



PC - SIA

Política de Certificación Certificados cualificados de Ciudadano

OID: 1.3.6.1.4.1.39131.10.1.3 (Nivel medio)

OID: 1.3.6.1.4.1.39131.10.1.17 (QSCD centralizado o nivel alto)

Versión: 1.8



SIA | PC

Certificado cualificado de ciudadano

Fecha: 14 de julio de 2025

AVISO LEGAL

Toda la información contenida en el presente documento y sus anexos, tiene carácter confidencial, y sólo puede ser utilizada con el fin de ser evaluada por el destinatario (sea cliente, proveedor, colaborador, partner, etc.) de la misma y a los solos efectos de conducir los tratos comerciales, o de otra naturaleza, que motivan el envío del documento (en lo sucesivo, el “Propósito”).

La información aquí presentada es elaborada por SISTEMAS INFORMATICOS ABIERTOS, S.A.U., (en adelante SIA) sociedad perteneciente al Grupo Indra, con C.I.F. A82733262 y domicilio en Av. de Bruselas, 35, 28108 Alcobendas (Madrid), España y anula y sustituye a las anteriores, y es constitutiva de secreto empresarial (también denominado en determinadas jurisdicciones, secreto comercial), y además, puede estar protegida por derechos de autor, derechos afines, patente, modelo de utilidad y/o diseño industrial por lo que queda terminantemente prohibida su divulgación y/o transmisión a terceros sin el permiso previo, expreso y por escrito de SIA.

Se limitará al máximo el acceso a la información confidencial por parte del personal del destinatario de la misma, o del personal de aquellos terceros a los que SIA haya autorizado a acceder a la información confidencial, limitándose únicamente a aquellas personas cuyo acceso resulte estrictamente necesario, y debiendo el destinatario de la información confidencial garantizar que informa a dichas personas del carácter confidencial y propietario de la información así como del Propósito, asegurando que dicho personal trata la información confidencial única y exclusivamente para el Propósito, y absteniéndose de toda divulgación. Una vez finalizado o concluido el Propósito, el cliente debe restituir a SIA toda la información confidencial sin conservar ninguna copia de la misma, no pudiendo utilizar de ninguna manera, ni para ningún fin la información confidencial y/o propietaria facilitada por SIA salvo que haya sido autorizado para ello previa y expresamente por escrito por SIA.

El destinatario de la información confidencial, después de finalizado el Propósito, no podrá utilizar de ninguna manera ni para ningún fin la información confidencial y/o propietaria facilitada por SIA.

Copyright © 2025 SIA. Todos los derechos reservados. España

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

Revisión	Fecha	Autor	Descripción
1.0	30 de Mayo de 2019	SIA	Primera versión del documento resultado de la fusión de las PCs de nivel medio y alto de este perfil de certificado
1.1	3 de Abril de 2020	SIA	Se añade la emisión en software para el nivel medio y corrección de erratas
1.2	17 de noviembre de 2020	SIA	Adecuación a Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
1.3	18 de mayo de 2021	SIA	Se añaden consideraciones según Orden ETD/465/2021 y revisión normativa Se incluye rfc822Name como opcional en el SubjectAlternativeName
1.4	11 de agosto 2021	SIA	Corrección de erratas.
1.5	1 de abril de 2022	SIA	Se incluye diferenciación en el CN de nivel medio centralizado o en software
1.6	16 de enero de 2023	SIA	Cambio de plantilla, actualización de domicilio social y corrección de erratas
1.7	20 de mayo de 2023	SIA	Posibilidad de generación de claves con algoritmos RSA-3072 y RSA-4096 y corrección de erratas
1.8	14 de julio de 2025	SIA	Corrección de erratas. Adecuación a eIDAS2.

INDICE

1. INTRODUCCIÓN	11
1.1 RESUMEN	11
1.2 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN	14
1.3 ENTIDADES Y PERSONAS INTERVINIENTES	14
1.3.1 Autoridad de Certificación / Prestador cualificado de Servicios de Confianza	14
1.3.2 Autoridades de Registro	15
1.3.3 Firmante	15
1.3.4 Suscriptor	15
1.3.5 Solicitudante	16
1.3.6 Terceras Partes Aceptantes.....	16
1.4 USO DE LOS CERTIFICADOS	16
1.4.1 Usos apropiados / permitidos de los certificados.....	16
1.4.2 Limitaciones y restricciones en el uso de los certificados	17
1.5 ADMINISTRACIÓN DE POLÍTICAS.....	18
1.5.1 Organización responsable	18
2. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS	19
2.1 NOMBRES.....	19
2.1.1 Uso de seudónimos	19
2.2 VALIDACIÓN DE LA IDENTIDAD INICIAL.....	19
2.2.1 Métodos para probar la posesión de la clave privada	19
2.2.2 Autenticación de la identidad de una persona física	19

2.2.3 Información no verificada sobre el solicitante	20
2.2.4 Comprobación de las facultades de representación	20
2.3 IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE RENOVACIÓN DE CLAVES	20
3. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS.....	21
3.1 SOLICITUD DE CERTIFICADOS	21
3.2 TRAMITACIÓN DE LAS SOLICITUDES DE CERTIFICADOS	21
3.3 EMISIÓN DE CERTIFICADOS.....	21
3.3.1 Actuaciones de la AC durante la emisión de los certificados	22
3.3.2 Notificación al solicitante de la emisión por la AC del certificado	22
3.4 ACEPTACIÓN DEL CERTIFICADO	22
3.4.1 Forma en la que se acepta el certificado	22
3.4.2 Publicación del certificado por la AC	23
3.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades	23
3.5 PAR DE CLAVES Y USO DEL CERTIFICADO	23
3.5.1 Uso de la clave privada del certificado por el titular	23
3.5.2 Uso de la clave pública y del certificado por los terceros aceptantes.....	23
3.6 RENOVACIÓN DE CERTIFICADOS SIN CAMBIO DE CLAVES	24
3.6.1 Circunstancias para la renovación de certificados sin cambio de claves	24
3.7 RENOVACIÓN DE CERTIFICADOS CON CAMBIO DE CLAVES	24
3.7.1 Circunstancias para una renovación con cambio de claves de un certificado	24
3.7.2 Quien puede pedir la renovación de un certificado	24
3.7.3 Tramitación de las peticiones de renovación con cambio de claves	25
3.7.4 Notificación de la emisión de nuevos certificados al titular	25

