SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA
Avenida de Europa, 2
Alcor Plaza Edificio B
Parque Oeste Alcorcón
28922 Alcorcón - Madrid (España)
Telf: (34) 902 480 580 Fax: (34) 91 641 95 13

psc.sia.es

PC - SIA

Política de Certificación

Certificados reconocidos de Firma Centralizada

OID: 1.3.6.1.4.1.39131.10.1.7

Versión: 1.1

AENOR Seguridad Información UNE-ISO/IEC 27001 SI-0013/2006
AENOR Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-01/2008
AENOR Madurez Software 2 ISO/IEC 15504
AENOR Gestión Continuidad Negocio ISO 22301
ISO 9001 ISO 14001 BUREAU VERITAS Certification
PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

Revisión	Fecha	Autor	Descripción
1.0	12 de abril de 2016	SIA	Primera versión del documento
1.1	26 de mayo de 2016	SIA	Alineación con Informe Preliminar del expediente de comunicación Alta de servicio de Firma Centralizada

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

INDICE

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

RELACION DE TABLAS

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

1. INTRODUCCIÓN

1.1 Resumen

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

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

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

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.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
    - (NOTA: Dicha Directiva será derogada cuando la gran mayoría del articulado de eIDAS sea aplicable, es decir, a partir del 1 de julio de 2016).
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica (Texto consolidado, última modificación: 2 de Octubre de 2015).

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (Norma derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.b) de la Ley 39/2015, de 1 de octubre).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (entrada en vigor: 2 de Octubre de 2016).
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal, como su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que en su Disposición final sexta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social, que en su disposición final cuarta se informa de la modificación de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

La regulación vigente en España, en la fecha de elaboración del presente documento de prácticas y políticas de certificación, continúa siendo la Ley 59/2003, de 19 de diciembre, de Firma Electrónica alineada con eIDAS y la Directiva 1999/93/CE.

Esta Ley ha tenido innumerables efectos beneficiosos si bien no ha conseguido los objetivos fijados en cuanto al uso masivo de la firma reconocida. Dicho nivel de firma tiene la máxima eficacia legal de manera que su utilización otorga una equivalencia automática con la firma manuscrita.

En el ámbito de las AAPP el uso estricto de firmas electrónicas reconocidas es inferior a lo esperado, debido a que las tecnologías necesarias para cualificar la firma electrónica como reconocida exigen en la práctica la utilización de un chip criptográfico certificado como dispositivo cualificado de creación de firma.

En el momento de la creación de la norma de 1999 se apostó por una tecnología muy concreta mediante el expediente técnico de hacer una norma técnica que definiese qué era un dispositivo cualificado de creación de firma, la actual EN419211. Es un perfil de protección que define los requisitos técnicos que debe cumplir en materia de seguridad funcional un producto, pero tal y como está hecho ese producto sólo puede ser un chip criptográfico.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

En este contexto, los Certificados de Firma Centralizada serán emitidos como **Certificados Electrónicos Reconocidos** cumpliendo los requisitos del anexo I de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, así como lo dispuesto a tal efecto en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y como **Certificados Cualificados** cumpliendo los requisitos establecidos en el anexo I de eIDAS. El prestador de servicios de certificación, SIA, cumplirá los requisitos expresados en el anexo II del reglamento indicado anteriormente, y desarrollado en Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

En este sentido, en el artículo 51 de eIDAS establece en el apartado segundo que, los certificados reconocidos expedidos para las personas físicas conforme a la Directiva 1999/93/CE se considerarán **Certificados Cualificados** de firma electrónica con arreglo al presente Reglamento hasta que caduquen.

Asimismo, se han tenido en cuenta los estándares en materia de certificados reconocidos o 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.

De acuerdo con la legislación señalada, se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo cualificado de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

La PC incluye todas las actividades encaminadas a la gestión de los certificados electrónicos en su ciclo de vida, y sirve de guía en la relación entre SIA y los usuarios de sus servicios telemáticos. En consecuencia, todas las partes involucradas tienen la obligación de conocer la PC y ajustar su actividad a lo dispuesto en la misma.

Los Certificados reconocidos de Firma Centralizada sólo pueden ser utilizados por la propia persona física a la cual esta emitido. La emisión de estos certificados se realizará en un dispositivo de creación de firma.

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

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

1.2 Nombre del documento e identificación

Nombre del documento	Política de Certificación de Certificados reconocidos de Firma centralizada
Versión del documento	1.0
Estado del documento	Vigente
Fecha de emisión	12/04/2016
Fecha de caducidad	No aplicable
OID	1.3.6.1.4.1.39131.10.1.7
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 PC

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

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. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece.
- "AC subordinada": Autoridad de Certificación subordinada de "AC raíz". Su función es la emisión de certificados finales, en este caso, la emisión de Certificados Reconocidos de firma centralizada.

