Autoridad Bancaria Europea (EBA) o en los registros públicos de la Autoridad Nacional del país en el que está registrado el Prestador de Servicios de Pago.

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.

Adicionalmente, para la solicitud de certificados de sello electrónico PSD2, se aportará la documentación que acredite al Proveedor de Servicios de Pago y que incluya número de autorización, el rol o roles del proveedor del servicio de pago y el nombre de la Autoridad Nacional Competente.

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.

En caso de los certificados cualificados de Sello Electrónico para PSD2, además de lo anterior, se validarán los atributos específicos de este tipo de organizaciones (Número de autorización, rol, nombre de la Autoridad Nacional Competente, etc.) mediante consulta a la información puesta a disposición por las Autoridades Nacionales Competentes. Si la Autoridad Nacional Competente proporciona normas para la validación de esta información, SIA AC aplicará esas normas.

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

Antes de generar claves y certificados, es necesaria la validación, revisión y aprobación de la solicitud de certificado por parte de la Autoridad de Registro (AR). Además, los datos deben darse de alta en el sistema del Proveedor de Servicios de Confianza (TSP).

Las claves para los certificados de Sello Electrónico - Nivel medio y certificados de Sello Electrónico PSD2- Nivel medio se generan en soporte software o en Módulos de Seguridad Hardware (HSM). Los certificados cualificados de sello electrónico y PSD2 nivel alto, se generan en el dispositivo cualificado de creación de firma (QSCD)

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 enviará por correo un CSR, que previamente habrá generado en su sistema. Opcionalmente, el TSP puede obtener el CSR del par de claves generadas en un módulo criptográfico seguro (HSM) o QSCD, previa petición y consentimiento del solicitante. Los certificados cualificados de nivel alto se generan en el dispositivo cualificado de creación de firma (QSCD).
3. Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registrada, incluyendo la clave pública certificada;
4. Se incluirán en el certificado las informaciones establecidas en el artículo 6 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
5. 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.

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

En el ámbito de los dispositivos cualificados de creación de firma o sello, una vez que se han registrado los datos en el sistema con nivel avanzado de garantía de registro y se ha solicitado expresamente la emisión de los certificados, el sistema generará la clave privada, la cual permanecerá almacenada en el dispositivo de forma protegida, de modo que se garantice su uso bajo el control exclusivo del titular.

Adicionalmente, para el nivel medio, la generación y almacenamiento podrá realizarse en software.

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.

La Autoridad Nacional Competente puede solicitar información sobre certificados que incluyan un número de autorización asignado por dicha institución a un Proveedor de Servicios de Pago (PSP). SIA AC proporcionará esta información sobre los certificados emitidos, conforme a lo establecido en cada repositorio correspondiente.

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

Únicamente en el caso de certificados PSD2, si la CA de SIA ha recibido notificación sobre la dirección de correo electrónico de la Autoridad Nacional Competente identificada en el certificado de nueva emisión, SIA remitirá a dicha dirección la información relativa al certificado emitido, conforme a lo establecido en la normativa aplicable. También enviará la información de contacto y las instrucciones para realizar solicitudes de revocación.

3.5 Par de claves y uso del certificado

3.5.1 Uso de la clave privada del certificado 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 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 a documentos electrónicos.

Los certificados cualificados de Sello Electrónico PSD2, de nivel medio y alto regulados en esta Política de Certificación, se emiten a Proveedores de Servicios de Pago debidamente acreditados ante la Autoridad Nacional Competente. Estos certificados cumplen los requisitos establecidos en el Reglamento Delegado (UE) 2018/389 de la Comisión, que complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y los estándares de comunicación abiertos, comunes y seguros. Asimismo, respetan lo dispuesto en el Real Decreto-ley 19/2018 de España y las directrices emitidas por la Autoridad Nacional Competente en materia de servicios de pago.

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 debe ser solicitada por el firmante.

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.

Antes de la renovación de los certificados cualificados de Sello Electrónico PSD2, SIA AC repetirá la verificación de los atributos específicos de PSD2 incluidos en el certificado tal y como se hizo en la

emisión inicial. Si la Autoridad Nacional Competente proporciona normas para la validación de estos atributos, SIA AC aplicará esas normas.