3.7.5 Forma de aceptación del certificado con nuevas claves.....	25
3.7.6 Publicación del certificado con las nuevas claves por la AC	25
3.7.7 Notificación de la emisión del certificado por la AC a otras Autoridades	26
3.8 MODIFICACIÓN DE CERTIFICADOS	26
3.8.1 Causas para la modificación de un certificado	26
3.9 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	26
3.9.1 Causas para la revocación.....	26
3.9.2 Quien puede solicitar la revocación	26
3.9.3 Frecuencia de emisión de CRLs.....	27
3.9.4 Requisitos de comprobación en línea de la revocación	27
3.9.5 Otras formas de divulgación de información de revocación.....	27
3.9.6 Requisitos especiales de renovación de claves comprometidas	27
3.9.7 Circunstancias para la suspensión	27
3.10 SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS	28
3.10.1 Características operativas	28
3.10.2 Disponibilidad del servicio	28
3.11 FINALIZACIÓN DE LA SUSCRIPCIÓN	28
3.12 CUSTODIA Y RECUPERACIÓN DE CLAVES.....	28
3.12.1 Prácticas y políticas de custodia y recuperación de claves	28
4. CONTROLES DE SEGURIDAD TÉCNICA.....	30
4.1 GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	30
4.1.1 Generación del par de claves	30

4.1.2 Entrega de la clave privada al titular	30
4.1.3 Entrega de la clave pública al emisor del certificado	30
4.1.4 Tamaño de las claves	31
4.1.5 Parámetros de generación de la clave pública y verificación de la calidad	31
4.1.6 Usos admitidos de la clave (campo KeyUsage de X.509 v3)	31
4.2 PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS	31
4.2.1 Estándares para los módulos criptográficos	31
4.2.2 Control multi-persona (n de m) de la clave privada.....	32
4.2.3 Custodia de la clave privada.....	32
4.2.4 Copia de seguridad de la clave privada	32
4.2.5 Archivo de la clave privada	32
4.2.6 Transferencia de la clave privada a o desde el módulo criptográfico	32
4.2.7 Almacenamiento de la clave privada en un módulo criptográfico.....	33
4.2.8 Método de activación de la clave privada	33
4.2.9 Método de desactivación de la clave privada	33
4.2.10 Método de destrucción de la clave privada	33
4.3 OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES	34
4.3.1 Periodos operativos de los certificados y periodo de uso para el par de claves.....	34
4.4 DATOS DE ACTIVACIÓN	34
4.4.1 Generación e instalación de los datos de activación	34
4.4.2 Protección de los datos de activación	34
5. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP	36

5.1 PERFIL DE CERTIFICADO	36
5.1.1 Número de versión	36
5.1.2 Extensiones del certificado	36
5.1.3 Identificadores de objeto (OID) de los algoritmos	38
5.1.4 Formatos de nombre	38
5.1.5 Restricciones de nombre	38
5.1.6 Identificador de objeto (OID) de la Política de Certificación	40
5.1.7 Uso de la extensión “PolicyConstraints”	40
5.1.8 Sintaxis y semántica de los “PolicyQualifier”	40
5.1.9 Tratamiento semántico para la extensión “Certificate Policy”	41
5.2 PERFILES DE CERTIFICADO CUALIFICADO DE CIUDADANO.....	41
5.2.1 Certificado cualificado de Ciudadano - Nivel medio	41
5.2.2 Certificado cualificado de Ciudadano - Nivel alto FIRMA	45
5.2.3 Certificado cualificado de Ciudadano - Nivel alto AUTH.....	49
6. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD	54
6.1 TARIFAS	54
6.1.1 Tarifas de emisión de certificado o renovación	54
6.1.2 Tarifas de acceso a los certificados.....	54
6.1.3 Tarifas de acceso a la información de estado o revocación	54
6.1.4 Tarifas de otros servicios tales como información de políticas	54
6.1.5 Política de reembolso.....	54

SIA | PC

Certificado cualificado de ciudadano

Fecha: 14 de julio de 2025

RELACION DE TABLAS

Tabla 1 - Datos identificación DPC	14
Tabla 2 - Organización responsable	18
Tabla 3 - Definición extensión SubjectAltName	38
Tabla 4 - OID políticas de certificación	40
Tabla 5 - Perfil certificado nivel medio.....	45
Tabla 6 - Perfil certificado nivel alto Firma.....	49
Tabla 7 - Perfil certificado nivel alto Auth	53

1. Introducción

1.1 Resumen

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

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

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

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

- Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior 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 video 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 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. (Derogado por 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.
- 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. 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 elDAS.

En este contexto, los certificados de ciudadano serán emitidos como certificados cualificados, de conformidad con los requisitos establecidos en los anexos I y II del Reglamento (UE) n.º 910/2014 (elDAS), y desarrollados en la 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: Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part5: QCStatements.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

La Política de Certificación (PC) abarca todas las actividades relacionadas con la gestión del ciclo de vida de los certificados electrónicos, y actúa como documento de referencia en la relación entre SIA y los usuarios de sus servicios telemáticos. En consecuencia, todas las partes involucradas están obligadas a conocer su contenido y a adecuar su actuación a lo establecido en la misma.

Los certificados cualificados de ciudadano están destinados exclusivamente al uso personal de su titular. Su emisión se efectuará en un dispositivo cualificado de creación de firma, o de forma opcional, en soporte software cuando se trate de certificados de nivel medio.