En el ámbito de los certificados de firma centralizada, SIA actúa como prestador cualificado de servicios de confianza, emitiendo los certificados electrónicos cualificados de firma y proveyendo servicios de firma electrónica basada en un certificado cualificado y creada mediante un dispositivo cualificado de creación de firma electrónica, conforme a lo establecido en eIDAS y en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

1.3.2 Autoridades de Registro

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

Principalmente, la propia entidad es quien actuará como Autoridad de Registro de SIA para la gestión de las solicitudes y la gestión de la emisión de certificados a aquellas personas físicas con las que tenga vinculación directa. La propia entidad podrá ser el Suscriptor de todos estos certificados emitidos.

Cada entidad que actúe como AR establecerá:

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

1.3.3 Firmante

Se entienden por firmante en el ámbito de certificados reconocidos o cualificados de Firma Centralizada, la persona física titular identificada en el certificado y que haga uso del mismo.

1.3.4 Suscriptor

En el caso de una vinculación directa entre el firmante y una entidad, el suscriptor es la propia entidad con personalidad jurídica que suscribe un contrato con SIA para la expedición de certificados reconocidos a las personas con las que mantenga vinculación directa.

1.3.5 Terceras Partes

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

1.3.6 Otros intervinientes

Según lo definido en la DPC de SIA.

1.4 Uso de los certificados

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

1.4.1 Usos apropiados / permitidos de los certificados

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

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

El propósito principal del Certificado de Firma Centralizada emitido por SIA a una persona física es permitir al titular firmar trámites o documentos. Este certificado (certificado reconocido según la Directiva Europea 99/93/CE y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y cualificado según el eIDAS y por la que se derogará la Directiva 1999/93/CE) permite sustituir la firma manuscrita por la electrónica en las relaciones del ciudadano con terceros. (Ley 59/2003, de 19 de diciembre, de Firma Electrónica artículos 3.4 y 15.2).

El reglamento eIDAS establece que los Certificados Cualificados de Firma Electrónica cumplirán los requisitos establecidos en el anexo I. Por otro lado, la Comisión podrá, mediante actos de ejecución, establecer números de referencia de normas relativas a los certificados cualificados de firma electrónica donde se presumirá el cumplimiento de los requisitos establecidos en dicho anexo cuando un certificado cualificado de firma electrónica se ajuste a dichas normas.

Los certificados de firma son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículo 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones EN 319 412-5.

El uso del certificado de firma proporciona las siguientes garantías:

- No repudio de origen

  Asegura que el documento proviene de la persona física de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del Certificado de Firma. El receptor de un mensaje firmado electrónicamente podrá verificar el certificado empleado para esa firma utilizando cualquiera de los Prestadores de Servicios de Validación. De esta forma garantiza que el documento proviene de un determinado titular.

  Dado que en el sistema de firma con certificados centralizados se garantiza que las claves de firma permanecen, con un alto nivel de confianza, bajo el exclusivo control del titular, la firma es la prueba efectiva del contenido y del autor del documento (garantía de “no repudio”).

- Integridad

  El Certificado reconocido de Firma Centralizado permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma electrónica. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de dicho resumen.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

1.4.2 Limitaciones y restricciones en el uso de los certificados

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

De forma específica, cabe reseñar que este certificado será utilizado por los firmantes en las relaciones que mantengan con terceros que confían, de acuerdo con lo usos autorizados en las extensiones “Key Usage” y “Extended Key Usage” del certificado y en conformidad con las limitaciones que consten en el certificado.

Los certificados no pueden utilizarse para actuar ni como Autoridad de Registro ni como Autoridad de Certificación, firmando certificados de clave pública de ningún tipo ni Listas de Certificados Revocados (CRL).

1.5 Administración de Políticas

1.5.1 Organización responsable

Esta PC es propiedad de SIA.

Nombre	SIA
Dirección correo	psc@sia.es
Dirección postal	Avenida de Europa, 2 Alcor Plaza Edificio B Parque Oeste Alcorcón 28922 Alcorcón - Madrid (España)
Teléfono	+34 902 480 580

Tabla 2 – Organización responsable

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

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

Una vez que el solicitante ha sido registrado en el sistema con nivel avanzado de garantía de registro y ha solicitado expresamente la emisión de su certificado de firma centralizada, dicha emisión se llevará a cabo la primera vez que acceda al procedimiento de generación con los diferentes controles, tales como su DNI, teléfono para segundo factor de autenticación, código de activación, certificado reconocido y dato de contraste.

El par de claves de los Certificados reconocidos de Firma Centralizada, los genera el solicitante, una vez se ha personado, ha sido validado por la Autoridad de Registro y ha firmado el documento de conformidad con la emisión del Certificado reconocido de Firma Centralizada.

Cuando el solicitante acceda al servicio de generación, el sistema informará al titular de que se le va a emitir su certificado de firma centralizada y generará en ese momento su correspondiente clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

La generación del certificado deberá hacerse acorde con los requisitos que la Ley marca con respecto a los plazos máximos permitidos desde que la persona física realizó el registro presencial.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

2.2.2 Autenticación de la identidad de una persona física

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

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

2.2.3 Información no verificada sobre el solicitante

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

2.2.4 Comprobación de las facultades de representación

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

2.3 Identificación y autenticación para peticiones de renovación de claves

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

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

En el ámbito del certificado de firma centralizada, 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.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

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

3.1 Solicitud de certificados

Para los certificados reconocidos de Firma Centralizada, SIA solo admite solicitudes de emisión de certificados expedidos a personas físicas mayores de edad, con capacidad plena de obrar y con capacidad jurídica suficiente.

