An Indra company

PC - SIA

Política de Certificación

Certificados de autenticación de sitio Web y Sede Electrónica

Certificados cualificados de autenticación de sitio web – Nivel medio

Certificados cualificados de autenticación de sitio web y PSD2 – Nivel medio

Certificados cualificados de Sede electrónica– Nivel medio

Certificados cualificados de Sede electrónica – Nivel alto

OID: 1.3.6.1.4.1.39131.10.1.21

Versión:1.4

SIA | PC

Certificado de autenticación de sitio web y Sede electrónica

Fecha: 10 de mayo de 2023

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

Revisión	Fecha	Autor	Descripción
1.0	17 de noviembre de 2020	SIA	Primera versión del documento
1.1	08 de junio de 2021	SIA	Revisión de nuevas versiones de CAB/Forum Aclaración OID políticas para PSD2, apartado 1.2
1.2	01 de mayo de 2022	SIA	Revisión de últimas versiones de CAB/Forum y ETSI 319 411-2 (2021-11)
1.3	16 de enero de 2023	SIA	Cambio de plantilla, actualización de domicilio social y corrección de erratas
1.4	10 de mayo de 2023		Revisión anual y detallar de manera más clara que no se emiten certificados DV ni OV.

INDICE

RELACION DE TABLAS

1. Introducción

1.1 Resumen

El presente documento recoge la Política de Certificación correspondiente a los certificados de Autenticación de Sitio Web, emitidos por la Autoridad de Certificación (en adelante AC) del prestador de servicios de confianza (TSP), Sistemas Informáticos Abiertos Sociedad Anónima(en adelante SIA), 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, de acuerdo con Certification Authority/Browser Forum (CA/B Forum) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificate (en adelante, Baseline Requirements), CA/B Forum Guidelines for Extended Validation Certificates (en adelante, EV Guidelines) y con el Reglamento (UE) 910/2014 (en adelante, el Reglamento eIDAS).

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 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate Profile for web site certificates.
- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

- *CA/Browser Forum* Guidelines For The Issuance And Management Of Extended Validation Certificates (*EVBR)*
- *CA/Browser Forum* Baseline Requirements for the Issuance and Management of publicly-Trusted Certificates (BR), publicados en http://www.cabforum.org por el CA/Browser Forum. En caso de cualquier inconsistencia entre esta Política de Certificación y los citados requisitos, prevalecerán dichos requisitos.

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

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante eIDAS) y por el que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de octubre de 2016).
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.

- Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera., que transpone la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior (PSD2)
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. El Ministerio de Hacienda y Administraciones Públicas define el perfil del certificado de sede electrónica.
- Artículo 45 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo del 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

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 cualificados de Autenticación de sitio Web de nivel medio serán emitidos como **Certificados Cualificados de Autenticación de sitios Web** (QWAC) cumpliendo los requisitos establecidos en el anexo IV de eIDAS.

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 autenticación de sitio web – Nivel medio, los certificados cualificados de autenticación de sitio web PSD2 – Nivel medio, como los certificados de Sede electrónica – Nivel medio y Nivel alto, cumplen los requisitos establecidos en el anexo IV del Reglamento eIDAS 910/2014.

Todos los certificados definidos en la presente política tienen como finalidad establecer comunicaciones de datos en servidores web vía SSL/TLS.

Permiten el cifrado de las comunicaciones entre el usuario y el sitio web, facilitando el intercambio de las claves de cifrado necesarias para el cifrado de la información a través de Internet. La emisión de estos certificados se realizará en soporte software o en Módulos de Seguridad Hardware (HSM).

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

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

Cumpliendo la norma EN 319 411-2, que establece requisitos para los proveedores de servicios de confianza que emiten certificados cualificados de la UE, en lo que respecta a los certificados de autenticación de sitios web cualificados, esta política ofrece el nivel de calidad definido en el Reglamento (UE) no 910/2014 para certificados cualificados.

Los requisitos de esta política de certificados incluyen todos los requisitos de la política de certificados de validación ampliada (EVCP), además de disposiciones adicionales adecuadas para admitir la emisión y gestión de certificados cualificados de la UE, tal como se especifica en el Reglamento (UE) no 910/2014."

La directiva de certificado de validación extendida (mencionada como base para la directiva de certificado cualificado de autenticación de sitio web), se define en la norma EN 319 411-1, que se refiere a todos los TSP que emiten certificados públicos. EVCP es una política para certificados SSL/TLS que ofrecen el nivel de garantía requerido por CA/Browser Forum para EV. Los requisitos de esta directiva de certificado se basan en los requisitos de directiva normalizados para la emisión y administración de certificados de certificado normalizado, mejorados para hacer referencia a los requisitos de las directrices de validación extendida.

De acuerdo con las políticas de certificación establecidas por ETSI, SIA sigue la siguiente política.

- EVCP (Extended Validation Certificates Policy)

SIA mantiene sitios diferentes con al menos un certificado final válido, otro caducado y otro revocado

En el ámbito del proyecto de Google Certificate Transparency, los certificados SSL emitidos se publicarán en el servicio CT de los proveedores de Log Servers con los cuales SIA mantiene un acuerdo.

Los distintos certificados definidos en la presente política son los siguientes:

Certificados Cualificados de Autenticación de Sitio Web (QWAC). SSL Cualificado Validación Extendida (EV)

Son certificados emitidos a servidores de páginas web expedidos de acuerdo con un conjunto específico de criterios de verificación de la identidad de la organización identificada en el certificado.

Un certificado SSL EV permite a los navegadores que se conectan a este servicio, mostrar un nivel de seguridad adicional.

Este certificado es emitido con la consideración de cualificado cumpliendo los requisitos establecidos en el anexo IV del Reglamento eIDAS 910/2014. Es un QWAC (ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-4 y CA/B Forum EV Guidelines).

Será utilizado para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía robusta al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado:

- La existencia legal, física y operativa de la entidad.

- La identidad de la entidad coincide con los registros oficiales.
- La entidad tiene el derecho exclusivo de usar el dominio especificado en el certificado EV
- La entidad ha autorizado adecuadamente la emisión del certificado EV.

Se ajusta a los requerimientos del CA/Browser Forum establecidos en el documento "Guidelines for the issuance and management of Extended Validation certificates" vigente en el momento de la publicación de la presente política.

Certificados Cualificados de Autenticación de Sitio Web para PSD2 (QWAC PSD2). SSL Cualificado Validación Extendida (EV)

Este certificado es emitido con la consideración de cualificado según Reglamento eIDAS, es un QWAC (ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-4 y CA/B Forum EV Guidelines) emitido en conformidad con la ETSI TS 119 495 y en cumplimiento con los Regulatory Technical Standards (RTS) del Reglamento Delegado (UE) 2018/389 de la Comisión, por el que se complementa la Directiva (UE) 2015/2366, y el Real Decreto-ley 19/2018 de España, respetando las directrices establecidas por la Autoridad Nacional Competente de servicios de pago. SIA AC garantiza un procedimiento de identificación de la titularidad del dominio y acreditación de la organización titular del mismo, equivalente al procedimiento seguido para la emisión de certificados con Validación Extendida (EV).

Certificados Cualificado de Sede Electrónica Nivel Medio y alto

En el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, SIA AC emite certificados del tipo sede electrónica. Se emiten según la política de ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-4, en conformidad con los EV Guidelines de CA/B Forum, CA/Forum Browser Guidelines y el perfil de certificado de Sede definido por el Ministerio de Hacienda y Administraciones Públicas. Son certificados cualificados de autenticación web de nivel medio o alto conforme al Reglamento eIDAS. Identifican a la Administración Pública, órgano o entidad administrativa titular de la sede.

1.2 Nombre del documento e identificación

Nombre del documento	Política de Certificación de autenticación de sitios web y Sede Electrónica
Versión del documento	1.4
Estado del documento	Vigente
Fecha de emisión	10/04/2023
Fecha de caducidad	No aplicable

OID	1.3.6.1.4.1.39131.10.1.21
Ubicación de la PC	https://psc.sia.es/
DPC relacionada	Declaración de Prácticas de Certificación de la PKI de SIA OID 1.3.6.1.4.1.39131.10.1.1.1.0 Disponible en https://psc.sia.es/

Tabla 1 – Datos identificación DPC

Se incluyen como cumplimiento de esta Política con los criterios adoptados por CA/B Forum y ETSI, los siguientes OID:

Certificados	OID ETSI	OID CA/Browser Forum
Certificados Cualificados de Autenticación de Sitio Web (QWAC). SSL Cualificado Validación Extendida (EV)	1.3.6.1.4.1.39131.10.1.21.1: OID SIA 0.4.0.194112.1.4: QEVCP-w 0.4.0.2042.1.4 (EVCP)	2.23.140.1.1
Certificados Cualificados de Autenticación de Sitio Web PSD2 (QWAC). SSL Cualificado Validación Extendida (EV)	1.3.6.1.4.1.39131.10.1.21.1: OID SIA 0.4.0.194112.1.4: QEVCP-w 0.4.0.19495.3.1: QCP-w-psd2 0.4.0.2042.1.4 (EVCP)	2.23.140.1.1
Certificados Cualificado de Sede Electrónica. Nivel Alto SSL Cualificado con Validación Extendida (EV)	1.3.6.1.4.1.39131.10.1.21.1: OID SIA 0.4.0.194112.1.4: QEVCP-w y 0.4.0.2042.1.4 (EVCP) En el ámbito de la Administración General del Estado de España y de sus organismos públicos, en la extensión CertificatePolicies (2.5.29.32), se incluirá en PolicyInformation En el caso de "Sede Electrónica Nivel Alto", la extensión CertificatePolicies (2.5.29.32) incluirá el OID: — 2.16.724.1.3.5.5.1	2.23.140.1.1

Certificados Cualificado de Sede Electrónica. Nivel Medio SSL Cualificado con Validación Extendida (EV)	1.3.6.1.4.1.39131.10.1.21.1: OID SIA 0.4.0.194112.1.4: QEVCP-w 0.4.0.2042.1.4 (EVCP). En el ámbito de la Administración General del Estado de España y de sus organismos públicos, en la extensión CertificatePolicies (2.5.29.32), se incluirá en PolicyInformation En el caso de "Sede Electrónica Nivel Medio/Sustancial", la extensión CertificatePolicies (2.5.29.32) incluirá el OID: — 2.16.724.1.3.5.5.2	2.23.140.1.1

Tabla 2 – Datos identificación certificados. OID políticas de certificación

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 solicitantes.
- Los Suscriptores.
- Las Terceras partes aceptantes de los certificados emitidos.
- Responsable de Dictámenes de Emisión

1.3.1 Autoridad de Certificación / Prestador cualificado de Servicios de Confianza

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

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

- "AC raíz" Autoridad de Certificación de primer nivel. Esta AC solo emite certificados para sí misma y sus AC subordinadas, a excepción de la emisión del certificado de validación de OCSP y la emisión de la ARL. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.
- "AC raíz 2020" Autoridad de Certificación de primer nivel. Esta AC solo emite certificados para sí misma y sus AC subordinadas, a excepción de la emisión del certificado de validación

de OCSP y la emisión de la ARL. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.