Esta PC desarrolla y complementa lo dispuesto en la Declaración de Prácticas de Certificación (DPC) del Prestador de Servicios de Confianza de SIA, incorporando las normas que regulan el uso de los certificados definidos en esta política, así como su ámbito de aplicación y las características técnicas asociadas.

Se parte del supuesto de que el lector posee conocimientos básicos sobre infraestructura de clave pública (PKI), certificados digitales y firma electrónica. En caso contrario, se recomienda adquirir una comprensión previa de dichos 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	
Versión del documento	1.8	
Estado del documento	Vigente	
Fecha de emisión	11/05/2025	
Fecha de caducidad	No aplicable	
OIDs	1.3.6.1.4.1.39131.10.1.3	(nivel medio)
	1.3.6.1.4.1.39131.10.1.17	(QSCD centralizado o nivel alto)
Ubicación de la PC	https://psc.sia.es/AC_SIA_PC_CIU_MEDIO_y_ALTO_v1.8.pdf	
DPC relacionada	Declaración de Prácticas de Certificación de la PKI de SIA OID 1.3.6.1.4.1.39131.10.1.1.0 Disponible en https://psc.sia.es/	

Tabla 1 - Datos identificación DPC

1.3 Entidades y personas intervenientes

Las entidades y personas intervenientes 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 Certificado cualificado de ciudadano.

En este ámbito, SIA actúa como prestador de servicios de confianza, emitiendo los certificados electrónicos cualificados de firma y proveyendo servicios de firma electrónica cualificada basada en un certificado cualificado y creado mediante un dispositivo cualificado de creación de firma electrónica, 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.

Cada entidad pública 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 entiende por firmante a la persona física titular del certificado cualificado, debidamente identificada en el mismo, que hace uso de los servicios de emisión, gestión y utilización del certificado electrónico.

1.3.4 Suscriptor

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

1.3.5 Solicitante

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

1.3.6 Terceras Partes Aceptantes

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

1.4 Uso de los certificados

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

Los certificados emitidos bajo los criterios de esta política están indicados para soportar firma electrónica avanzada con certificados cualificados, tal y como está definido en los artículos 26 y 27 de eIDAS, garantizando lo siguiente para todas las firmas:

- a) estar vinculada al firmante de manera única;
- b) permitir la identificación del firmante;
- c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
- d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Asimismo, los certificados de nivel alto emitidos conforme a los criterios establecidos en esta Política de Certificación (PC) están habilitados para soportar firma electrónica cualificada, siempre que se emplee un segundo factor de autenticación durante el proceso de firma. En caso de no utilizar dicho segundo factor, el certificado podrá emplearse para la firma electrónica avanzada, siempre que se cumplan las condiciones exigidas en los artículos 26 y 27 del Reglamento (UE) n.º 910/2014 (eIDAS).

1.4.1 Usos apropiados / permitidos de los certificados

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

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

El reglamento eIDAS establece que los Certificados Cualificados de Firma Electrónica cumplirán los requisitos establecidos en el anexo I y II. Por otro lado, la Comisión podrá, mediante actos de

ejecución, establecer números de referencia de normas relativas a los certificados cualificados de firma electrónica donde se presumirá el cumplimiento de los requisitos establecidos en dicho anexo cuando un certificado cualificado de firma electrónica se ajuste a dichas normas.

Los certificados de firma son certificados cualificados de acuerdo con lo que se establece en 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 firma proporciona las siguientes garantías:

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

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

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

1.4.2 Limitaciones y restricciones en el uso de los certificados

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

De forma específica, cabe reseñar que este certificado será utilizado por los firmantes en las relaciones que mantengan con terceros que confían, de acuerdo con los 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 ciudadano se generan a petición del solicitante, una vez se ha personado o realizado el procedimiento equivalente conforme al artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, ha sido validado por la Autoridad de Registro y ha firmado el documento de conformidad con la emisión del certificado cualificado de ciudadano, en el dispositivo cualificado de creación de firma u opcionalmente en software en el caso del nivel medio.

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

Opcionalmente, para certificados cualificados de ciudadano - Nivel medio, la generación de la clave podrá realizarse en software.

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

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

Adicionalmente y conforme al artículo 7.2 de la ley 6/2020 y a la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por video para la expedición de

certificados electrónicos cualificados, este proceso podrá realizarse mediante otros métodos de identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad, siendo por tanto un método de identificación reconocido a escala nacional, permitiendo así el método recogido en el artículo 24.1.bis.c) del Reglamento (UE) 2024/1183.

Los documentos de identidad utilizados deberán incluir una fotografía y disponer de características de seguridad automáticamente comprobables en un proceso de identificación remota por vídeo de forma que se garantice la detección de falsificaciones y manipulaciones.

2.2.3 Información no verificada sobre el solicitante

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

2.2.4 Comprobación de las facultades de representación

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

2.3 Identificación y autenticación para peticiones de renovación de claves

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

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

En el ámbito de emisión de certificados en dispositivos cualificados de creación de firma y opcionalmente en software para el nivel medio, 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 o realizar un procedimiento equivalente 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 o mediante procedimiento equivalente, donde procederá a verificar y firmar el documento de conformidad con la emisión del certificado cualificado de ciudadano de los datos de la solicitud. Con este hecho, acepta los requisitos establecidos en la DPC y en esta PC.

3.2 Tramitación de las solicitudes de certificados

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

Toda evidencia recogida durante el proceso quedará vinculada al mismo y custodiada por el prestador.

En todo momento, se cumplirán los requisitos exigidos en el tratamiento de datos de carácter personal conforme a lo indicado en la DPC.

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 ciudadano se generan en el dispositivo cualificado de creación de firma electrónica (QSCD, por sus siglas en inglés).

La AR verificará la identidad del solicitante y los datos que se incluyan en el certificado, siendo estos registrados en el sistema como un nuevo titular.