El solicitante deberá cumplimentar el formulario de solicitud del certificado asumiendo la responsabilidad de la veracidad de la información reseñada, y tramitarlo ante SIA por medio de la Autoridad de Registro Reconocida presencialmente, donde procederá a verificar y firmar el documento de conformidad con la emisión del certificado reconocido o cualificado de Firma Centralizada de los datos de la solicitud. Con este hecho, acepta los requisitos establecidos en la DPC y en esta PC.

3.2 Tramitación de las solicitudes de certificados

Compete a la Autoridad de Registro la comprobación de la identidad y circunstancias personales del solicitante, la verificación de la documentación aportada y la constatación de que el solicitante ha firmado el documento de comparecencia y conformidad con la emisión del Certificado reconocido de Firma Centralizada. Una vez completa la solicitud, la Autoridad de Registro la remitirá al Prestador de Servicios de Certificación para su tramitación.

3.3 Emisión de certificados

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

Las claves para los certificados de firma centralizada se generan en el dispositivo criptográfico centralizado en conformidad con los requisitos Common Criteria EAL 4+ ALC_FLR.1, AVA_VAN.5, así como con FIPS 140-2 Nivel 3 o equivalentes.

El producto utilizado para la generación de los certificados de firma centralizada está certificado por el Centro Criptológico Nacional del Centro Nacional de Inteligencia con fecha 11/09/2015, que cumple con lo especificado en la Declaración de Seguridad de referencia:

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

- SIAVAL Safecert. Declaración de Seguridad v1.3 de junio de 2015, según exigen las garantías definidas en las normas.
- Informe de Certificación del producto SIAVAL SafeCert v2.4.02-20150611-1657.
- Common Methodology for Information Technology Security Evaluation, en su versión 3.1 release 4 para el nivel de garantía de evaluación EAL4+ ALC_FLR.1 y AVA_VAN.5 otorgado por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.

El proceso de emisión se realizara en los siguientes pasos:

1. La AR verificará la identidad del solicitante y los datos que se incluyan en el certificado.
2. El solicitante firmará el documento de comparecencia y conformidad, activando la AR el proceso de emisión para que el solicitante pueda acceder a la web del prestador para completar el proceso de emisión.
3. El solicitante accede a la web del proceso de emisión utilizando como posibles controles, su DNI, datos de contraste, código de activación, certificado reconocido y un segundo factor de autenticación, de manera que para dni y datos de contraste, siempre van acompañados de un código de activación y/o un segundo factor de autenticación.
4. El sistema generará en ese momento su clave privada siguiendo las instrucciones de la AR y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.
5. El titular, deberá introducir la contraseña de protección de su certificado tan sólo conocido por el titular y no almacenada en los sistemas.
6. Se emite el certificado asociado a las claves privadas y se notifica al solicitante la finalización satisfactoria del proceso de emisión.

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

3.3.1 Actuaciones de la AC durante la emisión de los certificados

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

En la emisión de los certificados la AC:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Protege la confidencialidad e integridad de los datos de registro.
- Incluye en el certificado las informaciones establecidas en el artículo 11.2 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

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

El sistema informará al solicitante de que se le va a emitir su certificado de firma centralizada y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

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

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

En la finalización del proceso de generación del Certificado reconocido de Firma Centralizada, se informa al titular que se encuentra disponible dicho certificado para su uso, pudiendo ser usado a partir de ese mismo momento, para los procesos de firma electrónica.

3.4 Aceptación del certificado

3.4.1 Forma en la que se acepta el certificado

La aceptación del certificado es la acción mediante la cual su titular da inicio a sus obligaciones respecto al PSC SIA. El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el firmante y SIA haya sido firmado y los medios que permitan hacer uso del certificado se encuentren en posesión del firmante.

En el caso de generación del certificado centralizado de firma electrónica, el propio acto de emisión conlleva la aceptación implícita del certificado de firma previa aceptación y firma del documento de conformidad con la emisión del Certificado reconocido de Firma Centralizada.

3.4.2 Publicación del certificado por la AC

Los certificados no se publicarán en ningún repositorio de acceso libre.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

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

No se efectúan notificaciones a terceros.

3.5 Par de claves y uso del certificado

3.5.1 Uso de la clave privada del certificados por el titular

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta PC y de acuerdo con lo establecido en la extensión "Key Usage" del certificado.

Del mismo modo, el firmante solo podrá utilizar el par de claves y el certificado tras aceptar las condiciones de uso establecidas en la DPC y PC y solo para lo que éstas establezcan.

Tras la expiración o revocación del certificado, el firmante dejará de usar la clave privada.

Los Certificados de firma centralizada, tendrán como finalidad permitir la firma electrónica reconocida o cualificada de documentos.