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 mismo proceso que en la emisión inicial, una vez generado satisfactoriamente el nuevo certificado, se notificará al firmante que se ha realizado la renovación telemática de su certificado. También se le informará del nuevo periodo de validez, así como de que el certificado anterior ha sido revocado y ha dejado de tener validez.

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.

Solo en el caso de emisión de certificados PSD2, si SIA ha sido notificada de la dirección de correo electrónico de la Autoridad Nacional Competente (ANC) identificada en el certificado de nueva emisión, remitirá a dicha dirección la información relativa al certificado emitido, conforme a la normativa de referencia. Además, enviará la información de contacto, las instrucciones para las solicitudes de revocación y una copia del archivo del certificado.

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.

Adicionalmente, se considerará causa de compromiso de las claves privadas la pérdida, robo, hurto, modificación, divulgación o revelación de la clave personal de acceso que permite su activación, así como la revelación de las claves de acceso asociadas a un dispositivo de firma centralizada. También se incluirá cualquier otra circunstancia, incluso fortuita, que indique un posible uso de las claves privadas por parte de una entidad distinta de su titular.

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.
- En el caso de los Certificados cualificados de Sello Electrónico para PSD2, la solicitud de revocación puede ser realizada por el Banco de España o la Autoridad Nacional Competente (ANC).

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 proporciona de forma gratuita un servicio de publicación de Listas de Certificados Revocados (CRL) a través de su sitio web, sin restricciones de acceso para los usuarios. Asimismo, ofrece un servicio de verificación del estado de los certificados mediante el protocolo OCSP (Online Certificate Status Protocol), conforme a lo establecido en las correspondientes Políticas de Certificación.

3.10.2 Disponibilidad del servicio

Los servicios de descarga de Listas de Certificados Revocados (CRL) ofrecidos por SIA estarán disponibles 24 horas al día, 7 días a la semana, los 365 días del año. Para garantizar la continuidad del servicio, SIA dispone de un Centro de Proceso de Datos (CPD) replicado, de modo que, en caso de caída o indisponibilidad del nodo principal, el nodo secundario asumirá automáticamente la prestación del servicio, asegurando así su alta disponibilidad.

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

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

En el caso de dispositivos criptográficos de seguridad (HSM) y QSCD, las claves que se generen en dicho dispositivo podrán quedar custodiadas por el TSP, el cual hará copia de los datos de creación de firma manteniendo el mismo nivel de seguridad que los datos originales, teniendo en cuenta que el acceso a esta clave será realizado por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del firmante. En ningún caso se harán duplicados más allá del mínimo necesario para garantizar la continuidad del servicio.

En línea con la mención anterior, en el artículo 29 bis.1.b) del reglamento eIDAS se establece que, sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante, podrán duplicar los datos de creación de firmas electrónicas exclusivamente con fines de copia de seguridad, siempre y cuando se cumplan los requisitos de que la seguridad de los conjuntos de datos duplicados debe ser del mismo nivel que el previsto para los conjuntos de datos originales, y el número de conjuntos de datos duplicados no debe superar el mínimo necesario para garantizar la continuidad del servicio.

En este sentido, el acceso a dicha clave sólo puede ser efectuado por el titular de la misma mediante una aplicación al efecto donde el titular deberá estar debidamente autenticado. Posteriormente, para el sellado se recabará un segundo factor de autenticación que en el caso de operaciones automatizadas podrá estar basado en un OTP o en geolocalización.

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) QSCD.

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.

Cuando la clave privada se genera en un dispositivo cualificado de creación de firma bajo el control exclusivo del firmante, no existe ninguna entrega de la clave privada al titular.

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

Adicionalmente, para el nivel medio, cuya generación y almacenamiento de la clave se ha realizado en software, la clave privada finalmente se encuentra en posesión del titular y con la recomendación de protegerla adecuadamente para evitar usos no deseados de la misma.

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

Los certificados cualificados de sello electrónico utilizan claves de 2048, 3072 o 4096 bits, en función del nivel de seguridad requerido y de acuerdo con los estándares criptográficos vigentes.

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

Los requisitos técnicos relativos a los módulos criptográficos (incluidos los dispositivos de creación de firma) se describen en el apartado 6.2.1 de la DPC (Declaración de Prácticas de Certificación).

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 identifican tres escenarios posibles para la gestión de la custodia de claves:

- En el software: las claves son almacenadas por el aplicativo que hace uso del sello electrónico.