- "AC subordinada": Autoridad de Certificación subordinada de "AC raíz". Su función es la emisión de certificados para terceros.
- "AC subordinada SSL": 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 autenticación de sitio web – Nivel medio
    - Certificado cualificado de autenticación de sitio web para PSD2 – Nivel medio
    - Certificado cualificado de Sede electrónica – Nivel medio
    - Certificado cualificado de Sede electrónica – Nivel alto

En este ámbito, SIA actúa como prestador de servicios de confianza, emitiendo los certificados electrónicos cualificados de autenticación de sitio web, conforme a lo establecido en eIDAS .

1.3.2 Autoridades de Registro

La gestión de las solicitudes y emisión de los certificados será realizada por las entidades que actúen como Autoridades de Registro (en adelante AR) de SIA, tal y como viene estipulado en la DPC, apartados 1.3.2 y 9.6.2.

Cada entidad que actúe como AR establecerá:

- Qué criterios se deben cumplir para solicitar un certificado, sin entrar en contradicción con lo estipulado en la DPC y la presente PC.
- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del suscriptor, cumpliendo con lo estipulado en la DPC.
- Los dispositivos de creación de firma a utilizar, que previamente SIA haya homologado.

1.3.3 Suscriptor

En este caso es la persona jurídica identificada en el certificado, ya sean corporaciones, entidades privadas, públicas o de derecho público, representadas por una persona física. Los datos de la entidad que representa serán incluidos en el certificado.

El suscriptor del certificado de autenticación web 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
- Proveedor de servicios de iniciación de pagos

- Proveedor de información sobre cuentas
- Emisor de instrumentos de pago basados en tarjetas.

1.3.4 Solicitante

El solicitante de certificados definidos en esta política es la persona jurídica que solicita el certificado. Son los propios usuarios con poderes de representación de la propia entidad (bien sean corporaciones, empresas, entidades privadas o públicas).

En el caso de certificados de Sede Electrónica, podrán solicitarlos los administradores, representantes legales y voluntarios de las Corporaciones Públicas, con poder bastante a estos efectos.

Una vez que el certificado se ha emitido, pasa a denominarse suscriptor.

Siguiendo lo estipulado en la versión vigente del documento "Guidelines For The Issuance And Management Of Extended Validation Certificates", emitido por CA/Browser Forum, se establecen una serie de roles que pueden desempeñar diferentes personas relacionadas con el solicitante de un certificado SSL EV.

- **El solicitante o peticionario autorizado de certificados**
    - La solicitud de un certificado SSL EV debe ser realizada por un peticionario autorizado por el solicitante. Un solicitante puede ser el mismo solicitante (si este es una persona física), un empleado del solicitante, un agente autorizado que está autorizado por el solicitante para representarle, un empleado de una tercera parte (por ejemplo, un ISP o una empresa de hosting de sitios web). Su función es:
        - Completar y enviar las solicitudes de certificados.
- **El aprobador de certificados**
    - La solicitud de un certificado SSL EV debe ser aprobada por un aprobador autorizado por el solicitante o suscriptor. Un aprobador puede ser el mismo solicitante (si este es una persona física), un empleado del solicitante, un agente autorizado por el solicitante para representarle. El aprobador tiene autoridad expresa para representar al suscriptor para:
        - Actuar como un solicitante, completando y enviando solicitudes de certificados.
        - Autorizar a otros empleados o a terceras partes para actuar como solicitantes.
        - Aprobar las solicitudes de certificados enviadas por solicitantes.
- **El firmante del contrato de suscriptor**
    - Para solicitar un certificado SSL EV se debe firmar un contrato de suscripción aplicable al Certificado EV solicitado, por un firmante autorizado para ello. Un firmante de contrato es una persona física que puede ser el mismo solicitante, un empleado del solicitante o un agente autorizado por el solicitante para representarlo, que dispone de la autoridad para firmar el contrato de suscriptor en representación del solicitante. El firmante cumple la siguiente función:
        - Firmar el contrato de suscripción.
- **El representante del solicitante**
    - En el caso de que la CA y el suscriptor estén afiliados, los términos de uso aplicables a la solicitud de certificados SSL EV deben ser conocidos y aceptados por un representante

del suscriptor autorizado. Un representante del suscriptor es una persona física que puede ser el mismo solicitante, o un agente autorizado por el solicitante para representarle, y tiene la autoridad en nombre del suscriptor para:

- Confirmar el conocimiento y la aceptación de los términos de uso en representación del solicitante.

1.3.5 Terceras Partes Aceptantes

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

1.3.6 Especialista de validación

Es personal especializado de la Autoridad de Registro que junto con el personal adscrito al Departamento Jurídico de SIA AC es el encargado de comprobar la documentación aportada por las Autoridades de Registro. Determinan la suficiencia o deficiencia de esos documentos, comprueban la fiabilidad de la información aportada por el suscriptor, ordenando, si lo consideran, indagaciones complementarias.

El especialista, es responsable de Dictámenes de Emisión como especialista de validación de información especificada en esta política, determinará en cada caso la necesidad de completar la comprobación junto con el Departamento Jurídico de SIA AC, mediante la consulta telemática de los registros directamente o a través de servicios de terceros.

Finalmente, es el encargado de realizar el documento de dictamen de emisión junto con el Oficial de Registro.

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 cualificados emitidos bajo los criterios de esta política están indicados para permitir a sus suscriptores ofrecer una seguridad adicional en sus servicios web con certificados cualificados, tal y como está definido en los artículos 3 y 45 de eIDAS cumpliendo los requisitos establecidos en el anexo IV.

Los certificados de servidor seguro tienen como finalidad establecer comunicaciones de datos en servidores web vía SSL/TLS.

Permiten el cifrado de las comunicaciones entre el usuario y el sitio web, facilitando el intercambio de las claves de cifrado necesarias para el cifrado de la información a través de Internet.

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.

Los certificados de esta política pueden ser utilizados con los siguientes propósitos dependiendo del tipo de certificado:

- Los certificados de autenticación de sitio web permiten autenticar un sitio web y vinculan el sitio web con la persona física o jurídica a quien se ha expedido el certificado.
- Pueden ser utilizados para autenticar la identidad de un servidor o de una Sede Electrónica mediante el protocolo SSL (o TLS) y establecer luego un canal de transmisión seguro entre el servidor o la Sede y el usuario del servicio.
- Utilizados para la identificación de la titularidad del dominio y acreditación de la organización, proporcionando una garantía razonable al usuario de un navegador de Internet de que el sitio web al que accede es titularidad de la organización identificada en el certificado y que la comunicación entre el navegador del cliente y el servidor de páginas es confidencial debido al empleo del protocolo SSL
- Identificación de la titularidad del dominio que alberga el sitio web, proporcionando una garantía razonable al usuario de un navegador de Internet
- Los certificados serán utilizados en el ámbito de las competencias propias de la organización suscriptor del certificado

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 suscriptores en las relaciones que mantengan con terceros que confían, de acuerdo con lo usos autorizados en las extensiones “Key Usage” y “Extended Key Usage” del certificado y en conformidad con las limitaciones que consten en el certificado.

El reglamento eIDAS establece que los Certificados QWAC cumplirán los requisitos establecidos en el anexo IV. La Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de autenticación de sitios web. Se presumirá el cumplimiento de los requisitos establecidos en el anexo IV cuando un certificado cualificado de autenticación de sitios web se ajuste a dichas normas. Estos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48, apartado 2.

Los certificados cualificados dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones EN 319 412-5.

No se permite el uso de este tipo de certificado para la firma electrónica de documentos. SIA dispone de otras políticas de certificado apropiadas para tal fin.

No se permite la utilización distinta de lo establecido en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público para los certificados cualificados de Sede Electrónica.

1.5 Administración de Políticas

1.5.1 Organización responsable

Esta PC es propiedad de SIA.

Nombre	SIA
Dirección correo	psc@sia.es
Dirección postal	Avenida de Bruselas, 35 28108 Alcobendas - Madrid (España)
Teléfono	+34 91 307 79 97

Tabla 3 – Organización responsable

Los suscriptores, los terceros que confían, los proveedores de software de aplicación y otros terceros pueden ponerse en contacto con AC SIA mediante soc@sia.es para denunciar incidentes de seguridad relacionados con los certificados proporcionados por el TSP, un supuesto compromiso de la clave privada, un uso incorrecto de certificados, otros tipos de fraude, compromiso, uso indebido o conducta inapropiada relacionada con los certificados o PKI de SIA AC

1.6 Definiciones y Acrónimos

1.6.1 Definiciones

Las definiciones y acrónimos se definen en la DPC de SIA, excepto que se defina de otra manera en este documento:

Contacto de dominio: el Registrante de nombre de dominio, el contacto técnico o el contrato administrativo (o el equivalente bajo un ccTLD) como se indica en el registro de WHOIS del Nombre de dominio base o en un registro SOA de DNS, o como se obtiene a través del contacto directo con el Nombre de dominio Registrador.

ccTLD: Country Code Top-Level Domain

Nombre de dominio: la etiqueta asignada a un nodo en el sistema de nombres de dominio.

Nombre de dominio completo: un nombre de dominio que incluye las etiquetas de todos los nodos superiores en el sistema de nombres de dominio de Internet

Fuente de información gubernamental Cualificada: Una base de datos mantenida por una entidad gubernamental que cumple con los requisitos de la Sección 11.11.6 de los EV Guidelines.

Espacio de nombres de dominio: el conjunto de todos los posibles nombres de dominio que están subordinados a un solo nodo en el sistema de nombres de dominio.