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 la extensión "Key Usage" del certificado.

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

3.6 Renovación de certificados sin cambio de claves

3.6.1 Circunstancias para la renovación de certificados sin cambio de claves

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

3.7 Renovación de certificados con cambio de claves

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

El certificado reconocido o cualificado puede ser renovado, entre otros, por los siguientes motivos:

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

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

3.7.2 Quien puede pedir la renovación de un certificado

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

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

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

1. Para el inicio del proceso, el usuario deberá autenticarse con algunos de los siguientes mecanismos: DNI, datos de contraste, código de activación, certificado reconocido y segundo factor, de manera que para dni y datos de contraste, siempre van acompañados de un código de activación y/o un segundo factor de autenticación. Siguiendo las mismas pautas que cuando fue registrado previamente por el Oficial. Si son válidos pasará al siguiente paso.
2. Se solicita al titular que introduzca la contraseña de su nuevo certificado.
3. Se procede a la emisión del certificado. Este proceso engloba todas las operaciones necesarias para llevar a cabo la emisión del certificado y es compartido por los procesos de emisión y renovación de certificado.
4. En ese caso el sistema emitirá y protegerá automáticamente los nuevos certificados, revocando previamente los antiguos, de acuerdo a la normativa vigente sobre certificados electrónicos reconocidos o cualificados.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

5. En todo caso el sistema informará al titular que se ha procedido a la renovación telemática de su certificado y le informará del nuevo periodo de validez del mismo, informando también que el anterior ha sido revocado, especificando los motivos, la fecha y la hora en que el certificado quedará sin efecto.

3.7.3 Tramitación de las peticiones de renovación con cambio de claves

Para la renovación del mismo, aparecen dos formas de proceder:

- Si ha pasado un periodo inferior a cinco (5) años desde que el firmante se personó en la AR, éste deberá efectuar el proceso de emisión de certificados sin la necesidad de la personación en la AR.
- Si ha pasado un periodo superior a cinco (5) años desde que el firmante se personó en la AR, éste deberá personarse nuevamente en la AR y efectuar el proceso de emisión de certificados, como si del proceso inicial se tratara.

Cuando SIA reciba la solicitud del titular en debida forma, y tras comprobar su identidad, se procederá a la generación de nuevas claves criptográficas y a la emisión del nuevo certificado que tendrá como fecha de entrada en vigor el instante en que han sido generado, procediéndose en este mismo proceso al borrado de las claves y certificado anteriores.

Es de aplicación lo recogido en el apartado 3.3 respecto a la emisión de estos certificados.

3.7.4 Notificación de la emisión de nuevos certificados al titular

Al tratarse de una renovación de certificados con cambio de claves y siguiendo el proceso de emisión de certificados como si del proceso inicial se tratara, el sistema informará al titular de que se ha procedido a la renovación telemática de su certificado y le informará del nuevo periodo de validez del mismo, informando también de que el anterior certificado ha sido revocado, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

3.7.5 Forma de aceptación del certificado con nuevas claves

En el ámbito del certificado de firma centralizada, en los casos de renovación del certificado, el propio acto de renovación conlleva la aceptación implícita del certificado previa aceptación y firma del documento de conformidad con la emisión del certificado reconocido o cualificado de Firma Centralizada.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

3.7.6 Publicación del certificado con las nuevas claves por la AC

El certificado reconocido o cualificado de Firma Centralizada no se publicará en ningún repositorio de acceso libre.

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

No se efectúan notificaciones a terceros.

3.8 Modificación de certificados

3.8.1 Causas para la modificación de un certificado

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

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

3.9 Revocación y suspensión de certificados

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

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

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

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.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

Adicionalmente, por compromiso de las claves privadas, por pérdida, robo, hurto, modificación, divulgación o revelación de la clave personal de acceso que permite la activación de las claves privadas o revelación de las claves de acceso que permite la activación de la clave privada de firma centralizada, bien por cualquier otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por entidad ajena a su titular.

3.9.2 Quien puede solicitar la revocación

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

- El titular (persona física) a nombre del cual fue expedido el certificado reconocido o cualificado de firma centralizada.
- La Entidad de Registro que intervino en la emisión.
- La propia AC de SIA cuando tenga conocimiento de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de la DPC.

3.9.3 Frecuencia de emisión de CRLs

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

3.9.4 Requisitos de comprobación en línea de la revocación

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

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

3.9.5 Otras formas de divulgación de información de revocación

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

- 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.

3.10 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. Asimismo, puede ofrecer servicio mediante protocolo OCSP en las políticas de certificación que lo establezcan.

3.10.2 Disponibilidad del servicio

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

3.11 Finalización de la suscripción

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

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

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

3.12 Custodia y recuperación de claves

3.12.1 Prácticas y políticas de custodia y recuperación de claves

El PSC en ningún momento podrá recuperar la clave de los usuarios. En caso de pérdida de la misma se deberá revocar el certificado y emitir uno nuevo.