- En un HSM (Hardware Security Module): las claves se almacenan en un módulo criptográfico que cumple con la certificación requerida. Para más detalles sobre los estándares aplicables a los módulos criptográficos, véase el punto 6.2.1 del documento DPC (Declaración de Prácticas de Certificación).
- En un QSCD (Qualified Seal Creation Device): las claves se gestionan conforme a lo establecido en el Reglamento europeo eIDAS, y el dispositivo está incluido en la lista de dispositivos cualificados mantenida por la Comisión Europea: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd

4.2.4 Copia de seguridad de la clave privada

Toda copia de seguridad de claves privadas, independientemente de si estas se custodian en software o HSM, debe mantener al menos el mismo nivel de seguridad que el entorno principal.

4.2.5 Archivo de la clave privada

La Autoridad de Certificación (AC) no almacenará en ningún caso las claves privadas asociadas a los certificados cualificados de Sello Electrónico; la responsabilidad de su custodia y control exclusivo recae en el usuario final.

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) QSCD, 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) y QSCD, 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 o hardware, según sea el caso.

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 inferior a 5 años. El par de claves utilizado para la emisión de los certificados se crea para cada emisión y por tanto también tiene una validez inferior a 5 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 y un segundo factor cuando se emplea un QSCD.

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 y un segundo factor cuando se emplea un QSCD.

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: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- 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 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, 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.
- ETSI TS 119 495: Electronic Signatures and Trust Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.

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 Sello Electrónico 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 ingles del servicio prestado.
- **PSD2QcType**, adicionalmente y sólo para certificados del tipo PSD2, con la información de los roles del proveedor de servicios de pago, el nombre de la autoridad nacional competente y su identificador único, conforme a lo establecido en la ETSI TS 119 495 clausula 5.1: La función del Prestador de Servicios de Pago (PSP), que puede ser una o más de las siguientes:
    - servicio de cuentas (PSP_AS);
    - iniciación de pago (PSP_PI);
    - información de la cuenta (PSP_AI);
    - emisión de instrumentos de pago basados en tarjeta (PSP_IC).
- **Nombre de la Autoridad Nacional Competente** donde el PSP está registrado. Esta información se proporciona en dos formas: la cadena de nombre completo (NCAName) en inglés y un identificador único abreviado (NCAId).

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 proporciona 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. Su uso es opcional y sólo para entidades de carácter no público.

OID	Concepto	Descripción
1.3.6.1.4.1.39131.10.2.1	Tipo de certificado	Tipo de certificado.
1.3.6.1.4.1.39131.10.2.2	Nombre	Nombre del usuario.
1.3.6.1.4.1.39131.10.2.3	Apellido1	Primer apellido del usuario.
1.3.6.1.4.1.39131.10.2.4	Apellido2	Segundo apellido del usuario.
1.3.6.1.4.1.39131.10.2.5	DNI/NIE/Pasaporte/ID	DNI/NIE/Pasaporte/Documento de identificación del usuario.

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. Sólo para AAPP. Su uso es opcional a excepción del tipo de certificado, entidad suscriptora y NIF de la entidad suscriptora.

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 nivel medio

OID	Concepto	Descripción
2.16.724.1.3.5.6.1.1	Tipo de certificado	Tipo de certificado.
2.16.724.1.3.5.6.1.2	Entidad Suscriptora	Nombre de la Entidad suscriptora
2.16.724.1.3.5.6.1.3	NIF Entidad Suscriptora	Número de identificación de la Entidad suscriptora
2.16.724.1.3.5.6.1.4	DNI/NIE	DNI/NIE del responsable del sello
2.16.724.1.3.5.6.1.5	Descripción del componente	Descripción del componente que posee el sello
2.16.724.1.3.5.6.1.6	Nombre	Nombre de pila del responsable del sello
2.16.724.1.3.5.6.1.7	Apellido 1	Primer apellido del responsable del sello
2.16.724.1.3.5.6.1.8	Apellido 2	Segundo apellido del responsable del sello
2.16.724.1.3.5.6.1.9	Email	Correo electrónico del responsable del sello

Tabla 5 – Definición extensión SubjectAltName AAPP nivel alto

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 cualificados de Sello Electrónico, 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 distingan 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.