El proceso de emisión se realizará en los siguientes pasos:

1. La AR verificará la identidad del solicitante, la integridad 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.
- e) El solicitante accede a la web del proceso de emisión utilizando como posibles controles, su DNI, datos de contraste, código de activación, certificado cualificado y un segundo factor de

autenticación, de manera que para DNI y datos de contraste, siempre van acompañados de un código de activación y/o un segundo factor de autenticación.

- f) El titular deberá introducir la contraseña de protección de su clave privada, tan sólo conocido por el titular y no almacenada en los sistemas, de modo que se garantice el uso de las claves bajo su control exclusivo.

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

Adicionalmente, para certificados cualificados de ciudadano - Nivel Medio, la generación de la clave podrá realizarse en software.

3.3.1 Actuaciones de la AC durante la emisión de los certificados

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

En la emisión de los certificados la AC:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada;
- Protege la confidencialidad e integridad de los datos de registro;
- Incluye en el certificado las informaciones establecidas en el artículo 6 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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

El sistema generará su 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.

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

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

3.4 Aceptación del certificado

3.4.1 Forma en la que se acepta el certificado

La aceptación del certificado es la acción mediante la cual su titular da inicio a sus obligaciones respecto al TSP SIA. El certificado se aceptará en el momento que el instrumento jurídico

vinculante entre el firmante y SIA haya sido firmado y los medios que permitan hacer uso del certificado se encuentren en posesión del firmante.

En el proceso de generación del certificado sobre un dispositivo de creación de firma centralizado y adicionalmente en software para el nivel medio, el propio acto de emisión conlleva la aceptación implícita del certificado como evidencia de la aceptación deberá quedar firmado el documento de conformidad por ambas partes.

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

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

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

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

3.6 Renovación de certificados sin cambio de claves

3.6.1 Circunstancias para la renovación de certificados sin cambio de claves

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

3.7 Renovación de certificados con cambio de claves

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

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

- Expiración de la vigencia del certificado.
- Cambio de datos contenidos en el certificado.
- Claves comprometidas o pérdida de fiabilidad de las mismas.
- Olvido de la contraseña establecida en la emisión del certificado.
- Cambio de formato.

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

3.7.2 Quien puede pedir la renovación de un certificado

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

La renovación del Certificado cualificado de ciudadano en dispositivo de creación de firma centralizada se podrá llevar a cabo de forma telemática siempre y cuando se cumplan los requisitos que la Ley marca con respecto a los plazos máximos permitidos desde que el titular realizó el registro presencial. En caso contrario, para renovar su certificado, el titular tendrá que personarse en una oficina de registro para que pueda volver a activarse su usuario y el certificado.

El titular podrá iniciar el proceso de renovación de certificados de manera telemática como si de una nueva emisión se tratase. La funcionalidad se explica a continuación:

- a) Para el inicio del proceso, el usuario deberá autenticarse con algunos de los siguientes mecanismos: DNI, datos de contraste, código de activación, certificado cualificado y segundo factor, de manera que para dni y datos de contraste, siempre van acompañados de un código de activación y/o un segundo factor de autenticación. Siguiendo las mismas pautas que cuando fue registrado previamente por el Oficial. Si son válidos pasará al siguiente paso.
- b) Se solicita al titular que introduzca la contraseña de su nuevo certificado.
- c) Se procede a la emisión del certificado. Este proceso engloba todas las operaciones necesarias para llevar a cabo la emisión del certificado y es compartido por los procesos de emisión y renovación de certificado.

- d) En ese caso el sistema emitirá y protegerá automáticamente los nuevos certificados, revocando previamente los antiguos, de acuerdo con la normativa vigente sobre certificados electrónicos cualificados.
- e) En todo caso el sistema informará al titular que se ha procedido a la renovación telemática de su certificado y le informará del nuevo periodo de validez del mismo, informando también que el anterior ha sido revocado y que el certificado quedará sin efecto.

Adicionalmente, para los certificados de nivel medio, esta renovación podrá realizarse en software y no en dispositivo de creación de firma centralizada como si de una nueva emisión se tratara.

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 o proceso equivalente 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 o seguir procedimiento equivalente y efectuar el proceso de emisión de certificados, como si del proceso inicial se tratara.

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

3.7.4 Notificación de la emisión de nuevos certificados al titular

Al tratarse de una renovación de certificados con cambio de claves, siguiendo el proceso de emisión de certificados como si del proceso inicial se tratara, una vez generado éste satisfactoriamente, se notificará al firmante que se ha procedido a la renovación telemática de su certificado y le informará del nuevo periodo de validez del mismo, informando también de que el anterior certificado ha sido revocado y que el certificado quedará sin efecto.

3.7.5 Forma de aceptación del certificado con nuevas claves

Para el ámbito de certificados custodiados por dispositivos de creación de firma centralizada o adicionalmente en software para el nivel medio, en los casos de renovación del certificado, el propio acto de renovación conlleva la aceptación implícita del certificado previa aceptación y firma del documento de conformidad con la emisión del certificado cualificado de ciudadano.

3.7.6 Publicación del certificado con las nuevas claves por la AC

El certificado cualificado de ciudadano no se publicará.

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

No se efectúan notificaciones a terceros.

3.8 Modificación de certificados

3.8.1 Causas para la modificación de un certificado

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

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

3.9 Revocación y suspensión de certificados

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

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

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

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

3.9.1 Causas para la revocación

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

Adicionalmente, por compromiso de las claves privadas, por pérdida, robo, hurto, modificación, divulgación o revelación de la clave personal de acceso que permite la activación de las claves privadas o revelación de las claves de acceso que permite la activación de la clave privada alojada en un dispositivo de firma centralizada, bien por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por entidad ajena a 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 a nombre del cual fue expedido el certificado.
- El suscriptor, que es la entidad con personalidad jurídica que suscribe un contrato con SIA para la expedición de certificados.
- La Entidad de Registro que intervino en la emisión.
- La propia AC de SIA cuando tenga conocimiento de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.