En el ámbito del Certificado reconocido de Firma Centralizada, la clave privada que se genera quedará custodiada por el PSC, teniendo en cuenta que el acceso a esta clave será realizada por medios que garantizan, con un alto nivel de confianza, el control exclusivo por parte del firmante.

En este sentido, el acceso a dicha clave sólo puede ser efectuado por el titular de la misma mediante una aplicación al efecto donde el titular deberá estar debidamente autenticado. Posteriormente para la firma, deberá introducir el PIN de protección de su certificado tan sólo conocido por el titular y no almacenada en los sistemas, más un segundo factor de autenticación.

Sólo prestadores de servicios de certificación que expidan certificados reconocidos podrán gestionar los datos de creación de firma electrónica en nombre del firmante. Para ello, podrán efectuar una copia de seguridad de los datos de creación de firma siempre que la seguridad de los datos duplicados sea del mismo nivel que la de los datos originales y que el número de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio. No se podrán duplicar los datos de creación de firma para ninguna otra finalidad.

La autoridad competente realiza copias de seguridad de las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.

En línea con la mención anterior, en el apartado cuarto del anexo II eIDAS se establece que, sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante, podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos cumpliendo lo anteriormente descrito en referencia a la duplicidad de datos.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

4. CONTROLES DE SEGURIDAD FÍSICA

Según lo estipulado en la DPC de SIA.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

5. CONTROLES DE SEGURIDAD TÉCNICA

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

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

5.1 Generación e instalación del par de claves

5.1.1 Generación del par de claves

Las claves para los certificados de firma centralizada se generan en el dispositivo criptográfico centralizado en conformidad con los requisitos Common Criteria EAL 4+ ALC_FLR.1, AVA_VAN.5, así como con FIPS 140-2 Nivel 3 o equivalentes.

5.1.2 Entrega de la clave privada al titular

La clave privada la genera el titular mediante el proceso de emisión provisto por el prestador, una vez ha sido personado y validado por la AR, por medio de un proceso ajustado a la Ley.

La clave privada se genera en un dispositivo de creación de firma bajo el control exclusivo del firmante y, por lo tanto, no existe ninguna entrega de la clave privada al titular.

Una vez que el usuario se ha registrado en el sistema con nivel avanzado de garantía de registro y ha solicitado expresamente la emisión de sus certificados de firma centralizada, dicha emisión se llevará a cabo la primera vez que el titular acceda al procedimiento generación del certificado.

El sistema informará al titular de que se le va a emitir su certificado de firma centralizada y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

5.1.3 Entrega de la clave pública al emisor del certificado

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

5.1.4 Tamaño de las claves

El tamaño de las claves de los certificados reconocidos o cualificados de Firma Centralizada es de 2048 bits.

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

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

5.1.6 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 ficheros y transacciones.

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

Key Usage: Content Commitment[1].

[1] Nonrepudiation

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

5.2 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.

Los módulos utilizados para la creación de claves utilizadas por los certificados reconocidos o cualificados de firma centralizada cumplen los requisitos establecidos en un perfil de protección de producto de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3 o superior nivel de seguridad.

5.2.1 Estándares para los módulos criptográficos

El módulo criptográfico empleado en la emisión de los certificados adscritos a esta Política de Certificación cumplen los requisitos establecidos en un perfil de protección de producto de firma electrónica de autoridad de certificación normalizado, de acuerdo con ITSEC, Common Criteria o FIPS 140-1 Nivel 3 o superior nivel de seguridad.

5.2.2 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, con un alto nivel de confianza, bajo el control exclusivo de los firmantes. No está estipulado que exista control multi-persona para las claves privadas asociadas a los certificados de esta política.

5.2.3 Custodia de la clave privada

La custodia de la clave privada la realiza la autoridad competente siendo únicamente los titulares de las mismas los que pueden acceder a dicha clave, introducir un identificador de usuario (DNI/NIE), una contraseña tan sólo conocida por el titular y no almacenada en los sistemas de SIA, y un segundo factor de autenticación.

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

5.2.4 Copia de seguridad de la clave privada

En el ámbito de los certificados reconocidos o cualificados de firma centralizada, la autoridad competente realiza copias de seguridad de las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.

5.2.5 Archivo de la clave privada

En el ámbito de los certificados reconocidos o cualificados de Firma Centralizada, la autoridad competente mantiene, según la legislación vigente, las copias de seguridad con las claves privadas protegidas, siendo éstas únicamente accesibles por el titular.

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

La generación de las claves ligadas al Certificado reconocido de Firma Centralizada, se realiza en el dispositivo criptográfico centralizado en conformidad con los requisitos Common Criteria EAL 4+ ALC_FLR.1, AVA_VAN.5, así como con FIPS 140-2 Nivel 3 o equivalentes y se almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

5.2.7 Almacenamiento de la clave privada en un módulo criptográfico

En relación al certificado de firma centralizada, la clave privada asociada se genera y utiliza en un dispositivo criptográfico centralizado en conformidad con los requisitos Common Criteria EAL 4+ ALC_FLR.1, AVA_VAN.5, así como con FIPS 140-2 Nivel 3 o equivalentes.