En el caso de certificados con atributo de PSD2, el número de autorización está incluido en el atributo "organizationIdentifier", tal y como indica la ETSI TS 119 495:

- OI = Número de autorización en la ANC en formato "PSD", según norma ETSI EN 319 412-1 (5.1.4.3) y ETSI TS 119 495. Identificación basada en el número de autorización nacional de un PSP bajo la directiva de Proveedores de Servicios de pago (EU) 2015/2366.

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

Los OID de la presente PC son 1.3.6.1.4.1.39131.10.1.12, 1.3.6.1.4.1.39131.10.1.12.1 y 1.3.6.1.4.1.39131.10.1.12.2 para el nivel medio y 1.3.6.1.4.1.39131.10.1.13, 1.3.6.1.4.1.39131.10.1.13.1 y 1.3.6.1.4.1.39131.10.1.13.2 para el nivel alto. Los identificadores de los certificados expedidos bajo la presenta Política de Certificación son los siguientes:

OID	Descripción
1.3.6.1.4.1.39131.10.1.12	Nivel medio.
1.3.6.1.4.1.39131.10.1.12.1	Nivel medio para AAPP.
1.3.6.1.4.1.39131.10.1.12.2	Nivel medio PSD2.
1.3.6.1.4.1.39131.10.1.13	Nivel alto.
1.3.6.1.4.1.39131.10.1.13.1	Nivel alto para AAPP.
1.3.6.1.4.1.39131.10.1.13.2	Nivel alto PSD2.

Tabla 6 – OID presentes en esta PC

Política de Certificados	OID
Cualificado de Sello Electrónico	1.3.6.1.4.1.39131.10.1.12 (Nivel medio)
	1.3.6.1.4.1.39131.10.1.12.1 (Nivel medio para AAPP)
	1.3.6.1.4.1.39131.10.1.13 (Nivel alto)
	1.3.6.1.4.1.39131.10.1.13.1 (Nivel alto para AAPP)
Certificado de Sello Electrónico PSD2	1.3.6.1.4.1.39131.10.1.12.2 (Nivel medio PSD2)
	1.3.6.1.4.1.39131.10.1.13.2 (Nivel alto para PSD2)
QCP-l	0.4.0.194112.1.1
QCP-l-qscd	0.4.0.194112.1.3 (para el nivel alto)

Tabla 7 – 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-l**: indicación de certificado cualificado de sello, acorde a eIDAS.
- **QCP-l-qscd**: indicación de certificado cualificado de sello electrónico en qscd, acorde a eIDAS
- **OID del tipo de certificado**: Sólo para certificados cualificados de Sello Electrónico para AAPP.
    - OID: 2.16.724.1.3.5.6.2 (nivel medio)
    - OID: 2.16.724.1.3.5.6.1 (nivel alto).

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 Perfiles de Certificado de Sello

5.2.1 Certificado de Sello Electrónico o Sello Electrónico AAPP – 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, RSA-3072 o RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	ES
Organización (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	SISTEMAS INFORMATICOS ABIERTOS SAU
Organización Unit (OU)	QUALIFIED CA	QUALIFIED
serialNumber	A82733262	
organizationIdentifier		VATES-A82733262
Common Name (CN)	SIA SUB01	SIA SUB01 2025
Validity		
No Before	Fecha de emisión del certificado	
No After	Fecha de emisión + <=5 años	
Subject (Asunto)		
Country (C)	ES	España
Organización (O)	<NOMBRE DE LA ENTIDAD>	Nombre de la Organización
Organization Identifier (OI)	VATES-<NIF de la ENTIDAD>	

Organizatión Unit (OU)	SELLO ELECTRONICO	Naturaleza del certificado
Common Name (CN)	<Denominación del Sistema>	
Subject Public Key Info	Clave pública (RSA de 2048, 3072 o 4096 bits), codificada conforme al algoritmo criptográfico correspondiente.	
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	1 (seleccionado)	
Key Encipherment	1 (seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	1 (seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
ExtendedKeyUsage		
Email Protection	1 (seleccionado)	
Client Authentication	1 (seleccionado)	
CRL Distribution Point		
Distribution Point 1	http://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada
Distribution Point 2	https://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada

Authority Info Access		
Access Method	Id-ad-ocsp	
Access Method	https://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Location	https://psc.sia.es/ac_sub01.crt	https://psc.sia.es/ac_sub_2025.crt
Qualified Certificate Statements (Codificado en formato ASN.1)		
QcCompliance	OID 0.4.0.1862.1.1	Certificado cualificado
QcEuRetentionPeriod	OID 0.4.0.1862.1.3	Duración custodia (15 años)
QcType	OID 0.4.0.1862.1.6	
id-etsi-qct-eseal	OID 0.4.0.1862.1.6.2	Certificado de sello
QCSyntax-v2	OID 1.3.6.1.5.5.7.11.2	
id-etsi-qcs-SemanticsId-Legal	OID 0.4.0.194121.1.2	
QcPDS	OID 0.4.0.1862.1.5	
PdsLocation	https://psc.sia.es/en (en)	
Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.12	Sólo para entidades no públicas.
	1.3.6.1.4.1.39131.10.1.12.1	Sólo para AAPP.
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	"Certificado cualificado de sello electrónico de nivel medio. Condiciones de uso y vías de contacto en: https://psc.sia.es"	
Policy Identifier	QCP-l	
Policy Identifier	2.16.724.1.3.5.6.2	Sólo para AAPP.
Subject Alternative Name		

Tipo del certificado	OID: 2.16.724.1.3.5.6.2.1: SELLO ELECTRONICO DE NIVEL MEDIO	Sólo para AAPP.
Nombre entidad suscriptora	OID: 2.16.724.1.3.5.6.2.2:: <Entidad Suscriptora>	Entidad suscriptora, Sólo para AAPP.
NIF entidad suscriptora	OID: 2.16.724.1.3.5.6.2.3: <NIF entidad suscriptora>	NIF Entidad suscriptora, Sólo para AAPP.
DNI/NIE del responsable	OID: 2.16.724.1.3.5.6.2.4: <DNI / NIE>	DNI / NIE del responsable del sello, Sólo para AAPP.
Descripción del componente	OID: 2.16.724.1.3.5.6.2.5: <Descripción Componente>	Descripción del componente, Sólo para AAPP.
Nombre del responsable	OID: 2.16.724.1.3.5.6.2.6: <Nombre>	Nombre del responsable del sello, Sólo para AAPP.
Apellido 1 del responsable	OID: 2.16.724.1.3.5.6.2.7: <Apellido 1>	Apellido 1 del responsable del sello, Sólo para AAPP.
Apellido 2 del responsable	OID: 2.16.724.1.3.5.6.2.8: <Apellido 2>	Apellido 2 del responsable del sello, Sólo para AAPP.
Email del responsable	OID: 2.16.724.1.3.5.6.2.9: <Email>	Correo electrónico del responsable del sello, Sólo para AAPP.
Tipo de certificado	OID: 1.3.6.1.4.1.39131.10.2.1: SELLO ELECTRONICO DE NIVEL MEDIO	Tipo de certificado, Sólo para entidades no públicas.
Nombre del responsable	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del responsable del sello, Sólo para entidades no públicas.
Apellido 1 del responsable	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido 1>	Apellido 1 del responsable del sello, Sólo para entidades no públicas.
Apellido 2 del responsable	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido 2>	Apellido 2 del responsable del sello, Sólo para entidades no públicas.
DNI/NIE del responsable	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI/NIE>	DNI / NIE/documento de identificacion del responsable del sello, Sólo para entidades no públicas.

Tabla 8 – Perfil certificado nivel medio

5.2.2 Certificado de Sello Electrónico PSD2 – 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, RSA-3072 o RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	ES
Organización (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	SISTEMAS INFORMATICOS ABIERTOS SAU
Organización Unit (OU)	QUALIFIED CA	QUALIFIED
serialNumber	A82733262	
organizationIdentifier		VATES-A82733262
Common Name (CN)	SIA SUB01	SIA SUB01 2025
Validity		
No Before	Fecha de emisión del certificado	
No After	Fecha de emisión + <=5 años	
Subject (Asunto)		
Country (C)	ES	España
Organización (O)	<NOMBRE DE LA ENTIDAD>	Contendrá la denominación exacta de la persona jurídica según aparezca en el Registro público de la Autoridad Nacional Competente del Estado Miembro de origen o que resulte de las notificaciones a la EBA (Autoridad Bancaria Europea), o en la ANC del país de autorización/registro del PSP.