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 emitidos bajo esta política lo genera el solicitante, una vez se ha personado, ha sido validado por la Autoridad de Registro y ha firmado el documento de conformidad con la emisión del certificado de autenticación de sitio web, en soporte software o en Módulos de Seguridad Hardware (HSM).

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

Previa a la emisión de todo certificado SSL, SIA valida la existencia de un registro CAA para cada nombre DNS de las extensiones CN y subjectAltName del certificado, según especificaciones de la RFC 6844.

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. Se inspeccionarán los documentos para detectar cualquier indicio de alteración o falsificación y verificará la dirección del solicitante utilizando el mismo DNI, NIE o Pasaporte y se seguirá un proceso de 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 de los certificados.

Este proceso presencial puede ser evitado en caso de legitimación de la firma del contrato ante notario o en caso de firma con certificado cualificado en el contrato y solicitud, garantizando así la autenticidad de su identidad y que el Representante del Suscriptor coincide con la persona física que solicita el certificado.

Para los certificados que no sean EV, se verificará la solicitud utilizando métodos confiables de comunicación según los requisitos establecidos en CA/Browser Forum Baseline Requirements.

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 los 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.

En función al tipo de representación del solicitante, se le solicitará según se establezca, la documentación acreditativa a dicha representación. tomando medidas razonables para determinar que una solicitud realizada en nombre de una Organización es legítima y está debidamente autorizada y el representante legal solicitante posee poderes de representación suficientes.

En el formulario de solicitud de un certificado, el suscriptor deberá identificar y autorizar de forma expresa al responsable del certificado y personas autorizadas para su gestión.

SIA AC verificará la autenticidad de la solicitud y documentación aportada siguiendo la definición de CA/Browser Forum Baseline Requirements for the Issuance and Management of publicly-Trusted Certificates y CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates según aplique.

2.2.5 Autenticación de la identidad de una Organización y Dominio

SIA revisará minuciosamente cualquier documento usado en esta sección para detectar alteraciones o falsificaciones de estos.

Se verifica la titularidad o control del nombre de dominio, certificada por un representante legal de la organización, además del nombre de la persona jurídica a la que se expida el certificado y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales.

2.2.5.1 Identidad de la Organización

En caso de que el certificado deba incluir los datos de una organización, SIA AC verificará la identidad y la dirección de la organización y que la dirección, es la dirección de existencia u operación del solicitante, de acuerdo con la sección 3.2.2.1 de CA/Forum Browser Baseline Requirements.

La existencia de la entidad y dirección se comprueba mediante la documentación aportada y el cotejo con los registros públicos o base de datos de terceros que se actualice periódicamente y se considere una fuente de datos fiable.

- Cuando el Suscriptor es una **entidad privada,** se verificará su existencia, dirección e identidad, que está legalmente reconocida, activa en ese momento e inscrita formalmente, mediante consulta al Registro Mercantil y Agencia de protección de datos o Certificado o documento por Registro Mercantil o equivalente, LEI o Cámara de Comercio.
- En el caso de **entidades públicas**, dicha verificación se realizará mediante consulta al Boletín Oficial correspondiente, Agencia de protección de datos, original o copia auténtica de un certificado relativo a los datos de constitución y personalidad jurídica de las mismas. Para aquellas entidades creadas por norma, aportarán referencia a la norma de creación.
- Si la naturaleza del Suscriptor fuera **distinta de los dos casos anteriores**, las verificaciones relativas a la existencia legal, dirección y la identidad se realizará mediante consulta directa al registro oficial correspondiente y Agencia de protección de datos o certificado del registro oficial correspondiente.

Para los EV la información incluida en los certificados relativa a la organización es conforme al aparto 11 de "Guidelines For The Issuance And Management Of Extended Validation Certificates" de CAB/Forum.

Para los EV, se comprueba fehacientemente la actividad operativa de la entidad, así como a qué categoría de entidad pertenece según la clasificación fijada en las políticas marcadas por CA/Browser Forum en "Guidelines For The Issuance And Management Of Extended Validation Certificates".

- Private Organization,
- Government Entity,
- Business Entity
- Non-Commercial Entity.

Esta comprobación se realizará mediante el análisis del régimen jurídico aplicable a cada entidad y mediante consulta a los registros de actividad empresarial del mercado o mediante la entrega física de las escrituras notariales.

Además, se verifica:

- Que los datos o documentos aportados no tengan una antigüedad superior a 1 año.
- Que la antigüedad de existencia legal de la organización es de 3 años mínimo o se encuentra registrada en los registros oficiales.
- Que no se trata de empresas erradicadas en países donde exista una prohibición gubernamental para hacer negocios o formen parte de alguna lista negra de entidades gestionada por el prestador.

Se verifica el Número de Identificación Fiscal de la identidad a través de las siguientes fuentes:

- Entidad pública: Agencias de Protección de Datos, Boletín Oficial o registro oficial correspondiente.

- Entidad privada: Agencias de Protección de Datos, certificación registral original o nota simple informativa.
- Empresa: Agencias de Protección de Datos, o Registro Mercantil
- Entidad internacional no comercial / sin ánimo de lucro: Comprobación de que la entidad es una Organización Internacional reconocida

En Administraciones públicas: No se exige la documentación acreditativa de la existencia de la administración pública, organismo o entidad de derecho público, dado que dicha identidad forma parte del ámbito corporativo de la Administración General del Estado o de otras AAPP del Estado.

2.2.5.2 Nombre comercial (DBA)

Si la información de la identidad incluye un nombre comercial o marca registrada, se utilizará los mismos procedimientos y criterios de verificación anteriores para verificar el derecho del Solicitante a usar el nombre comercial o marca registrada.

2.2.5.3 Validación de Autorización y Control de Dominio

SIA confirma que, de manera previa a la emisión de cualquier tipo de certificado de servidor seguro, se ha validado el control sobre el dominio y SAN por parte del suscriptor en base al nombre de dominio completo (FQDN) que figura en el Certificado utilizando alguno de los métodos enumerados en la sección 3.2.2.4 de los Baseline Requirements CA/Browser Forum y enumerados a continuación.

Se confirma que el representante del suscriptor posee control sobre los FQDN y que la solicitud proviene del contacto que tiene el control sobre dicho dominio o tiene autorización por parte de este para representarle.

SIA mantendrá un registro de qué método de validación de dominio, fecha en la que se realiza, evidencia de la verificación y el número de versión de BR que se aplica en el momento de validar cada dominio.

Los métodos utilizados se detallan a continuación:

1) **BRG 3.2.2.4.4**. Email construido al contacto del dominio: SIA envía un correo electrónico a una o más de las siguientes direcciones “admin”, “administrator”, “webmaster”, “hostmaster” o “postmaster”, seguido por el símbolo “@” y el nombre de dominio para el cual se solicita el certificado SSL. El correo electrónico enviado incluye un código aleatorio y único. Cualquier persona de la organización solicitante puede responder el correo electrónico indicando el código aleatorio. Este código tiene un periodo de validez de 30 días desde su creación.
2) **BRG 3.2.2.4.7**. Cambio acordado en DNS: El solicitante realiza un cambio en el registro DNS del dominio para el que peticiona el certificado SSL. El solicitante debe añadir el código aleatorio y único enviado por SIA en un campo CNAME, TXT o CAA, en su registro DNS. Una vez realizado el cambio por parte del solicitante, SIA lo verifica.
3) **BRG 3.2.2.4.13**. Email a contacto DNS CAA: SIA envía al solicitante un código único y aleatorio por correo electrónico a la dirección que aparece en el registro DNS CAA.

Cualquier persona de la organización solicitante puede contestar, indicando el código aleatorio.

4) **BRG 3.2.2.4.14.** Email a contacto DNS TXT: SIA envía al solicitante un código único y aleatorio por correo electrónico a la dirección que aparece en el registro DNS TXT. Cualquier persona de la organización solicitante puede contestar, indicando el código aleatorio.

Se comprobará con registros púbicos para verificar que no es un dominio de alto riesgo.

2.2.5.3.1 Validación de Dominio wildcard

En el caso de certificados SSL DV y SSL OV se permitirían los wildcard en subdominios o nombres de host, siempre que la entidad solicitante pueda demostrar su legítimo control del dominio completo según el punto 2.2.5.3,. En caso contrario se rechazará la solicitud.

Si un *Certificado* wildcard cayera dentro de la etiqueta inmediatamente a la izquierda de un sufijo público, SIA rechazará la emisión de dicho *Certificado* a menos que el *Solicitante* demuestre el control legítimo de todo el espacio de nombres del dominio.

SIA no emitirá certificados a dominios privados o IP.

Actualmente, SIA no emite certificados OV ni DV.

Los Certificados cualificados de autenticación de sito Web (QWAC) y PSD2 y los Certificados Cualificados de Sede Electrónica no pueden ser wildcard, sin embargo, todos podrá ser multidominio, protegiendo con el certificado varios nombres de host a través de múltiples dominios.

2.2.5.4 Verificación de País

Si se incluye el campo subject:countryName, SIA AC verificará el país asociado con el Sujeto mediante el método identificado en la Sección 3.2.2.1 de CA/Browser Forum Baseline Requirements y punto 2.2.5.1 de esta política con la documentación aportada, alternativamente, mediante el ccTLD del Nombre de dominio solicitado.

Para los certificados EV, se verifica el país de jurisdicción de la organización según el punto EVG 9.2.4.

2.2.5.5 Registro CAA

Cuando la solicitud sea para un certificado que incluya un nombre de dominio para la autenticación de un servidor, SIA examinará el registro de la CAs autorizadas, CAA para cada nombre DNS de las extensiones CN y subjectAltname del certificado, según la RFC 6844, y si esos registros CAA están presentes y no permiten a SIA emitir esos certificados porque no se encuentra registrado, SIA no emitirá ese certificado pero permitirá a los solicitantes volver a realizar la solicitud una vez haya podido subsanar esa posible incidencia. SIA procesa los tags “issue” e “issuewild”. El registro CAA que identifica a dominios para los que se autoriza la emisión por parte de SIA es “sia.es”.

2.2.6 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, además:

- 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 estos 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.

2.2.6.1 Autenticación para una dirección IP

Bajo la presente *política,* no se emiten certificados para identificar direcciones IP.