Es responsabilidad del firmante la confidencialidad del acceso a las mismas.

5.2.8 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 implementa el uso de un dato de activación y contraseña para la activación de la clave privada.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

La activación de la clave privada requiere autenticación del titular en el sistema de firma centralizada, siendo necesario introducir un identificador de usuario (DNI/NIE), una contraseña tan sólo conocida por el titular y no almacenada en los sistemas, más un segundo factor de autenticación.

5.2.9 Método de desactivación de la clave privada

La desactivación se realizará cuando el firmante cierre la aplicación software de creación de firma.

Si un titular autenticado en el sistema se equivoca repetidas veces en su contraseña de firma, tanto su clave como el certificado de firma se bloquearán automáticamente de manera temporal, pudiendo ser implementado una prueba de Turing (Captcha).

5.2.10 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.

En el ámbito de los certificados de esta PC, en procesos de renovación/revocación se destruyen las claves de los firmantes. El certificado es revocado por SIA, y las claves y certificados dados de baja de forma segura incluyendo las copias realizadas para garantizar la continuidad del servicio.

5.3 Otros aspectos de la gestión del par de claves

5.3.1 Periodos operativos de los certificados y periodo de uso para el par de claves

Los certificados emitidos al amparo de la presente política tienen una validez de tres (3) años. El par de claves utilizado para la emisión de los certificados se crea para cada emisión y por tanto también tiene una validez de tres (3) años.

En el caso que haya transcurrido más de 5 años desde la identificación inicial de la persona física, en cumplimiento del artículo 13 de la Ley de Firma Electrónica ("*La identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará …*") la renovación deberá tramitarse ante SIA por medio de la Autoridad de Registro Reconocida presencialmente.

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

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

5.4 Datos de activación

5.4.1 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.

El acceso a los certificados de firma centralizada, sólo puede ser efectuado por el titular del mismo mediante una aplicación al efecto donde el firmante deberá estar autenticado. Para poder usar la firma centralizada, será necesario activar la misma. Para la firma, deberá introducir la contraseña de protección de su certificado tan sólo conocido por el firmante y no almacenada en los sistemas, más un segundo factor de autenticación.

5.4.2 Protección de los datos de activación

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

La contraseña de acceso a la clave privada del certificado de firma centralizada es confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados en los servicios ofrecidos a través de una red de comunicaciones; por lo tanto, deben tenerse en cuenta unas normas de seguridad para su custodia y uso:

- Memorícelas y procure no anotarlas en ningún documento físico ni electrónico que el Titular conserve.
- No envíe ni comunique a nadie ni por ningún medio, ya sea vía telefónica, correo electrónico, etc.
- Recuerde que son personales e intransferibles. Si cree que esta información puede ser conocida por otra persona, debe cambiarla. El uso de las mismas por persona distinta del Titular presupone grave negligencia por parte del mismo y permite la activación de las claves privadas para poder realizar operaciones de firma electrónica en su nombre. Es obligación del titular notificar la pérdida de control sobre su clave privada, a causa del compromiso de las mismas, ya que es motivo de revocación del certificado asociado a dichas claves.
- Como medida adicional, deberá abstenerse de escoger un número relacionado con sus datos personales, así como cualquier otro código que pueda resultar fácilmente predecible por terceras personas (fecha de nacimiento, teléfono, series de números consecutivos, repeticiones de la misma cifra, secuencias de cifras que ya forman parte de su número de DNI, etc.)
- Se recomienda cambiarlo periódicamente.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

6. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

6.1 Perfil de certificado

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

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and CRL Profile".
- RFC 3739 "Internet x509 Public Key Infrastructure. Qualified Certificates Profile" (prevaleciendo en caso de conflicto la EN).
- Perfiles de Certificados Electrónicos para la Administración General del Estado según Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Los perfiles están definidos en el Anexo II de la Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

6.1.1 Número de versión

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

6.1.2 Extensiones del certificado

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

Los campos singulares para identificar al certificado reconocido o cualificado de Firma Centralizada son:

- Datos de identificación personal de titular del certificado:
  - Nombre y apellidos.
  - Número de Documento Nacional de Identidad (DNI) o Número de Identificación del Extranjero (NIE).
  - Clave pública asociada a la persona física

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

Las extensiones utilizadas en los certificados son:

- Authority Key Identifier.
- Subject Key Identifier.
- KeyUsage. Calificada como crítica.
- CRL Distribution Point.
- Authority Information Access.
- Qualified Certificate Statements.
- CertificatePolicies.
- Subject Alternative Name.

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

Los certificados que son expedidos con la calificación de reconocidos o 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 "QcStatement", conforme a las normas vigentes. En concreto, los Certificados reconocidos de Firma Centralizada incluyen las siguientes declaraciones:

- QcCompliance, establece la calificación con la que se ha realizado la emisión del "Certificado reconocido".
- QcEuRetentionPeriod, determina el periodo de conservación de toda la información relevante para el uso de un certificado, tras la caducidad de este. En el caso de SIA, es de quince (15) años.
- QcSSCD. Indica el uso de dispositivo cualificado de creación de firma.