Organization Identifier (OI)	Incluirá el número de autorización. P. Ej. PSDES-BE-<authorization number by NCA> (PSDES-BE-0240)	El número de autorización está incluido en el atributo "organizationIdentifier", tal y como indica la ETSI TS 119 495
Organizatión Unit (OU)	SELLO ELECTRONICO	Naturaleza del certificado
Common Name (CN)	<Denominación del Sistema>	
Subject Public Key Info	Clave pública (RSA de 2048, 3072 o 4096 bits), codificada conforme al algoritmo criptográfico correspondiente.	
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	1 (seleccionado)	
Key Encipherment	1 (seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	1 (seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
ExtendedKeyUsage		
Email Protection	1 (seleccionado)	
Client Authentication	1 (seleccionado)	
CRL Distribution Point		

Distribution Point 1	http://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada
Distribution Point 2	https://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada
Authority Info Access		
Access Method	Id-ad-ocsp	
Access Method	https://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Location	https://psc.sia.es/ac_sub01.crt	https://psc.sia.es/ac_sub_2025.crt
Qualified Certificate Statements (Codificado en formato ASN.1)		
QcCompliance	OID 0.4.0.1862.1.1	Certificado cualificado
QcEuRetentionPeriod	OID 0.4.0.1862.1.3	Duración custodia (15 años)
QcType	OID 0.4.0.1862.1.6	
id-etsi-qct-eseal	OID 0.4.0.1862.1.6.2	Certificado de sello
QCSyntax-v2	OID 1.3.6.1.5.5.7.11.2	
id-etsi-qcs-SemanticsId-Legal	OID 0.4.0.194121.1.2	
QcPDS	OID 0.4.0.1862.1.5	
PdsLocation	https://psc.sia.es/en (en)	
PSD2QcType	OID 0.4.0.19495.2	De acuerdo con la ETSI TS 119 495
rolesOf PSP	OID 0.4.19495.1.1: PSP_AS OID 0.4.19495.1.2: PSP_PI OID 0.4.19495.1.3: PSP_AI OID 0.4.19495.1.4: PSP_IC	Roles de PSP. Podrá disponer de uno o varios. OID del rol Nombre del rol
NCAName	<Nombre de la ANC>	Nombre
nCAId	<identificador de la ANC	Idenficador
Certificate Policies		

Policy Identifier	1.3.6.1.4.1.39131.10.1.12.2	
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	"Certificado cualificado de sello electrónico PSD2 de nivel medio. Condiciones de uso y vías de contacto en: https://psc.sia.es"	
Policy Identifier	QCP-l	
Subject Alternative Name		
Tipo de certificado	OID: 1.3.6.1.4.1.39131.10.2.1: SELLO ELECTRONICO PSD2 DE NIVEL MEDIO	Tipo de certificado
Nombre del responsable	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del responsable del sello
Apellido 1 del responsable	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido 1>	Apellido 1 del responsable del sello
Apellido 2 del responsable	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido 2>	Apellido 2 del responsable del sello
DNI/NIE del responsable	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI/NIE>	DNI / NIE/documento de identificacion del responsable del sello

Tabla 9 – Perfil certificado PSD2 nivel medio

5.2.3 Certificado de Sello Electrónico o Sello Electrónico AAPP – Nivel alto

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, RSA-3072 o RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	ES

Organización (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	SISTEMAS INFORMATICOS ABIERTOS SAU
Organización Unit (OU)	QUALIFIED CA	QUALIFIED
serialNumber	A82733262	
organizationIdentifier		VATES-A82733262
Common Name (CN)	SIA SUB01	SIA SUB01 2025
Validity		
No Before	Fecha de emisión del certificado	
No After	Fecha de emisión + <=5 años	
Subject (Asunto)		
Country (C)	ES	España
Organización (O)	<NOMBRE DE LA ENTIDAD>	Nombre de la Organización
Organization Identifier (OI)	VATES-<NIF de la ENTIDAD>	
Organización Unit (OU)	SELLO ELECTRONICO	Naturaleza del certificado
Common Name (CN)	<Denominación del Sistema>	
Subject Public Key Info	Clave pública (RSA de 2048, 3072 o 4096 bits), codificada conforme al algoritmo criptográfico correspondiente.	
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	1 (seleccionado)	
Key Encipherment	1 (seleccionado)	
Data Encipherment	0 (no seleccionado)	