2.3 Identificación y autenticación para peticiones de renovación de claves

En el supuesto de renovación de la clave, SIA informará previamente al suscriptor 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 suscriptor, es como si de una nueva emisión de certificados se tratase.

SIA AC corrobora la existencia y la validez del certificado al cual se pretende realizar la renovación de claves, y que la información utilizada para verificar la identidad y atributos del sujeto siguen siendo válidos, teniendo en cuenta que las comprobaciones son válidas durante 398 días.

La vigencia de la entidad y competencia de solicitud no será requerida en caso de certificado vigente de firma o sello emitido por SIA al solicitante, siempre que el certificado haya sido emitido en los últimos 398 días.

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.

En el caso de los Certificados QWAC, SIA AC solo emitirá este tipo de certificados a los Solicitantes que cumplan con los requisitos de Organización Privada, Entidad Gubernamental, Entidad de negocios y Entidad No Comercial especificados en el apartado 8.5 de los EV Guidelines de CA/B Forum.

Previa solicitud y emisión del certificado, deberá firmarse el contrato de suscripción debidamente cumplimentado, debiendo el suscriptor personarse por medio de su representante legal ante una Autoridad de Registro Reconocida aportando además la documentación que acredite su representación, en cuya presencia se procederá a firmar el contrato de suscripción y aceptación de los términos y condiciones. Esta firma podrá realizarse electrónicamente mediante un certificado cualificado de firma electrónica. Con este hecho, acepta los requisitos establecidos en la DPC y en esta PC.

El solicitante deberá cumplimentar el formulario de solicitud del certificado asumiendo la responsabilidad de la veracidad de la información reseñada, en el que se indique el cargo del solicitante(s) y aprobador(es) si son requeridos y firmar presencialmente en la personación ante una Autoridad de Registro Reconocida, ante notario o electrónicamente con certificado cualificado, aceptando así los requisitos establecidos en la DPC y en esta PC.

Cuando la solicitud no es presencial sino electrónica, La AR, verifica que el *Solicitante* tiene suficiente capacidad de representación mediante la firma electrónica del formulario de solicitud, con *Certificado* cualificado de representante de la persona jurídica suscriptora, para cuya expedición ha sido acreditada la capacidad de representación.

Cuando el citado formulario se firma mediante un *Certificado* cualificado diferente al anterior, la AR comprueba la facultad de representación del firmante de la solicitud mediante la documentación certificada aportada o consulta a registros oficiales (Registro Mercantil, Boletines Oficiales, etc. en función de la naturaleza de la representación). Si del resultado de estas consultas no se obtuvieran evidencias de representación suficiente, la AR se pondrá en contacto con el *Suscriptor* para recabar dichas evidencias.

Podrá prescindirse de dicha firma cuando el representante legal de la entidad delegue la capacidad de realizar solicitudes de certificados SSL/TLS.

Dicha delegación se realiza mediante una carta de autorización que autoriza a una o varias personas a desempeñar las funciones descritas en el rol de solicitante o autorizado y aprobador de certificados. En ese caso, deberá estar firmada por las personas autorizadas que, a partir de ese momento, podrán solicitar/aprobar certificados y ser firmada por el representante legal:

- Electrónicamente, con certificado cualificado o con el certificado de Persona física Representante de persona Jurídica emitido por SIA a la firma del contrato de suscripción.

- Presencialmente en el momento de personación ante la Autoridad de Registro, donde también se procederá a verificar y firmar el documento de conformidad con la emisión del certificado, aportando además la documentación que acredite su representación.

Para los certificados cualificados de Sede Electrónica, la solicitud del certificado la deberá realizar un representante del Titular de la Sede Electrónica debidamente acreditado y autorizado para ello.

Excepto en el caso de solicitudes de certificados SSL-DV, cuando SIA los emita, aquellas entidades no públicas cuya información de constitución no esté disponible para su consulta en el Registro Mercantil se deberá aportar:

- Copia de la publicación en el registro correspondiente
- Copia del CIF

Adicionalmente, para la solicitud de certificados cualificados de autenticación de sitio web para 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.

El formulario de solicitud, para la solicitud de certificados EV, debe ser enviado desde el correo electrónico de uno de los aprobadores de certificados o mediante acceso a la solicitud de certificados que pruebe el control de correo electrónico. El hecho de solicitar la emisión de Certificados de Autenticación de sitios Web supone también el hecho de aprobar la emisión del certificado, por parte de un aprobador indicado en el punto 1.3.4.

La solicitud de certificados DV y OV podría ser tramitada de manera electrónica.

SIA utilizará los métodos confiables de comunicación según los requisitos establecidos en CA/Browser Forum Baseline Requirements

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 y dominio para los que se solicita el certificado es válida, por los medios de los que dispone el TSP.

SIA comprobará el registro CAA según se define en el punto 2.2.5.5. Registro CAA.

Dependiendo del tipo de certificado solicitado, se requerirá realizar validaciones adicionales. Las validaciones necesarias para la emisión de certificados cualificados de sitio web requiere de validaciones que también aplican a otro tipo de certificados SSL como son DV y OV.

Para los Certificados de Servidor Seguro SSL Domain Validation (DV), se requerirían las verificaciones indicadas en el punto 2.2.5.3 y 2.2.5.4 de esta Política de certificación:

- 2.2.5.3. Validación de Autorización y control de dominio
- 2.2.5.4 Verificación de País

Para los Certificados de Servidor Seguro SSL Organization Validation (OV), se requerirían las verificaciones indicadas para Certificados de Servidor Seguro SSL Domain Validation (DV), y adicionalmente los puntos 2.2.5.1 y 2.2.5.2 aplicables a OV:

- Identidad de la Organización
- Nombre Comercial (DBA)
- Competencia del solicitante para solicitar el certificado mediante el cotejo de la documentación aportada con los registros públicos o bases de datos de confiables.
- Verificar que un Firmante del Contrato haya firmado el Acuerdo de Suscriptor o que un Representante solicitante debidamente autorizado haya reconocido y aceptado los Términos de Uso
- Verificación de lista de denegados:
    - Se verifica que el suscriptor no está registrado en la lista negra de individuos y entidades o está operando en un lugar donde las políticas de CA prohíben la emisión de certificados. SIA AC actualiza regularmente sus registros con todas las personas que aparecen en la búsqueda e incautación, y enlaza esta lista negra con el control de solicitud de certificado.

Para los certificados cualificados de Autenticación de Sito Web, certificados cualificados de Autenticación de Sito Web para PSD2 y certificados cualificados de Sede Electrónica nivel medio y alto, se verificará adicionalmente a las verificaciones descritas para certificados OV, lo siguiente aplicable a EV:

- 2.2.5.1 Identidad de la Organización
- 2.2.5.2. Nombre Comercial (DBA)
- Comprobación del nombre, cargo y capacidad de la persona que autoriza la Solicitud, del Solicitante del certificado y del firmante de la Solicitud y que están autorizados para gestionar los certificados de la organización.
- Verificar que el Firmante del Contrato haya firmado el Acuerdo de Suscriptor o que un Representante solicitante debidamente autorizado haya reconocido y aceptado los Términos de Uso.
- Verificar que un aprobador de certificado ha firmado o aprobado de otro modo la solicitud de certificado EV.
- SIA AC realiza una comprobación dual, interviniendo el Área Técnica, El Oficial de Registro, Responsable del dictamen de emisión y Asesoría Jurídica.

En caso de los certificados cualificados de Autenticación de sitio Web 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.

SIA AC mantiene procedimientos documentados que identifican y requieren verificaciones adicionales para las Solicitudes de Certificados de Alto Riesgo antes de la validación del certificado, según sea razonablemente necesario para garantizar que dichas solicitudes se verifiquen correctamente.

Una vez completa la solicitud, SIA dejará constancia de las comprobaciones en el documento de comprobación de la documentación y recopilará las evidencias correspondientes a las comprobaciones realizadas que quedarán almacenadas en el repositorio designado.

El proceso de emisión del certificado no se iniciará en tanto en cuanto el Oficial de Registro Especialista de Validación Responsable del Dictámenes de Emisión no haya emitido el correspondiente informe de conformidad con 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 la vinculación con la entidad y dominio para los que se solicita el certificado. El plazo máximo establecido para la emisión del informe será de 15 días.

El RDE puede requerir del suscriptor información o documentación complementaria y el suscriptor dispondrá de 15 días para hacer entrega de esta. Transcurrido este plazo sin que se haya cumplimentado este requerimiento, el RDE emitirá informe denegando la emisión.

En caso de que el RDE compruebe que la información facilitada por el suscriptor no es veraz, denegará la emisión del certificado, generará un incidente informando al Coordinador de Seguridad, a fin de determinar la inclusión o no del suscriptor en la lista negra de personas y entidades.

La Autoridad de Registro, remitirá la solicitud al Prestador de Servicios de confianza para su tramitación.

3.3 Emisión de certificados

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

Las claves para los certificados de esta política se generan en soporte software o en Módulos de Seguridad Hardware (HSM).

Deben ser claves RSA con una longitud mínima de 2.048 bits

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, el requerimiento de autorización para certificados EV que requieren autorización dual, indicado en el punto 3.1, así como la información verificada en el punto 3.2.
2. El solicitante enviará por correo un CSR, que previamente habrá generado en su sistema.
3. SIA realizará la validación técnica de la petición PKCS#10 y la validación de los datos que contenga.

4. Previa a la emisión de todo certificado SSL, SIA valida la existencia de un registro CAA para cada nombre DNS de las extensiones CN y subjectAltName del certificado, según especificaciones de la RFC 6844.
    1. En el caso de que se emita el certificado, la validación se realizará antes del TTL del registro CAA, y en cualquier caso no superior a 8 horas.
    2. SIA procesa los tags "issue" e "issuewild".
    3. Los registros CAA que identifican a dominios para los que se autoriza la emisión por parte de SIA son "sia.es".
5. La AC emitirá el certificado x.509 de la clave pública asociado a su clave privada, y se le entrega al solicitante vía email a la dirección de correo electrónico consignada en el formulario de solicitud

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

3.4 Aceptación del certificado

3.4.1 Forma en la que se acepta el certificado

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

Como evidencia de la aceptación deberá quedar una hoja de aceptación firmada por el suscriptor. 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 se publican en los repositorios al efecto.

La Autoridad Nacional Competente, puede solicitar información sobre los certificados que contienen un número de autorización de un Proveedor de Servicios de Pago (PSP) asignado por esa institución. SIA AC informará sobre los certificados emitidos de acuerdo con lo establecido en cada repositorio.