3.9.3 Frecuencia de emisión de CRLs

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

3.9.4 Requisitos de comprobación en línea de la revocación

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

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

3.9.5 Otras formas de divulgación de información de revocación

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

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

3.9.6 Requisitos especiales de renovación de claves comprometidas

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

3.9.7 Circunstancias para la suspensión

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

3.10 Servicios de información del estado de certificados

3.10.1 Características operativas

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

3.10.2 Disponibilidad del servicio

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

3.11 Finalización de la suscripción

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

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

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

3.12 Custodia y recuperación de claves

3.12.1 Prácticas y políticas de custodia y recuperación de claves

El TSP en ningún momento podrá recuperar la clave de los usuarios. En caso de pérdida u olvido de la contraseña de acceso a las mismas se deberá revocar el certificado y emitir uno nuevo.

En el ámbito del Certificado Cualificado de ciudadano alojado en dispositivo de Firma Centralizada, la clave privada que se genera en un dispositivo cualificado de creación de firma quedará custodiada por el TSP, 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 este sentido, el acceso a dicha clave sólo puede ser efectuado por el titular de la misma mediante una aplicación al efecto donde el titular deberá estar debidamente autenticado. Posteriormente para la firma, deberá introducir el PIN de protección de su certificado tan sólo conocido por el titular y no almacenado en los sistemas, más un segundo factor de autenticación en el caso de los certificados de nivel alto.

Sólo Prestadores de servicios de certificación que expidan certificados cualificados podrán gestionar los datos de creación de firma electrónica en nombre del firmante. Para ello, podrán efectuar una copia de seguridad de los datos de creación de firma siempre que la seguridad de los datos duplicados sea del mismo nivel que la de los datos originales y que el número de datos duplicados

no supere el mínimo necesario para garantizar la continuidad del servicio. No se podrán duplicar los datos de creación de firma para ninguna otra finalidad.

La autoridad competente realiza copias de seguridad de las claves privadas protegidas, tanto las que están en dispositivo de firma como en software, siendo éstas únicamente accesibles por el titular.

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.

Adicionalmente, para el nivel medio, cuya generación y almacenamiento de la clave se haya realizado en software, la custodia también será responsabilidad del titular.

4. CONTROLES DE SEGURIDAD TÉCNICA

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

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

4.1 Generación e instalación del par de claves

4.1.1 Generación del par de claves

Los pares de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan en un dispositivo cualificado de creación de firma o QSCD (apartado 6.2.1 de la DPC). Las claves son protegidas por el firmante con su PIN o contraseña y un segundo factor en el caso de los certificados de nivel alto para la realización de firma electrónica cualificada.

Adicionalmente, los certificados de nivel medio, podrán emitirse en software.

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 o realizado procedimiento equivalente y validado y validado por la AR, por medio de un proceso ajustado a la Ley.

La clave privada se genera en un dispositivo cualificado de creación de firma bajo el control exclusivo del firmante y, por lo tanto, 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 cualificado de creación de firma electrónica o puede ser generada en software para el nivel medio 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 ciudadano emplean claves con un tamaño de 2048, 3072 o 4096 bits, en función del nivel de seguridad requerido y conforme a 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)

Para nivel medio: la clave definida por la presente política, y por consiguiente el certificado asociado, se utilizará para la firma electrónica de documentos relacionados con el suscriptor.

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

- **Key Usage:** nonRepudiation, DigitalSignature y Key Encipherment.

Para nivel alto: la clave definida por la presente política, y por consiguiente de los certificados asociados, se utilizarán para la firma electrónica de documentos relacionados con el suscriptor y la autenticación.

A tal efecto, en el campo “key Usage” de los certificados se ha incluido los siguientes usos en función del certificado (autenticación o firma):

- **Key Usage:** nonrepudiation (para certificado de firma), DigitalSignature y Key Encipherment (para certificado de autenticación).

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.

El dispositivo empleado para la creación de claves utilizadas por los certificados cualificados de ciudadano es un dispositivo de creación de firma o QSCD (apartado 6.2.1 de la DPC).

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

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

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

Para las claves generadas en software, el usuario final es el encargado de su custodia, y éste será el responsable de mantenerla bajo su exclusivo control.

4.2.4 Copia de seguridad de la clave privada

En el ámbito de los certificados cualificados de ciudadano sobre dispositivo cualificado de creación de firma o de claves generadas en software (opcionalmente sólo nivel medio), la autoridad competente realiza copias de seguridad de las claves privadas protegidas, manteniendo el nivel de seguridad y siendo éstas únicamente accesibles por el titular.

4.2.5 Archivo de la clave privada

En el caso del dispositivo cualificado de creación de firma electrónica y de claves generadas en software, la autoridad competente mantiene, según la legislación vigente, las copias de seguridad con las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.

Adicionalmente, en el caso de las claves generadas en software, el usuario final también es el encargado de su archivado, y éste será el responsable de mantenerla bajo su exclusivo control.

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

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

4.2.7 Almacenamiento de la clave privada en un módulo criptográfico

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

4.2.8 Método de activación de la clave privada

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

El acceso a la clave privada del titular depende del dispositivo en el que esté generada, debiendo introducir al menos una contraseña tan sólo conocida por el titular y no almacenada en los sistemas.

La activación de la clave privada en el caso del dispositivo cualificado de creación de firma electrónica, requiere autenticación del titular en el sistema, siendo necesario introducir un identificador de usuario (DNI/NIE/Pasaporte), una contraseña tan sólo conocida por el titular y no almacenada en los sistemas, más un segundo factor de autenticación en el caso de los certificados de nivel alto para la realización de firma electrónica cualificada.

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.

Si un titular autenticado en el sistema introduce repetidamente una contraseña de firma incorrecta, tanto su clave como su certificado de firma se bloquearán temporalmente de forma automática. En el caso de un dispositivo cualificado de creación de firma centralizado, podrá implementarse una prueba de Turing (captcha) como medida adicional de seguridad.