Key Agreement	1 (seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
ExtendedKeyUsage		
Email Protection	1 (seleccionado)	
Client Authentication	1 (seleccionado)	
CRL Distribution Point		
Distribution Point 1	http://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada
Distribution Point 2	https://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada
Authority Info Access		
Access Method	Id-ad-ocsp	
Access Method	https://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Location	https://psc.sia.es/ac_sub01.crt	https://psc.sia.es/ac_sub_2025.crt
Qualified Certificate Statements (Codificado en formato ASN.1)		
QcCompliance	OID 0.4.0.1862.1.1	Certificado cualificado
QcEuRetentionPeriod	OID 0.4.0.1862.1.3	Duración custodia (15 años)
QcType	OID 0.4.0.1862.1.6	
id-etsi-qct-eseal	OID 0.4.0.1862.1.6.2	Certificado de sello
QCSyntax-v2	OID 1.3.6.1.5.5.7.11.2	
id-etsi-qcs-SemanticsId-Legal	OID 0.4.0.194121.1.2	

QcPDS	OID 0.4.0.1862.1.5	
PdsLocation	https://psc.sia.es/en (en)	
QcSSCD	OID 0.4.0.1862.1.4	Uso de dispositivo cualificado de creación de firma electrónica
Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.13	Sólo para entidades no públicas.
	1.3.6.1.4.1.39131.10.1.13.1	Sólo para AAPP.
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	"Certificado cualificado de sello electrónico de nivel alto. Condiciones de uso y vías de contacto en: https://psc.sia.es"	
Policy Identifier	QCP-l-qscd : 0.4.0.194112.1.3	
Policy Identifier	2.16.724.1.3.5.6.1	Sólo para AAPP.
Subject Alternative Name		
Tipo del certificado	OID: 2.16.724.1.3.5.6.1.1: SELLO ELECTRONICO DE NIVEL ALTO	Sólo para AAPP.
Nombre entidad suscriptora	OID: 2.16.724.1.3.5.6.1.2:: <Entidad Suscriptora>	Entidad suscriptora, Sólo para AAPP.
NIF entidad suscriptora	OID: 2.16.724.1.3.5.6.1.3: <NIF entidad suscriptora>	NIF Entidad suscriptora, Sólo para AAPP.
DNI/NIE del responsable	OID: 2.16.724.1.3.5.6.1.4: <DNI / NIE>	DNI / NIE del responsable del sello, Sólo para AAPP.
Descripción del componente	OID: 2.16.724.1.3.5.6.1.5: <Descripción Componente>	Descripción del componente, Sólo para AAPP.
Nombre del responsable	OID: 2.16.724.1.3.5.6.1.6: <Nombre>	Nombre del responsable del sello, Sólo para AAPP.
Apellido 1 del responsable	OID: 2.16.724.1.3.5.6.1.7: <Apellido 1>	Apellido 1 del responsable del sello, Sólo para AAPP.

Apellido 2 del responsable	OID: 2.16.724.1.3.5.6.1.8: <Apellido 2>	Apellido 2 del responsable del sello, Sólo para AAPP.
Email del responsable	OID: 2.16.724.1.3.5.6.1.9: <Email>	Correo electrónico del responsable del sello, Sólo para AAPP.
Tipo de certificado	OID: 1.3.6.1.4.1.39131.10.2.1: SELLO ELECTRONICO DE NIVEL ALTO	Tipo de certificado, Sólo para entidades no públicas.
Nombre del responsable	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del responsable del sello, Sólo para entidades no públicas.
Apellido 1 del responsable	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido 1>	Apellido 1 del responsable del sello, Sólo para entidades no públicas.
Apellido 2 del responsable	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido 2>	Apellido 2 del responsable del sello, Sólo para entidades no públicas.
DNI/NIE del responsable	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI/NIE>	DNI / NIE/documento de identificacion del responsable del sello, Sólo para entidades no públicas.