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

En caso de certificados de PSD2, si la CA de SIA ha sido notificada sobre la dirección de correo electrónico de la Autoridad Nacional Competente identificada en el certificado de nueva emisión, SIA remitirá a dicha dirección de correo electrónico la información relativa al certificado emitido de acuerdo con lo establecido en la normativa de referencia, así como la información de contacto y las instrucciones para las solicitudes de revocación.

Los certificados de Servidor Seguro (SSL) EV, serán publicados en el servicio Certificate Transparency Log Server (CT), según política de Google. El resto de certificados no se notifican a ninguna entidad.

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 suscriptor 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 suscriptor dejará de usar la clave privada.

Los certificados cualificados de Autenticación de sito Web PSD2 – Nivel medio regulados en esta PC, se emiten a Proveedores de Servicios de Pago debidamente acreditados ante la Autoridad Nacional Competente, cumpliendo los requisitos establecidos en el 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 y el Real Decreto-ley 19/2018 de España, respetando las directrices establecidas por la Autoridad Nacional Competente 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 los 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 de esta política 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 estas.
- Cambio de formato.

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

No será emitido un certificado con un nombre de dominio que haya sido emitido previamente en nombre de otra organización, debiendo constar evidencia de la propiedad legítima del nombre" del suscriptor para el cambio.

3.7.2 Quien puede pedir la renovación de un certificado

La renovación del certificado cualificado, la debe de solicitar el suscriptor o responsable del certificado con suficientes poderes de representación, así como los autorizados al efecto.

3.7.3 Tramitación de las peticiones de renovación con cambio de claves

La AC informará al suscriptor de que su certificado está próximo a expirar.

Para renovar un certificado, el solicitante deberá seguir el proceso de emisión de certificados establecido, teniendo en cuenta que las comprobaciones son válidas durante 398 días. SIA corrobora la existencia y la validez del certificado al cual se pretende realizar la renovación de claves, y que la información utilizada para verificar la identidad y atributos del sujeto siguen 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 suscriptor del certificado y que éste está de acuerdo con las mismas.

Antes de la renovación de los certificados cualificados de Autenticación Web 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 proceso de emisión de certificados como si del proceso inicial se tratara, el sistema informará al titular de que se ha procedido a la renovación telemática de su certificado y le informará del nuevo periodo de

validez de este, informando también de que el anterior certificado ha sido revocado y que el certificado quedará sin efecto.

3.7.5 Forma de aceptación del certificado con nuevas claves

El suscriptor confirma y acepta las condiciones de uso y expresa su voluntad de obtener el *Certificado* en el proceso de solicitud.

3.7.6 Publicación del certificado con las nuevas claves por la AC

Los certificados de este perfil se publicarán en los repositorios al efecto.

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

No se efectúan notificaciones a terceros.

Sólo en caso de emisión de certificados de PSD2, si SIA ha sido notificado sobre la dirección de correo electrónico de la ANC identificada en el certificado de nueva emisión, SIA remitirá a dicha dirección de correo electrónico la información relativa al certificado emitido de acuerdo con lo establecido en la normativa de referencia, así como la información de contacto y las instrucciones para las solicitudes de revocación y una copia del archivo del certificado.

En el ámbito del proyecto Google Certificate Transparency (CT), los certificados emitidos con la calificación EV (Extended Validation) se publicarán en diferentes operadores de CT Log, para cumplir con la propuesta RFC 6962 Certificate Transparency.

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 los 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 de este, 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, SIA AC, deberá revocar un certificado en un período de 24 horas si se da una más de las siguientes circunstancias:

1. El Suscriptor solicita por escrito que SIA AC revoque el Certificado;
2. El Suscriptor notifica a SIA AC que la solicitud de certificado original no fue autorizada y no otorga retroactivamente la autorización
3. SIA AC obtiene evidencia de que la Clave Privada del Suscriptor correspondiente a la Clave Pública en el Certificado sufrió un Compromiso de la Clave;
4. SIA AC obtiene evidencia de que no se debe confiar en la validación de la autorización o el control del dominio para cualquier Nombre de Dominio (FQDN) o Dirección IP en el Certificado.

SIA AC deberá revocar un certificado en un período de 5 días si se da una o más de las siguientes circunstancias:

1. El Certificado ya no cumple con los requisitos de los apartados 6.1.5 y 6.1.6 de los CA/B Forum Baseline Requirements;
2. SIA AC obtiene evidencia de que el certificado fue utilizado de forma incorrecta;
3. SIA AC tiene conocimiento de que un Suscriptor ha violado una o más de sus obligaciones importantes en virtud del Contrato de Suscripción o los Términos y Condiciones;
4. SIA AC tiene conocimiento de cualquier circunstancia que indique que el uso de un Nombre de dominio (FQDN) o una Dirección IP en el Certificado ya no está legalmente permitido.
5. SIA AC tiene conocimiento de que se ha utilizado un certificado Wildcard para autenticar un nombre de dominio engañoso o fraudulento;
6. SIA AC tiene conocimiento de un cambio importante en la información contenida en el Certificado;
7. SIA AC tiene conocimiento de que el Certificado no se emitió de acuerdo con los Baseline Requirements de CA/B Forum, esta PC o la DPC de SIA AC;
8. SIA AC determina o se le informa que cualquiera de la información que aparece en el Certificado es inexacta;
9. El derecho de SIA AC a emitir Certificados conforme a los Baseline Requirements de CA/B Forum expira o se revoca o finaliza, a menos que SIA AC haya hecho arreglos para continuar manteniendo el Repositorio de CRL / OCSP;
10. La revocación es requerida por la PC de SIA AC y / o la DPC;
11. SIA AC tiene conocimiento de un método demostrado o comprobado que compromete la Clave privada del suscriptor, se han desarrollado métodos que pueden calcularlo

fácilmente según la Clave pública (como una clave débil de Debian, consulte http://wiki.debian.org/SSLkeys), o si existe evidencia clara de que el método específico utilizado para generar la clave privada fue defectuoso.

Además, en el caso de certificados de CAs subordinadas, éstas se revocarán en un plazo máximo de 7 días por las siguientes causas:

1. La CA intermedia lo solicita por escrito.
2. La CA intermedia notifica a la CA emisora que la petición de certificado original no fue autorizada y no admite una autorización retroactiva.
3. La CA emisora obtiene una evidencia de que la clave privada de la CA intermedia correspondiente a la clave pública del certificado ha sufrido un compromiso de clave o ha dejado de cumplir con los requisitos de los apartados 6.1.5 y 6.1.6 de los BR.
4. La CA emisora obtiene una evidencia de que el certificado fue emitido de forma incorrecta.
5. La CA emisora detecta que el certificado no fue emitido de acuerdo con la Política del Certificado o la DPC.
6. La CA emisora determina que algún dato que aparece en el certificado es impreciso o incorrecto.
7. La CA emisora o la CA intermedia cesa sus operaciones por cualquier razón y no se ha habilitado los acuerdos con otra CA para proporcionar el servicio de revocación.
8. Finaliza o se revoca el derecho de la AC para emitir certificados bajo esta política, a menos que la CA emisora haya habilitado los acuerdos para continuar manteniendo el repositorio de CRL/OCSP.
9. Se requiere la revocación por parte de la política de la CA emisora y/o por la DPC.

Además, en el caso de los certificados regulados en esta documentación específica SIA,

1. Presentará al suscriptor, a terceras partes y a los navegadores de Internet, instrucciones claras para la presentación de denuncias o sospechas de compromiso de la clave privada, de mal uso de certificados o de otros tipos de fraude, compromiso, mal uso, o conducta impropia en relación con los certificados.
2. Investigará los informes de problemas dentro de las veinticuatro horas siguientes a su recepción y decidirá sobre la revocación, atendiendo a los siguientes criterios:

   a)La naturaleza del supuesto problema;

   b) El número de informes recibidos de problemas de un certificado o página web.

   c)Consecuencias de revocación.

   d) La identidad de los denunciantes.

   e) La legislación vigente.

3.9.2 Quien puede solicitar la revocación

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

- La propia AC de SIA cuando tenga conocimiento de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de la DPC.
- La Entidad de Registro que intervino en la emisión.
- 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.
    - Se entiende que están autorizados para solicitar la revocación del certificado: el Representante Legal de la entidad suscriptora o tercero autorizado por este.
- El solicitante
- En el caso de los Certificados cualificados de Autenticación de sito Web para PSD2, la solicitud de revocación puede ser realizada por el Banco de España o la Autoridad Nacional Competente (ANC).
- Los proveedores de software de aplicación con los que el prestador mantenga acuerdos.

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 definido en esta política, con una validez de 24 horas.

La CRL de los certificados de las CAs (ARLs) se emite cada 12 meses o cuando se produzca una revocación.

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”.
- El certificado de firma de la respuesta OCSP de la AC Sub SSL está emitido por la CA que emite el certificado que se quiere validar.
- La información proporcionada a través del servicio OCSP se actualiza al menos cada cuatro días. siendo la validez de la respuesta, de 10 días.

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

Según lo dispuesto en la DPC y apartados anteriores.

Además, cuando la solicitud de revocación es debida a un supuesto compromiso de clave, la comunicación de compromiso de clave se indicará dirigiéndose al correo electrónico "soc@sia.es" indicado en el apartado 1.5.1. Deberá incluir en todo caso una prueba de dicho compromiso e indicar en el asunto del correo electrónico: "Compromiso de claves".

Terceras partes pueden utilizar los siguientes métodos para demostrar un posible compromiso de claves:

- Enviar un CSR firmado, la clave privada que ha sido comprometida u otra respuesta de desafío firmada por dicha Clave privada y verificable por la clave pública.
- Proporcionar referencias a vulnerabilidades y / o fuentes de incidentes de seguridad a partir de las cuales el compromiso de la clave sea verificable.

SIA analizará otros posibles métodos o solicitudes y podrá aceptar otro tipo de evidencias que demuestren adecuadamente el compromiso de claves.