En el caso de claves generadas en software es responsabilidad del titular desactivar el acceso a la clave privada

4.2.10 Método de destrucción de la clave privada

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

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

En el caso de claves generadas en software es también responsabilidad del titular su destrucción.

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 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.

En el caso que haya transcurrido menos de 5 años desde la identificación inicial de la persona física, y en cumplimiento de los requisitos indicados en el artículo 7.6 de la Ley 6/2020 de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, no será requerida una nueva identificación, en caso contrario, la renovación deberá tramitarse ante SIA por medio de la Autoridad de Registro Reconocida presencialmente o utilizando otros métodos de identificación reconocidos a escala nacional que garanticen una seguridad equivalente en términos de fiabilidad a la presencia física

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

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

4.4 Datos de activación

4.4.1 Generación e instalación de los datos de activación

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

4.4.2 Protección de los datos de activación

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

Cuando la generación se realiza en software, la instalación y puesta en marcha de la clave privada asociada a los certificados, requiere la utilización de los sistemas de seguridad del propio usuario, debiendo introducir al menos una contraseña tan sólo conocida por él y no almacenada en los sistemas.

La contraseña que protege la clave privada asociada a un certificado digital tiene carácter confidencial, personal e intransferible. Su correcta custodia resulta esencial, ya que es el mecanismo que salvaguarda el uso de la clave privada y permite la utilización segura del certificado en los servicios ofrecidos a través de redes de comunicación.

Por ello, deben observarse estrictamente las siguientes normas de seguridad:

- Memorice la contraseña y evite anotarla en cualquier soporte, ya sea físico o electrónico, que conserve el Titular.
- No la comparta ni la comunique a terceros bajo ningún concepto, independientemente del medio (teléfono, correo electrónico, mensajería, etc.).
- Recuerde que la contraseña es de uso exclusivo del Titular. En caso de que exista la posibilidad de que haya sido conocida por otra persona, deberá cambiarla de inmediato.
- El uso de la contraseña por parte de alguien distinto al Titular se considerará una negligencia grave y puede dar lugar al uso indebido de la clave privada, incluida la realización de operaciones de firma electrónica en su nombre.
- El Titular tiene la obligación de notificar de forma inmediata cualquier pérdida de control sobre su clave privada o indicios de compromiso, ya que esto constituye motivo de revocación del certificado asociado.
- Como medida adicional, evite utilizar contraseñas relacionadas con datos personales (fechas de nacimiento, números de teléfono, secuencias repetitivas o fácilmente predecibles, fragmentos del DNI, etc.).
- Se recomienda modificar la contraseña de forma periódica, reforzando así la seguridad del certificado.

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 Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Público (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 Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

5.1.1 Número de versión

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

5.1.2 Extensiones del certificado

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

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

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

Las extensiones utilizadas en los certificados son:

- Authority Key Identifier.
- Subject Key Identifier.
- KeyUsage. Calificada como crítica.
- ExtKeyUsage.
- CRL Distribution Point.
- Authority Information Access.

- Qualified Certificate Statements.
- CertificatePolicies.
- Subject Alternative Name.

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

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

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

SIA tiene definida una política de asignación de OIDs dentro de su rango privado de numeración por la cual el OID de todas las Extensiones propietarias de Certificados de SIA comienza por el prefijo 1.3.6.1.4.1.39131.10.3.

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

OID	Concepto	Descripción
1.3.6.1.4.1.39131.10.2.1	Tipo de certificado	Tipo de certificado
1.3.6.1.4.1.39131.10.2.2	Nombre	Nombre del usuario
1.3.6.1.4.1.39131.10.2.3	Apellido1	Primer apellido del usuario
1.3.6.1.4.1.39131.10.2.4	Apellido2	Segundo apellido del usuario

1.3.6.1.4.1.39131.10.2.5	DNI/NIE/Pasaporte	DNI/NIE/Pasaporte del usuario
1.3.6.1.4.1.39131.10.2.8	Nombre Colegio	Nombre del colegio profesional (Opcional)
1.3.6.1.4.1.39131.10.2.9	Número de Colegio	Identificados del colegio profesional (Opcional)
1.3.6.1.4.1.39131.10.2.10	Número de Colegiado	Número o Identificador del colegiado (Opcional)
1.3.6.1.4.1.39131.10.2.11	Comunidad	Comunidad de la Oficina (Opcional)
1.3.6.1.4.1.39131.10.2.12	Provincia	Provincia de la Oficina (Opcional)
1.3.6.1.4.1.39131.10.2.13	Localidad	Localidad de la Oficina (Opcional)

Tabla 3 - Definición extensión SubjectAltName

5.1.3 Identificadores de objeto (OID) de los algoritmos

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

5.1.4 Formatos de nombre

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

5.1.5 Restricciones de nombre

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

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

- CN, GN, SN, serialNumber, OU, O, C.

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

Para nivel medio

- CN, dependiendo del documento con el que se realice la identificación del titular y la información que se muestre en el CN, las opciones son las siguientes:
 - DNI, CN = Apellido1 Apellido2 Nombre - DNI NNNNNNNNA
 - NIE, CN = Apellido1 Apellido2 Nombre - NIE ANNNNNNNNA

- Pasaporte, CN = Apellido1 Apellido2 Nombre - PAS AAAAAAAA
 - No se muestra nada, independientemente del documento aportado, CN = Apellido1 Apellido2 Nombre.
 - Podrá contener la cadena “SW” al final para los certificados en software
- GN = Nombre
- SN = Apellido1
- serialNumber = Codificado según las normas ETSI EN 319 412-1 y RFC 3739 apartado 3.2.6.1, relativo a la codificación de la información semántica. Las opciones en función del documento de identidad serían las siguientes:
 - DNI sería IDCES-NNNNNNNNNA
 - NIE sería IDCES-ANNNNNNNNA
 - Pasaporte sería PASES-XXXXXXXXXX
- OU= Código de entidad suscriptora
- O= Razón social de SIA
- C = País del ciudadano. En este caso, España. El atributo “C” (country) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en PrintableString.