SIA tiene definida una política de asignación de OIDs dentro de su rango privado de numeración por la cual el OID de todas las extensiones propietarias de Certificados de SIA comienza por el prefijo 1.3.6.1.4.1.39131.10.2.

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

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

OID	Concepto	Descripción
1.3.6.1.4.1.39131.10.2.1	Tipo de certificado	Tipo de certificado
1.3.6.1.4.1.39131.10.2.2	Nombre	Nombre del usuario
1.3.6.1.4.1.39131.10.2.3	Apellido1	Primer apellido del usuario
1.3.6.1.4.1.39131.10.2.4	Apellido2	Segundo apellido del usuario
1.3.6.1.4.1.39131.10.2.5	DNI	DNI del usuario

Tabla 3 – Definición extensión SubjectAltName

Los certificados de firma centralizada se emiten en calidad de certificados reconocidos o cualificados y, por tanto contiene los campos que establece la normativa legalmente aplicable en materia de Certificados Reconocidos:

Artículo 11 del Capítulo II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Anexo I de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

Requisitos Legales	Modo de cumplimiento
La indicación que se expiden como certificados reconocidos (artículo 11.2.a 59/2003)	Inclusión de la extensión Qualified Certificate Statements que incorpora las siguientes declaraciones: 1.- id-etsi-qcs-QcCompliance – Indica que el certificado se emite como reconocido de acuerdo a los Anexo I y II de la Directiva del Parlamento Europeo 1999/93/CE y a la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. 2.- id-etsi-qcs-QcSSCD –. Indica que la clave privada correspondiente al certificado está almacenada en un dispositivo cualificado de creación de firma de acuerdo al Anexo III de la Directiva del Parlamento Europeo 1999/93/CE y a la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

La identificación del prestador de servicios de certificación que expide el certificado y el país en el que está establecido (artículo 11.2.c 59/2003)	**A través de la información que se recoge en el campo Issuer del certificado tal y como contempla la RFC3739.** **En el certificado se recoge claramente el país en el que se establece el PSC en el atributo Country del DN del campo Issuer.** **En la presente PC, se recoge el nombre o razón social, domicilio, dirección electrónica y número de identificación fiscal de la Institución que actúa como PSC de los certificados de firma centralizada: SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA.**
La identificación del firmante, por su nombre y apellidos y DNI o equivalente, o a través de un seudónimo que conste de manera inequívoca. (artículo 11.2.e 59/2003)	**A través de la información que se recoge en el campo Subject del certificado tal y como contempla la RFC3739: Nombre, Apellidos y DNI.** **No se contempla la utilización de seudónimos.**
Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante. (artículo 11.2.f 59/2003)	**La clave pública del firmante se encuentra en el certificado tal y como contempla la RFC5280. (Subject Public Key Info)**
El comienzo y el final del periodo de validez del certificado. (artículo 11.2.g 59/2003)	**El periodo de validez de las claves y el certificado asociado se encuentra recogido en el campo del certificado contemplado en la ITU-T Recommendation X.509 y en RFC5280.**
El código identificativo único del certificado. (artículo 11.2.b 59/2003)	**La pareja formada por el Número de serie del certificado y el Issuer tal y como se contempla en la ITU-T Recommendation X.509 y en RFC5280.**
La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado. (artículo 11.2.d 59/2003)	**La firma digital del emisor del certificado de acuerdo con la ITU-T Recommendation X.509 y la RFC5280.**
Los límites de uso del certificado, si se prevén. (artículo	**Estos límites estarán reflejados en la Políticas de Certificación asociadas a los certificados y en la extensión**

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

11.2.h 59/2003)	KeyUsage tal y como se contempla en la ITU-T Recommendation X.509 y en RFC5280.
Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen. (artículo 11.2.i 59/2003)	No estipulado en el certificado.

Tabla 4 – Normativa legal aplicable I

Artículos 18, 19, 20 del Capítulo II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Anexo II de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

Requisitos Legales	Modo de cumplimiento
El requisito B) establece la necesidad de un servicio de comprobación del estado de los certificados. (artículo 18.d 59/2003)	La extensión AIA (Authority Information Access) contiene la URL del servicio de validación de certificados de Identidad Pública. Así mismo también se dispone de la extensión cRLDistributionPoint.
El requisito i) establece un periodo mínimo de retención de la información relevante (artículo 20.1.f 59/2003)	No estipulado en el certificado. No se prevé la destrucción de la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación, aunque de establecer un periodo de retención, este no sería inferior a los 15 años establecidos en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
El requisito K) establece que los términos y condiciones de uso de los certificados deben estar accesibles a las terceras partes que hacen uso del certificado. (artículo II.19.2 59/2003)	En la extensión Certificate Policies se indica la URL en la que están accesibles esta DPC y las Políticas de Certificación asociadas.

Tabla 5 – Normativa legal aplicable II

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

6.1.3 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).

6.1.4 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.