3.9.7 Circunstancias para la suspensión

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

3.10 Servicios de información del estado de certificados

3.10.1 Características operativas

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

3.10.2 Disponibilidad del servicio

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

3.11 Finalización de la suscripción

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

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

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

3.12 Custodia y recuperación de claves

3.12.1 Prácticas y políticas de custodia y recuperación de claves

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

4. CONTROLES DE SEGURIDAD TÉCNICA

Los controles de seguridad técnica para los componentes internos de SIA, y concretamente para las AC raíz y AC subordinadas 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 los sistemas del solicitante utilizando sus propias aplicaciones compatibles con los estándares de PKI.

Deben ser claves RSA con una longitud mínima de 2.048 bits

4.1.2 Entrega de la clave privada al titular

Las claves de los certificados de entidad final que tienen una extensión EKU que contiene KeyPurposeIds id-kp-serverAuth las genera el suscriptor, por tanto, no se hace entrega de clave privada, ésta se encuentra en posesión del titular bajo su exclusivo control.

4.1.3 Entrega de la clave pública al emisor del certificado

La clave pública para certificar es generada junto a la clave privada sobre el dispositivo de generación de claves y es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10.

4.1.4 Tamaño de las claves

El tamaño de las claves de los certificados de autenticación de sitio web es de 2048, 3072 o 4096 bits.

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

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

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

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

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

Key Usage:

- Digital Signature
- Key Encipherment

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

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

4.2.1 Estándares para los módulos criptográficos

El módulo criptográfico empleado en la emisión de los certificados adscritos a esta Política de Certificación es un dispositivo software. Si el firmante utiliza un navegador Internet Explorer o Chrome en un entorno Microsoft Windows, el equipo utilizará CSP (Cryptographic Service Provider). En Unix/Linux y navegadores Mozilla Firefox, se emplea PKCS#11. También cabe la posibilidad de que la entidad suscrita emplee el uso de Módulos de Seguridad Hardware (HSM), en ese caso el dispositivo tendrá como mínimo una certificación FIPS 140-2 nivel 3.

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 suscriptores. No está estipulado que exista control multi-persona para las claves privadas asociadas a los certificados de esta política.

4.2.3 Custodia de la clave privada

Se pueden dar dos casos de custodia de claves:

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

4.2.4 Copia de seguridad de la clave privada

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

4.2.5 Archivo de la clave privada

Las claves privadas de los certificados emitidos bajo el ámbito de la presente Política de Certificación nunca serán archivadas por la AC.

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

La generación de las claves vinculadas a los certificados de servidor seguro SSL se realizará en el propio dispositivo software del sistema. Se puede utilizar un fichero en formato PKCS#12 para transferir la clave privada a otro sistema, pero la responsabilidad de proteger este fichero y esta operación es del propio usuario.

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

4.2.7 Almacenamiento de la clave privada en un módulo criptográfico

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

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

4.2.8 Método de activación de la clave privada

La activación de la clave privada asociada a los certificados de esta PC requiere la utilización de los programas o sistemas informáticos que sirvan para aplicar los datos de creación de firma. SIA no controla ni define el control de acceso lógico a la clave privada de estos dispositivos de creación de firma, pero recomienda el uso de un dato de activación o contraseña para la utilización de la clave privada.

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

Los dispositivos de usuario final están bajo su custodia, y éste será el responsable de mantenerla bajo su exclusivo control.

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.

En dispositivos de usuario final depende del dispositivo en el que esté generada, pero como regla general es responsabilidad del suscriptor 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 suscriptor 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 validez de 13 meses, inferior a 398 días. El par de claves utilizado para la emisión de los certificados se crea para cada emisión y por tanto también tiene una validez de 13 meses.

La caducidad deja automáticamente sin validez a los certificados emitidos bajo esta política, originando el cese permanente de su operatividad conforme a los usos que le son propios e inhabilita el uso legítimo por parte del suscriptor.

4.4 Datos de activación

4.4.1 Generación e instalación de los datos de activación

Los datos de activación de la clave privada consisten en la creación de la contraseña que custodiará las claves y la generación de las mismas cuando estas sean generadas en un soporte Software. En el caso en que se emplee un HSM, el proceso de activación de la clave privada constara de un mayor nivel de complejidad.

4.4.2 Protección de los datos de activación

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

5. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

5.1 Perfil de certificado

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

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- RFC 5280 “Internet X.509 Public Key Infrastructure. Certificate and CRL Profile”.
- RFC 3739 “Internet x509 Public Key Infrastructure. Qualified Certificates Profile”.
- Perfiles de Certificados derivados 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 EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- ETSI TS 119 495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- *CA/Browser Forum* Guidelines For The Issuance And Management Of Extended Validation Certificates (*EVBR)*
- *CA/Browser Forum* Baseline Requirements for the Issuance and Management of publicly-Trusted Certificates (BR), publicados en http://www.cabforum.org por el CA/Browser Forum.

5.1.1 Número de versión

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

5.1.2 Extensiones del certificado

Los certificados cualificados emitidos por SIA, 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 de los certificados cualificados incluidos en los certificados son al menos:

- 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.
- SignedCertificateTimestampList (SCT)
- Subject Alternative Name.
- cabfOrganizationIdentifier

cabfOrganizationIdentifier (OID: 2.23.140.3.1) debe ser incluida a partir del 31 de enero de 2020 cuando se encuentra presente el campo organizationIdentifier.

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

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

- QcCompliance, establece la calificación con la que se ha realizado la emisión del “Certificado cualificado”.
- QcEuRetentionPeriod, determina el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este. En el caso de SIA, es de quince (15) años.
- QcType, indicativo del tipo de certificado, firma, sello o web.
- QcSyntax-V2, habilitado indicando el OID. 0.4.0.194121.1.2.

- QcPDS, indica URL de la PDS, un resumen de la DPC en 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. No se incluirán en estos certificados

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.

La información sobre el sujeto de los certificados de suscriptor sigue los requisitos especificados en el apartado 7.1.4.2 de los Baseline Requirements.

Los Certificados EV incluirán la información sobre la organización del Sujeto en los campos enumerados en el apartado 9.2 de los EV Guidelines.

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, estará compuesto de los siguientes elementos:

- CN, OI, SN, O, L, ST y C

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

- CN = Dominio DNS. FQDN. Debe ser uno de los indicados en la extensión subjectAltname
- OI = NIF de la entidad en formato VATES – NIF entidad, según norma ETSI EN 319 412-1. Excepto DV
- SN = CIF de la entidad
- O = Nombre de la organización. Excepto DV
- L= Localidad de la organización
- ST = Provincia de la organización
- 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.

Los perfiles de los diferentes certificados siguen las indicaciones del punto 9 de CA/Browser Forum EV guidelines y punto 7 de CA/Browser Forum Baseline.

Los certificados DV (2.23.140.1.2.1) no incluirían información sobre la organización (organizationName, givenName, surname, streetAddress, localityName, stateOrProvinceName, o postalCode) en el campo Subject de los certificados.

Tanto los certificados 2.23.140.1.2.2(OV) como los certificados 2.23.140.1.1(EV), contienen los siguientes atributos en el campo Subject del certificado:

- **organizationName**: Nombre de la organización verificada bajo la sección 3.2.2.2 de CA/Browser Forum Baseline. Acepta variaciones o abreviaturas
- **localityName** (OID: 2.5.4.7) : Localidad de registro de la organización. Definido en la sección 7.1.4.2.2 de BR,
- **stateOrProvinceName**: Provincia de registro de la organización Definido en la sección 7.1.4.2.2 de BR,
- **countryName**: Pais

Adicionalmente, los certificados EV contienen además información sobre la información de la organización en la sección **jurisdictionCountryName** y **bussinesCategory**. La categoría de negocio será una de las siguientes:

- 2.5.4.15 = Private Organization

- 2.5.4.15 = Government Entity
- 2.5.4.15 = Business Entity
- 2.5.4.15 = Non-Commercial Entity

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

El OID de la presente PC es 1.3.6.1.4.1.39131.10.1.21.

Los identificadores de los certificados expedidos bajo la presenta Política de Certificación son los establecidos en el punto 1.2

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

Certificados Cualificados de Autenticación de Sitio Web y Sede electrónica	
Certificados Cualificados de Autenticación de Sitio Web y Sede electrónica	1.3.6.1.4.1.39131.10.1.21.1: QWAC, QWAC PSD2, Sede nivel medio y Sede nivel alto

Tabla 4 – OID política de certificación

5.1.7 Uso de la extensión “PolicyConstraints”

No estipulado.

5.1.8 Sintaxis y semántica de los “PolicyQualifier”

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

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

Y el siguiente “Policy Identifier”:

- QEVCP-w: indicación de certificado cualificado de autenticación de sitio web, acorde a eIDAS.
- QCP-w-psd2: indicación de certificado cualificado de autenticación de sitio web para PSD2, acorde a ETSI 119-495
- OID del tipo de certificado, OID: 2.16.724.1.3.5.5.2. Sólo para certificados cualificados de Sede Electrónica para AAPP nivel medio.

- OID del tipo de certificado, OID: 2.16.724.1.3.5.5.1. Sólo para certificados cualificados de Sede Electrónica para AAPP nivel alto.
- Los identificadores de las políticas de certificado especificados en el documento ETSI 319 411-1 son:
    - 0.4.0.2042.1.4 (EVCP)
    - 0.4.0.2042.1.6 (DVCP)
    - 0.4.0.2042.1.7 (OVCP)
- OID de CA/B FORUM
    - 2.23.140.1.2.1 (DV)
    - 2.23.140.1.2.2 (OV)
    - 2.23.140.1.1 (EV)

5.1.9 Tratamiento semántico para la extensión "Certificate Policy"

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

5.2 Perfil SIA ROOT CA 2020

Certificado SIA ROOT CA 2020		
Nombre atributo	Valor	Observaciones
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC SIA Root	CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) containing at least **64 bits** of output from a CSPRNG.
Signature Algorithm	SHA-256 con RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organization Identifier (OI)	VATES- A82733262	identificador de la organización según

2.5.4.97		norma ETSI EN 319 412-1
Common Name (CN)	SIA ROOT CA 2020	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 25 años	
Subject (Asunto)		
Country (C)	ES	País. El atributo "C" (country) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en PrintableString
OrganizationName (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	Verificado 3.2.2.2
Organization Identifier (OI) 2.5.4.97	VATES- A82733262	identificador de la organización según norma ETSI EN 319 412-1
Common Name (CN)	SIA ROOT CA 2020	
Subject Public Key Info	Clave pública (RSA-4096 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública	
Subject Key Identifier	Identificador de la clave pública del la CA root 2	
Basic Constraints	CA:TRUE	Marcado como crítica
KeyUsage		Marcado como crítica
Digital Signature	0 (no seleccionado)	
Content Commitment (nonRepudiation)	0 (no seleccionado)	
Key Encipherment	0 (no seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	0 (no seleccionado)	
Key Certificate Signature	1 (seleccionado)	
CRL Signature	1 (seleccionado)	
EncipherOnly	0 (no seleccionado)	