Tabla 10 – Perfil certificado nivel alto

5.2.4 Certificado de Sello Electrónico PSD2 – Nivel Alto

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, RSA-3072 o RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	ES
Organización (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	SISTEMAS INFORMATICOS ABIERTOS SAU

Organizatión Unit (OU)	QUALIFIED CA	QUALIFIED
serialNumber	A82733262	
organizationIdentifier		VATES-A82733262
Common Name (CN)	SIA SUB01	SIA SUB01 2025
Validity		
No Before	Fecha de emisión del certificado	
No After	Fecha de emisión + <=5 años	
Subject (Asunto)		
Country (C)	ES	España
Organizatión (O)	<NOMBRE DE LA ENTIDAD>	Contendrá la denominación exacta de la persona jurídica según aparezca en el Registro público de la Autoridad Nacional Competente del Estado Miembro de origen o que resulte de las notificaciones a la EBA (Autoridad Bancaria Europea), o en la ANC del país de autorización/registro del PSP.
Organization Identifier (OI)	Incluirá el número de autorización. P. Ej. PSDES-BE-<authorization number by NCA> (PSDES-BE-0240)	El número de autorización está incluido en el atributo "organizationIdentifier", tal y como indica la ETSI TS 119 495
Organizatión Unit (OU)	SELLO ELECTRONICO	Naturaleza del certificado
Common Name (CN)	<Denominación del Sistema>	
Subject Public Key Info	Clave pública (RSA de 2048, 3072 o 4096 bits), codificada conforme al algoritmo criptográfico correspondiente.	
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	1 (seleccionado)	
Key Encipherment	1 (seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	1 (seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
ExtendedKeyUsage		
Email Protection	1 (seleccionado)	
Client Authentication	1 (seleccionado)	
CRL Distribution Point		
Distribution Point 1	http://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada
Distribution Point 2	https://psc.sia.es/crlc[N].crl	N es el número correspondiente a la CRL particionada
Authority Info Access		
Access Method	Id-ad-ocsp	
Access Method	https://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Location	https://psc.sia.es/ac_sub01.crt	https://psc.sia.es/ac_sub_2025.crt
Qualified Certificate Statements (Codificado en formato ASN.1)		
QcCompliance	OID 0.4.0.1862.1.1	Certificado cualificado
QcEuRetentionPeriod	OID 0.4.0.1862.1.3	Duración custodia (15 años)

QcType	OID 0.4.0.1862.1.6	
id-etsi-qct-eseal	OID 0.4.0.1862.1.6.2	Certificado de sello
QCSyntax-v2	OID 1.3.6.1.5.5.7.11.2	
id-etsi-qcs-SemanticsId-Legal	OID 0.4.0.194121.1.2	
QcPDS	OID 0.4.0.1862.1.5	
PdsLocation	https://psc.sia.es/en (en)	
QcSSCD	OID 0.4.0.1862.1.4	Uso de dispositivo cualificado de creación de firma electrónica
PSD2QcType	OID 0.4.0.19495.2	De acuerdo con la ETSI TS 119 495
rolesOf PSP	OID 0.4.19495.1.1: PSP_AS OID 0.4.19495.1.2: PSP_PI OID 0.4.19495.1.3: PSP_AI OID 0.4.19495.1.4: PSP_IC	Roles de PSP. Podrá disponer de uno o varios. OID del rol Nombre del rol
NCAName	<Nombre de la ANC>	Nombre
nCAId	<identificador de la ANC	Indenficador
Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.13.2	
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	"Certificado cualificado de sello electrónico PSD2 de nivel alto. Condiciones de uso y vías de contacto en: https://psc.sia.es"	
Policy Identifier	QCP-l-qscd : 0.4.0.194112.1.3	
Subject Alternative Name		
Tipo de certificado	OID: 1.3.6.1.4.1.39131.10.2.1: SELLO ELECTRONICO PSD2 DE NIVEL ALTO	Tipo de certificado,

Nombre del responsable	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del responsable del sello,
Apellido 1 del responsable	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido 1>	Apellido 1 del responsable del sello,
Apellido 2 del responsable	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido 2>	Apellido 2 del responsable del sello,.
DNI/NIE del responsable	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI/NIE>	DNI / NIE/documento de identificacion del responsable del sello,

Tabla 11 – Perfil certificado PSD2 nivel alto

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 aplicará ninguna tarifa.

6.1.4 Tarifas de otros servicios tales como información de políticas

No se aplicará 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.

An Indra company

Persona de contacto
psc@sia.es

Av. de Bruselas, 35

28108 Alcobendas, Madrid
T +34 91 307 79 97

sia.es