Para nivel alto

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

Si es de autenticación, la codificación del campo sería:

- DNI sería NNNNNNNNNNA
- NIE sería ANNNNNNNNNNA
- Pasaporte sería XXXXXXXXXX
- OU= Código de entidad suscriptora
- O= Razón social de SIA
- C = País del ciudadano. En este caso, España. El atributo “C” (country) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en PrintableString.

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

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

Los El OIDs de la presente PC son 1.3.6.1.4.1.39131.10.1.3 para nivel medio y 1.3.6.1.4.1.39131.10.1.17 para nivel alto. Los identificadores de los certificados expedidos bajo la presente Política de Certificación son los siguientes:

Política de Certificados	OID
Cualificados de Ciudadano	1.3.6.1.4.1.39131.10.1.3 (nivel medio)
	1.3.6.1.4.1.39131.10.1.17 (QSCD centralizado o nivel alto)
QCP-n-qscd	0.4.0.194112.1.2

Tabla 4 - OID políticas de certificación

5.1.7 Uso de la extensión “PolicyConstraints”

No estipulado.

5.1.8 Sintaxis y semántica de los “PolicyQualifier”

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

- **URL DPC:** contiene la URL donde puede obtener la última versión de la DPC y de las Políticas de Certificación asociadas.
- **Notice Reference:** Nota de texto que se despliega en la pantalla, a instancia de una aplicación o persona, cuando un tercero verifica el certificado.

Y el siguiente “Policy Identifier”:

Para nivel medio

- **QCP-n:** indicación de certificado cualificado de firma, acorde a eIDAS.

Para nivel alto

- **OID 1.3.6.1.4.1.39131.10.1.17:** del certificado cualificado de Ciudadano - Nivel alto en QSCD centralizado.
- **QCP-n-qscd:** indicación de certificado cualificado de firma, acorde a eIDAS. Sólo para el certificado de firma.
- **NCP+:** Indicación de certificado acorde a una política normalizada, en dispositivo seguro acorde al Reglamento eIDAS. Sólo para el certificado de autenticación.

5.1.9 Tratamiento semántico para la extensión “Certificate Policy”

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

5.2 Perfiles de Certificado cualificado de Ciudadano

5.2.1 Certificado cualificado de Ciudadano - 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 + <=3 años	
Subject (Asunto)		
Country (C)	<Código de país de dos letras>	País de dos letras donde esté registrada la empresa
Organización (O)	<Razón social de la Empresa del Usuario> - NIF <NIF de la Empresa del usuario>	Razón social y NIF de la empresa del usuario
Organización Unit (OU)	<Código de entidad suscriptora>	
Serial Number (SerialNumber)	Ej: IDCES-<DNI> IDCES-<NIE> PASES-<Pasaporte>	DNI/NIE/Pasaporte/ Documento de identificación del usuario según ETSI EN 319 412-1
Common Name (CN)	<Nombre> <Apellido1> <Apellido2> [- <ID>]	Nombre, apellidos y DNI/NIE/Pasaporte/ Documento de identificación del usuario de empresa
Surname	<Apellido1>	Primer apellido
Given Name	<Nombre>	Nombre de pila
Subject Public Key Info	Clave pública (RSA-2048 Bits, RSA-3072 o RSA-4096), 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	1 (seleccionado)	
Key Encipherment	1 (seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	0 (no seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
ExtendedKeyUsage		
Email Protection	1 (seleccionado)	
Client Authentication	1 (no 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)
QCSyntax-v2	OID 1.3.6.1.5.5.7.11.2	

id-etsi-qcs-semanticsId-Natural	OID 0.4.0.194121.1.1
QcType	OID 0.4.0.1862.1.6
id-etsi-qct-esign	OID 0.4.0.1862.1.6.1
QcPDS	OID 0.4.0.1862.1.5
PdsLocation	https://psc.sia.es/en (en)
Certificate Policies	
Policy Identifier	1.3.6.1.4.1.39131.10.1.3
Policy Qualifier ID	Especificación de la DPC
CPS Pointer	https://psc.sia.es/
User Notice	“Certificado cualificado de Ciudadano de nivel medio. Condiciones de uso y vías de contacto en: https://psc.sia.es ”
Policy Identifier	QCP-n
Subject Alternative Name	
rfc822Name	<email> Email del usuario (Opcional)
Tipo del certificado	OID: 1.3.6.1.4.1.39131.10.2.1: CIUDADANO
Nombre	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre> Nombre del usuario
Primer apellido	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido1> Primer apellido del usuario
Segundo apellido	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido2> Segundo apellido del usuario
DNI	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI> <NIE> <Pasaporte> DNI NIE Pasaporte del usuario
Nombre Colegio	OID: 1.3.6.1.4.1.39131.10.2.8: <Nombre Colegio> Nombre del colegio profesional

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

Tabla 5 - Perfil certificado nivel medio

5.2.2 Certificado cualificado de Ciudadano - Nivel alto FIRMA

Nombre Atributo	Valor	Observaciones
Campos X509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada emisora	
Signature Algorithm	SHA-256 con RSA-2048, 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 + <=3 años	
	Subject (Asunto)	
Country (C)	ES	España
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	Razón social de SIA
Organizational Unit (OU)	< Código de entidad suscriptora >	
Serial Number (serialNumber)	IDCES-<DNI> IDCES-<NIE> PASES-<Pasaporte>	DNI/NIE/Pasaporte del usuario según ETSI EN 319 412-1
Surname	<Apellido1>	Primer apellido
Given Name	<Nombre>	Nombre de pila
Common Name (CN)	<Apellido1> <Apellido2> <Nombre>[- DNI <DNI> NIE <NIE> PAS <Pasaporte>] FIRMA	Nombre, apellidos y DNI/NIE/Pasaporte del ciudadano
Subject Public Key Info	Clave pública (RSA-2048 Bits, RSA-3072 o RSA-4096), codificada de acuerdo con el algoritmo criptográfico	
	Extensiones x509 v3	
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage	Marcado como crítica	
Digital Signature	0 (no seleccionado)	
Content Commitment	1 (seleccionado)	
Key Encipherment	0 (no seleccionado)	
Data Encipherment	0 (no seleccionado)	