DecipherOnly	0 (no seleccionado)	

5.3 Perfil SIA SSL SUB01 CA

Certificado SIA SSL SUB01 CA		
Nombre atributo	Valor	Observaciones
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC SIA Root	CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) containing at least **64 bits** of output from a CSPRNG.
Signature Algorithm	SHA-256 con RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organization Identifier (OI) 2.5.4.97	VATES- A82733262	identificador de la organización según norma ETSI EN 319 412-1
Common Name (CN)	SIA ROOT CA 2020	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 15 años	
Subject (Asunto)		
Country (C)	ES	País. El atributo “C” (country) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en PrintableString
OrganizationName (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	

Organization Identifier (OI) 2.5.4.97	VATES- A82733262	identificador de la organización según norma ETSI EN 319 412-1
Common Name (CN)	SIA SSL SUB01 CA	
Subject Public Key Info	Clave pública (RSA-4096 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del la CA subordinada	
Basic Constraints	CA:TRUE	Marcado como crítica
KeyUsage		Marcado como crítica
Digital Signature	0 (no seleccionado)	
Content Commitment (nonRepudiation)	0 (no seleccionado)	
Key Encipherment	0 (no seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	0 (no seleccionado)	
Key Certificate Signature	1 (seleccionado)	
CRL Signature	1 (seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	
Extended Key Usage		
Server Authentication	1 (seleccionado)	.
Client Authentication	1 (seleccionado)	
CRL Distribution Point		
Distribution Point 1	http://psc.sia.es/arl2020.crl	
Authority Info Access		
Access Method 1	Id-ad-ocsp	
Access Location 1	http://psc.sia.es/ocsp 1.3.6.1.5.5.7.48.1	
Access Method 2	id-ad-calssuers *1.3.6.1.5.5.7.48.2*	Opcional

Access Location 2	http://psc.sia.es/ac_raiz_2020.crt	Es el enlace que permite descargar el certificado CA OCSP
Certificate Policies		
Policy Identifier	2.5.29.32.0 (anyPolicy)	Opcional
Policy Qualifier ID	Especificación de la DPC	Opcional
CPS Pointer	http://psc.sia.es/	Opcional

5.4 Perfil de Certificado de Autenticación de Sitio Web (QWAC) y PSD2 – Nivel medio

Certificado Cualificado Autenticación de Sitio Web (QWAC)– Nivel medio *Certificado Cualificado* Autenticación de Sitio Web (QWAC) PSD2- *Nivel medio*		
Nombre atributo	Valor	Observaciones
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada SSL emisora	
Signature Algorithm	SHA-256 con RSA-2048, RSA-3072 o RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Organization Identifier (OI) 2.5.4.97	VATES- A82733262	identificador de la organización según norma ETSI EN 319 412-1
Common Name (CN)	SIA SSL SUB01 CA	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 13 meses	

Subject (Asunto)		
Country (C)	ES	País. El atributo "C" (country) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en PrintableString
ST, StateOfProvince	Provincia	Provincia de registro de la organización. Opcional (si organizationName y L) Obligatorio
Locality (L)	Localidad	Localidad de registro de la organización. Opcional si tiene StateOfProvince
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	País	(EVG 9.2.4) Subject Jurisdiction of Incorporation or Registration
jurisdictionStateOrProvinceName 1.3.6.1.4.1.311.60.2.1.2	Provincia	Provincia en la que está registrada la empresa (Opcional)
jurisdictionLocalityName 1.3.6.1.4.1.311.60.2.1.1	Localidad	Localidad en la que está registrada la empresa (Opcional)
OrganizationName (O)	Razón Social	Nombre oficial de la organización
businessCategory OID.2.5.4.15	Una de las siguientes: 2.5.4.15 = Private Organization 2.5.4.15 = Government Entity 2.5.4.15 = Business Entity 2.5.4.15 = Non-Commercial Entity	(EVG 9.2.3) Categoría de organización: Organización privada Entidad pública Empresa Entidad no comercial
SERIAL NUMBER (SN)	CIF	CIF de la Organización suscriptora del certificado
Organization Identifier (OI)	Identificador de la organización	identificador de la organización según norma ETSI EN 319 412-1 (*(VATES + NIF de la entidad)* Para PSD2, según ETSI 119-495 *PSDES-BDE-58A230*

Common Name (CN)	Dominio (DNS)	FQDN. Debe ser uno de los indicados en la extensión subjectAltname Denominación del sistema (OID 2.5.4.3) (EVG 9.2.2) Nombre de un único dominio. (BR. 7.1.4.2.2.a) Este dominio debe coincidir con el indicado (o con uno de los indicados) en el Subject Alt Names).
Subject Public Key Info	Clave pública (RSA-2048, RSA-3072 o RSA-4096 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage		Marcado como crítica Opcional
Digital Signature	1 (seleccionado)	
Content Commitment (nonRepudiation)	0 (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		
Server Authentication	1 (seleccionado)	
CRL Distribution Point		

Distribution Point 1	http://psc.sia.es/crlc_ssl_sub01[N].crl	N es el número correspondiente a la CRL particionada
Authority Info Access		
Access Method	Id-ad-ocsp	
Access Location	http://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Method	http://psc.sia.es/ac_ssl_sub01.crt	
Qualified Certificate Statements (Codificado en formato ASN.1)		
QcCompliance	OID 0.4.0.1862.1.1	Certificado cualificado
QcEuRetentionPeriod	15 años	Duración custodia
QcType	OID 0.4.0.1862.1.6.	
id-etsi-qct-web	OID 0.4.0.1862.1.6.3	Certificado Web
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	(Solo PSD2) De acuerdo con la ETSI TS 119 495 • rolesOf PSP • NCAName • NCAId
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	1.3.6.1.4.1.39131.10.1.21.1	
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	http://psc.sia.es/	
User Notice	“Certificado cualificado de autenticación de sitio web de nivel medio. Condiciones	QWAC

	de uso y vías de contacto en: https://psc.sia.es"	
	"Certificado cualificado de autenticación de sitio web PSD2 de nivel medio. Condiciones de uso y vías de contacto en: https://psc.sia.es"	QWAC PSD2
Policy Identifier	0.4.0.194112.1.4 QEVCP-w	ETSI EN 319 411-1 y ETSI EN 319 411-2
Policy Identifier	0.4.0.19495.3.1 QCP-w-psd2	ETSI 119 495 Adicional sólo PSD2
Policy Identifier	0.4.0.2042.1.4	Extended Validation Certificate Policy
Policy Identifier	2.23.140.1.1	OID CAB/Forum
SignedCertificateTimestampList (SCT)	signed_certificate_timestamp (OID 1.3.6.1.4.1.11129.2.4.2)	SCT (Octet String) obtenidos al publicar en dos log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.
Subject Alternative Name		
DNSName	Dominios DNS	Dominios DNS adicionales Certificados wildcard prohibidos para EV
cabfOrganizationIdentifier 2.23.140.3.1		Esquema: identificador de esquema de tres dígitos (VAT, PSD, …) País: código de país de dos dígitos ISO 3166-1 Referencia: identificado de la organización de acuerdo al esquema y país

Tabla 5 – Perfil certificado de Autenticación de Sitio Web (QWAC) y PSD2

5.5 Perfil de Certificado de Sede Electrónica

5.5.1 Certificado de Sede Electrónica – Nivel medio

Certificado Cualificado de Sede Electrónica – Nivel Medio		
Nombre atributo	Valor	Observaciones
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada SSL emisora	
Signature Algorithm	SHA-256 con RSA-2048, RSA-3072 o RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Organization Identifier (OI) 2.5.4.97	VATES- A82733262	identificador de la organización según norma ETSI EN 319 412-1
Common Name (CN)	SIA SSL SUB01 CA	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 13 meses	
Subject (Asunto)		
Country (C)	ES	País. El atributo “C” (country) se codificará de acuerdo a “ISO 3166-1-alpha-2 code elements”, en PrintableString
ST, StateOfProvince	Provincia	Provincia de registro de la sede. Opcional (si organizationName y L) Obligatorio

Locality (L)	Localidad	Localidad de registro de la sede
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	País "ES"	(EVG 9.2.4) Subject Jurisdiction of Incorporation or Registration
jurisdictionStateOrProvinceName 1.3.6.1.4.1.311.60.2.1.2	Provincia	Provincia en la que está registrada la empresa (Opcional)
jurisdictionLocalityName 1.3.6.1.4.1.311.60.2.1.1	Localidad	Localidad en la que está registrada la empresa (Opcional)
OrganizationName (O)	Razón Social	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación (custodio del certificado)
businessCategory OID.2.5.4.15	2.5.4.15 = Government Entity	(EVG 9.2.3) Categoría de organización: Entidad pública
SERIAL NUMBER (SN)	CIF	CIF de la entidad responsable de la sede electrónica
Organization Identifier (OI)	Identificador de la organización EJ. (VATES + NIF de la entidad)	Identificador de la organización según norma ETSI EN 319 412-1.
Common Name (CN)	Dominio (DNS)	FQDN. Debe ser uno de los indicados en la extensión subjectAltname Denominación del sistema (OID 2.5.4.3) (EVG 9.2.3) Nombre de un único dominio.