6.1.5 Restricciones de los nombres

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

El DN para los Certificados reconocidos de Firma Centralizada, estará compuesto de los siguientes elementos:

- CN, G, SN, SerialNumber, C

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

La sintaxis de estos atributos es la siguiente:

- CN = Apellido1 Apellido2 Nombre – DNI NNNNNNNNA (FIRMA CENTRALIZADA)
- SN = Apellido1
- G = Nombre
- SerialNumber = DNI/NIE en formato NNNNNNNNA
- C = País de la persona física. El atributo "C" (country) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en PrintableString.

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

El OID de la presente PC es 1.3.6.1.4.1.39131.10.1.7.

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

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

Política de Certificados Reconocidos de Firma Centralizada	1.3.6.1.4.1.39131.10.1.7

Tabla 6 – OID política de certificación

6.1.7 Uso de la extensión "PolicyConstraints"

No estipulado.

6.1.8 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.

6.1.9 Tratamiento semántico para la extensión "Certificate Policy"

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

6.2 Certificado de Firma Centralizada

Certificado reconocido de Firma Centralizada		
Nombre atributo	**Valor**	**Observaciones**
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada emisora	

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

Signature Algorithm	SHA-256 con RSA-2048	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Serial Number (serialNumber)	A82733262	
Common Name (CN)	SIA SUB01	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 3 años	
Subject (Asunto)		
Country (C)	ES	España
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	Razón social de SIA
Serial Number (serialNumber)	<DNI>	DNI del usuario
Surname	<Apellido1>	Primer apellido
Given Name	<Nombre>	Nombre de pila
Common Name (CN)	<Apellido1> <Apellido2> <Nombre> – DNI <DNI> (FIRMA CENTRALIZADA)	Nombre, apellidos y DNI del ciudadano
Subject Public Key Info	Clave pública (RSA-2048 Bits), codificada de acuerdo con el algoritmo criptográfico	
Extensiones x509 v3		
Authority Key Identifier	Identificador de la clave pública del emisor	
Subject Key Identifier	Identificador de la clave pública del firmante del certificado	
KeyUsage		Marcado como crítica
Digital Signature	**1 (seleccionado)**	
Content Commitment (nonRepudiation)	**1 (seleccionado)**	
Key Encipherment	0 (no seleccionado)	
Data Encipherment	0 (no seleccionado)	
Key Agreement	**1 (seleccionado)**	
Key Certificate Signature	0 (no seleccionado)	
CRL Signature	0 (no seleccionado)	
EncipherOnly	0 (no seleccionado)	
DecipherOnly	0 (no seleccionado)	

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

Extended Key Usage		
Email Protection	0 (no seleccionado)	
Client Authentication	**1 (seleccionado)**	
CRL Distribution Point		
Distribution Point 1	https://psc.sia.es/ac_sub01.crl	
Distribution Point 2	http://psc.sia.es/ac_sub01.crl	
Authority Info Access		
Access Method	id-ad-caIssuers	
Access Method	https://psc.sia.es/ac_sub01.crt	
Access Method	Id-ad-ocsp	
Access Location	https://psc.sia.es/ocsp	
Qualified Certificate Statements		
QcCompliance	OID 0.4.0.1862.1.1	Certificado reconocido
QcEuRetentionPeriod	15 años	Duración custodia
QcSSCD	OID 0.4.0.1862.1.4	Uso de dispositivo cualificado de firma
Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.7	
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	"Certificado reconocido de firma centralizada". Consulte las condiciones de uso en https://psc.sia.es. Contacto: Avda. de Europa, 2 Alcor Plaza. Edificio B Parque Oeste Alcorcón - 28922 Alcorcón - Madrid"	
Subject Alternative Name		
Nombre RFC822	< correo electrónico de la persona responsable del certificado >	Correo electrónico de la persona responsable del certificado
Tipo del certificado	OID: 1.3.6.1.4.1.39131.10.2.1: Certificado electronico reconocido de Firma Centralizada	
Nombre	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del usuario
Primer apellido	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido1>	Primer apellido del usuario
Segundo apellido	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido2>	Segundo apellido del usuario
DNI	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI>	DNI del usuario

Tabla 7 – Perfil certificado

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª

7. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

7.1 Tarifas

7.1.1 Tarifas de emisión de certificado o renovación

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

7.1.2 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.

7.1.3 Tarifas de acceso a la información de estado o revocación

El acceso a la información de estado o revocación de los certificados es libre y gratuita y por tanto no se aplicara ninguna tarifa.

7.1.4 Tarifas de otros servicios tales como información de políticas

No se aplicara ninguna tarifa por el servicio de información sobre esta política ni por ningún otro servicio adicional del que se tenga conocimiento en el momento de la redacción del presente documento.

7.1.5 Política de reembolso

La política de reembolso se detallará en la página web del prestador SIA.

Sistemas Informáticos Abiertos S.A. – C.I.F.: A/82733262 – Inscrita en el registro Mercantil de Madrid, Tomo 15.741, folio 28, Sección 8, hoja M-265398, inscripción 1ª