Key Agreement	0 (no seleccionado)	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
ExtendedKeyUsage		
Email Protection	0 (no seleccionado)	
Client Authentication	0 (no 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)
QcSSCD	OID 0.4.0.1862.1.4	Uso de dispositivo cualificado de creación de firma electrónica
QcType	OID 0.4.0.1862.1.6	
id-etsi-qct-esign	OID 0.4.0.1862.1.6.1	
QCSyntax-v2	OID 1.3.6.1.5.5.7.11.2	

id-etsi-qcs- semanticsId-Natural	OID 0.4.0.194121.1.1	
QcPDS	OID 0.4.0.1862.1.5	
PdsLocation	https://psc.sia.es/en (en)	
Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.17	QSCD centralizado o nivel alto
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	“Certificado cualificado de firma electrónica de Ciudadano de nivel alto. Condiciones de uso y vías de contacto en: https://psc.sia.es ”	
Policy Identifier	1.3.6.1.4.1.39131.10.1.17	QSCD centralizado o nivel alto
Subject Alternative Name		
rfc822Name	<email>	Email del usuario (Opcional)
Tipo del certificado	OID: 1.3.6.1.4.1.39131.10.2.1: CIUDADANO	
Nombre	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del usuario
Primer apellido	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido1>	Primer apellido del usuario
Segundo apellido	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido2>	Segundo apellido del usuario
DNI	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI> <NIE> <Pasaporte>	DNI NIE Pasaporte del usuario
Nombre Colegio	OID: 1.3.6.1.4.1.39131.10.2.8: <Nombre Colegio>	Nombre del colegio profesional
Número de Colegio	OID: 1.3.6.1.4.1.39131.10.2.9: <Nº de Colegio>	Identificador del colegio profesional

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

Tabla 6 - Perfil certificado nivel alto Firma

5.2.3 Certificado cualificado de Ciudadano - Nivel alto AUTH

Nombre Atributo	Valor	Observaciones
Campos X509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada emisora	
Signature Algorithm	SHA-256 con RSA-2048, RSA-3072 o RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	ES
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	SISTEMAS INFORMATICOS ABIERTOS SAU
Organization 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 + <=3 años	
	Subject (Asunto)	
Country (C)	ES	España
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	Razón social de SIA
Organizational Unit (OU)	< Código de entidad suscriptora >	
Serial Number (serialNumber)	<DNI> <NIE> <Pasaporte>	DNI/NIE/Pasaporte del usuario
Surname	<Apellido1>	Primer apellido
Given Name	<Nombre>	Nombre de pila
Common Name (CN)	<Apellido1> <Apellido2> <Nombre>[- DNI <DNI> NIE <NIE> PAS <Pasaporte>] AUTH	
Subject Public Key Info	Clave pública (RSA-2048 Bits, RSA-3072 o RSA-4096), codificada de acuerdo con el algoritmo criptográfico	
	Extensiones x509 v3	
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage	Marcado como crítica	
Digital Signature	1 (seleccionado)	

Content Commitment (nonRepudiation)	0 (no seleccionado)
Key Encipherment	1 (seleccionado)
Data Encipherment	0 (no seleccionado)
Key Agreement	0 (no seleccionado)
Key Certificate Signature	0 (no seleccionado)
CRL Signature	0 (no seleccionado)
EncipherOnly	0 (no seleccionado)
DecipherOnly	0 (no seleccionado)
Extended Key Usage	Extended Key Usage
Email Protection	0 (no 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
Certificate Policies	
Policy Identifier	1.3.6.1.4.1.39131.10.1.17 QSCD centralizado o nivel alto
Policy Qualifier ID	Especificación de la DPC

CPS Pointer	https://psc.sia.es/	
User Notice	“Certificado de Ciudadano de nivel alto, autenticación. Condiciones de uso y vías de contacto en: https://psc.sia.es ”	
Policy Identifier	NCP+	
Subject Alternative Name		
rfc822Name	<email>	Email del usuario (Opcional)
Tipo del certificado	OID: 1.3.6.1.4.1.39131.10.2.1: CIUDADANO	
Nombre	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del usuario
Primer apellido	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido1>	Primer apellido del usuario
Segundo apellido	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido2>	Segundo apellido del usuario
DNI	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI> <NIE> <Pasaporte>	DNI NIE Pasaporte del usuario
Nombre Colegio	OID: 1.3.6.1.4.1.39131.10.2.8: <Nombre Colegio>	Nombre del colegio profesional
Número de Colegio	OID: 1.3.6.1.4.1.39131.10.2.9: <Nº de Colegio>	Identificador del colegio profesional
Número de Colegiado	OID: 1.3.6.1.4.1.39131.10.2.10: <Nº de Colegiado>	Número o Identificador del colegiado
Comunidad	OID: 1.3.6.1.4.1.39131.10.2.11: <Comunidad>	Comunidad de la Oficina

Provincia	OID: 1.3.6.1.4.1.39131.10.2.12: <Provincia>	Provincia de la Oficina
Localidad	OID: 1.3.6.1.4.1.39131.10.2.13: <Localidad>	Localidad de la Oficina
Numero de Oficina	OID: 1.3.6.1.4.1.39131.10.2.14: <Nº Oficina>	Número o Identificador de la Oficina
Tipo de Oficina	OID: 1.3.6.1.4.1.39131.10.2.15: <Tipo Oficina>	Tipo de la Oficina

Tabla 7 - Perfil certificado nivel alto Auth

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 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