		(BR. 7.1.4.2.2.a) Este dominio debe coincidir con el indicado (o con uno de los indicados) en el Subject Alt Names).
Subject Public Key Info	Clave pública (RSA-2048, RSA-3072 o RSA-4096 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage		Marcado como crítica opcional
Digital Signature	1 (seleccionado)	
Content Commitment (nonRepudiation)	0 (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		
Server Authentication	1 (seleccionado)	
CRL Distribution Point		
Distribution Point 1	http://psc.sia.es/crlc_ssl_sub01[N].crl	N es el número correspondiente a la CRL particionada
Authority Info Access		
Access Method	Id-ad-ocsp	

Access Location	http://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Method	http://psc.sia.es/ac_ssl_sub01.crt	Es el enlace que permite descargar el certificado CA OCSP
Qualified Certificate Statements (Codificado en formato ASN.1)		
QcCompliance	OID 0.4.0.1862.1.1	Certificado cualificado
QcEuRetentionPeriod	15 años	Duración custodia
QcType	OID 0.4.0.1862.1.6.	
id-etsi-qct-web	OID 0.4.0.1862.1.6.3	Certificado Web
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	1.3.6.1.4.1.39131.10.1.21.1	
Policy Identifier	0.4.0.194112.1.4 QEVCP-w	ETSI EN 319 411-1 y ETSI EN 319 411-2
Policy Identifier	0.4.0.2042.1.4	Extended Validation Certificate Policy
Policy Identifier	2.23.140.1.1	OID CAB/Forum
Policy Identifier	2.16.724.1.3.5.5.2 Nivel Medio	OID Política Sede Electronica nivel medio
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	http://psc.sia.es/	
User Notice	"Certificado cualificado de Sede electrónica de nivel medio. Condiciones de uso y vías de contacto en: https://psc.sia.es"	Sede Electronica nivel medio
SignedCertificateTimestampList (SCT)	signed_certificate_timestamp (OID 1.3.6.1.4.1.11129.2.4.2)	SCT (Octet String) obtenidos al publicar en dos log el pre-certificado. Se obtendrá un SCT por cada log en el que se

		publique este certificado.
Subject Alternative Name		
DNSName	Dominios DNS	Dominios DNS adicionales Certificados wildcard prohibidos para EV
cabfOrganizationIdentifier 2.23.140.3.1		Esquema: identificador de esquema de tres dígitos (VAT, PSD, …) País: código de país de dos dígitos ISO 3166-1 Referencia: identificado de la organización de acuerdo al esquema y país

Tabla 6 – Perfil certificado Sede Electrónica – Nivel Medio

5.5.2 Certificado de Sede Electrónica – Nivel alto

Certificado Cualificado de Sede Electrónica – Nivel alto		
Nombre atributo	Valor	Observaciones
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada SSL emisora	
Signature Algorithm	SHA-256 con RSA-2048, RSA-3072 o RSA-4096	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Organization Identifier (OI)	VATES- A82733262	identificador de la organización según

2.5.4.97		norma ETSI EN 319 412-1
Common Name (CN)	SIA SSL SUB01 CA	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 13 meses	
Subject (Asunto)		
Country (C)	ES	País. El atributo "C" (country) se codificará de acuerdo con "ISO 3166-1-alpha-2 code elements", en PrintableString
ST, StateOfProvince	Provincia	Provincia de registro de la sede. Opcional (si organizationName y L) Obligatorio
Locality (L)	Localidad	Localidad de registro de la sede
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	País "ES"	(EVG 9.2.4) Subject Jurisdiction of Incorporation or Registration
jurisdictionStateOrProvinceName 1.3.6.1.4.1.311.60.2.1.2	Provincia	Provincia en la que está registrada la empresa (Opcional)
jurisdictionLocalityName 1.3.6.1.4.1.311.60.2.1.1	Localidad	Localidad en la que está registrada la empresa (Opcional)
OrganizationName (O)	Razón Social	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación

		(custodio del certificado)
businessCategory OID.2.5.4.15	2.5.4.15 = Government Entity	(EVG 9.2.3) Categoría de organización: Entidad pública
SERIAL NUMBER (SN)	CIF	CIF de la entidad responsable de la sede electrónica
Organization Identifier (OI)	Identificador de la organización EJ. (VATES + NIF de la entidad)	Identificador de la organización según norma ETSI EN 319 412-1.
Common Name (CN)	Dominio (DNS)	FQDN. Debe ser uno de los indicados en la extensión subjectAltname Denominación del sistema (OID 2.5.4.3) (EVG 9.2.3) Nombre de un único dominio. (BR. 7.1.4.2.2.a) Este dominio debe coincidir con el indicado (o con uno de los indicados) en el Subject Alt Names).
Subject Public Key Info	Clave pública (RSA-2048 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage		Marcado como crítica opcional

Digital Signature	1 (seleccionado)	
Content Commitment (nonRepudiation)	0 (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		
Server Authentication	1 (seleccionado)	
CRL Distribution Point		
Distribution Point 1	http://psc.sia.es/crlc_ssl_sub01[N].crl	N es el número correspondiente a la CRL particionada
Authority Info Access		
Access Method	Id-ad-ocsp	
Access Location	http://psc.sia.es/ocsp	
Access Method	id-ad-calssuers	
Access Method	http://psc.sia.es/ac_ssl_sub01.crt	Es el enlace que permite descargar el certificado CA OCSP
Qualified Certificate Statements (Codificado en formato ASN.1)		
QcCompliance	OID 0.4.0.1862.1.1	Certificado cualificado
QcEuRetentionPeriod	15 años	Duración custodia
QcType	OID 0.4.0.1862.1.6.	
id-etsi-qct-web	OID 0.4.0.1862.1.6.3	Certificado Web
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	1.3.6.1.4.1.39131.10.1.21.1	

Policy Identifier	0.4.0.194112.1.4 QEVCP-w	ETSI EN 319 411-1 y ETSI EN 319 411-2
Policy Identifier	0.4.0.2042.1.4	Extended Validation Certificate Policy
Policy Identifier	2.23.140.1.1	OID CAB/Forum
Policy Identifier	2.16.724.1.3.5.5.1 Nivel Alto	OID política Sede Electronica nivel alto
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	http://psc.sia.es/	
User Notice	"Certificado cualificado de Sede electrónica EV de nivel alto. Condiciones de uso y vías de contacto en: https://psc.sia.es"	Sólo para Sede Electronica nivel alto
SignedCertificateTimestampList (SCT)	signed_certificate_timestamp (OID 1.3.6.1.4.1.11129.2.4.2)	SCT (Octet String) obtenidos al publicar en dos log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.
Subject Alternative Name		
DNSName	Dominios DNS	Dominios DNS adicionales Certificados wildcard prohibidos para EV
cabfOrganizationIdentifier 2.23.140.3.1		Esquema: identificador de esquema de tres dígitos (VAT, PSD, …) País: código de país de dos dígitos ISO 3166-1 Referencia: identificado de la organización de acuerdo con el esquema y país

Tabla 7 – Perfil certificado Sede Electrónica– Nivel Alto

6. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

6.1 Tarifas

6.1.1 Tarifas de emisión de certificado o renovación

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

6.1.2 Tarifas de acceso a los certificados

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

6.1.3 Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se 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 se detallará en la página web del prestador SIA.

6.2 Obligaciones

Aplican las obligaciones generales definidas en la Declaración de Prácticas de Certificación (DPC) de SIA.

6.2.1 Obligaciones de la AC

Cuando SIA AC emite un certificado definido en esta política, SIA AC representa y garantiza a los Beneficiarios del Certificado enumerados en la Sección 9.6.1 de CA/B Forum Baseline, durante el período en que el certificado es válido, que SIA AC ha cumplido con los requisitos de CA/B Forum Guidelines y CA/B Forum Baselines, con su DPC y esta PC, en la emisión y administración del certificado y en la verificación de la precisión de la información contenida en el certificado.

Las garantías de certificación EV incluyen las especificadas en la sección 7.1. de los EV Guidelines.

6.2.2 Obligaciones de identificación

SIA comprueba, por si misma o por medio de aquellas entidades con las que suscriba el correspondiente instrumento legal, la identidad y cualesquiera otras circunstancias personales de los solicitantes y suscriptores de los certificados. En ningún caso SIA delega la comprobación de la titularidad o control sobre el dominio.

6.2.3 Obligaciones del suscriptor del certificado

Los suscriptores de certificados EV realizan los compromisos y garantías establecidos en la Sección 9.6.3 de la DPC de SIA AC para el beneficio de la CA y los Beneficiarios del Certificado.

El instrumento legal existente entre las partes incluirá la exigencia de cumplimiento de lo indicado en los documentos del *CA/Browser Forum*

Son obligaciones del suscriptor las recogidas en la Declaración de Prácticas de Certificación, Política de Certificación, Términos y condiciones y en el Acuerdo de Divulgación de Clave Pública (PDS) añadiendo las siguientes.

- Aportar de forma fehaciente la información y documentación que se le requiere según el tipo de certificado de autenticación web solicitado (OV-EV) necesaria para acreditar la existencia de la entidad y control que tiene sobre el dominio, todo ello de acuerdo con los requisitos que en cada momento determinen las políticas de la comunidad mundial CABFORUM en sus “Baseline Requirements” y “EV SSL Certificate guidelines”
- Tomar todas las medidas razonables para asegurar el control, mantener la confidencialidad y proteger adecuadamente en todo momento la clave privada que corresponde a la clave pública que se incluirá en el Certificado o Certificados solicitados (y cualquier dato o dispositivo de activación asociado, pines y contraseñas);
- Revisar y verificar la exactitud del Contenido del Certificado;
- Instalar el Certificado solo en servidores accesibles en el(los) subjectAltName(s) enumerado(s) en el Certificado, y de utilizar el Certificado únicamente de conformidad con todas las leyes aplicables y únicamente de acuerdo con el Acuerdo de Suscriptor o términos de uso;
- Solicitar sin demora la revocación del Certificado y dejar de usarlo y su clave privada asociada, si:
    - Hay algún uso o compromiso real o sospechoso de la clave privada del Suscriptor asociada con la Clave Pública incluida en el Certificado,
    - Cualquier información del Certificado es o se vuelve incorrecta o inexacta.
- Cesar de inmediato todo uso de la clave privada correspondiente a la clave pública incluida en el certificado tras la revocación de dicho Certificado por razones de compromiso de clave.
- Responder a las instrucciones de la AC sobre el compromiso de claves o el uso indebido del certificado dentro de un período de tiempo especificado.
- Reconocer y aceptar que la CA tiene derecho a revocar el certificado inmediatamente si el Solicitante viola los términos del Acuerdo de Suscriptor o términos de uso o si la CA descubre

que el Certificado se está utilizando para habilitar actividades delictivas como ataques de phishing, fraude o la distribución de malware.

6.2.4 Obligaciones de los terceros aceptantes

Según la DPC general de SIA.

An Indra company

Persona de contacto
psc@sia.es

Av. de Bruselas, 35

28108 Alcobendas, Madrid
T +34 91 307 79 97

sia.es