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 de Ciudadano

OID: **1.3.6.1.4.1.39131.10.1.3**

Versión: 1.1

HISTÓRICO DE CONTROL DE CAMBIOS DEL DOCUMENTO

Revisión	Fecha	Autor	Descripción
1.0	30 de enero de 2015	SIA	Primera versión del documento
1.1	20 de mayo de 2015	SIA	Alineación con Informe Preliminar del expediente de comunicación del inicio de actividad.

INDICE

1. INTRODUCCIÓN 12

1.1 Resumen 12

1.2 Nombre del documento e identificación 13

1.3 Entidades y personas intervinientes 13

1.3.1 Autoridad de Certificación 14

1.3.2 Autoridades de Registro 14

1.3.3 Firmante 14

1.3.4 Terceras Partes Aceptantes 15

1.3.5 Otros intervinientes 15

1.4 Uso de los certificados 15

1.4.1 Usos apropiados / permitidos de los certificados 15

1.4.2 Limitaciones y restricciones en el uso de los certificados 15

1.5 Administración de Políticas 16

1.5.1 Organización responsable 16

1.5.2 Persona de contacto 16

1.5.3 Responsables de adecuación de la PC 16

1.5.4 Procedimientos de aprobación de esta PC 16

1.6 Definiciones y Acrónimos 17

1.6.1 Definiciones 17

1.6.2 Acrónimos 19

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN 21

2.1 Repositorios 21

2.2 Publicación de información de certificación 21

2.3 Temporalidad o frecuencia de publicación 21

2.4 Controles de acceso a los repositorios 21

3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS 22

3.1 Nombres 22

3.1.1 Tipos de nombres 22

3.1.2 Necesidad de que los nombres sean significativos 22

3.1.3 Uso de seudónimos 22

3.1.4 Reglas para interpretar varios formatos de nombres 22

3.1.5 Unicidad de los nombres 22

3.1.6 Procedimientos de resolución de conflictos sobre nombres 22

3.1.7 Reconocimiento, autenticación y papel de las marcas registradas 23

3.2 Validación de la identidad inicial 23

3.2.1 Métodos para probar la posesión de la clave privada 23

3.2.2 Autenticación de la identidad de una persona jurídica 23

3.2.3 Autenticación de la identidad de una persona física 23

3.2.4 Información no verificada sobre el solicitante 23

3.2.5 Comprobación de las facultades de representación 24

3.3 Identificación y autenticación para peticiones de renovación de claves 24

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS 25

4.1 Solicitud de certificados 25

4.2 Tramitación de las solicitudes de certificados 25

4.3 Emisión de certificados 25

4.4 Aceptación del certificado 26

4.4.1 Forma en la que se acepta el certificado 26

4.4.2 Publicación del certificado por la AC 26

4.4.3 Notificación de la emisión del certificado por la AC a otras Autoridades 26

4.5 Par de claves y uso del certificado 26

4.5.1 Uso de la clave privada del certificados por el titular 26

4.5.2 Uso de la clave pública y del certificado por los terceros aceptantes 27

4.6 Renovación de certificados sin cambio de claves 27

4.6.1 Circunstancias para la renovación de certificados sin cambio de claves 27

4.7 Renovación de certificados con cambio de claves 27

4.7.1 Circunstancias para una renovación con cambio de claves de un certificado 27

4.7.2 Quien puede pedir la renovación de un certificado 27

4.7.3 Tramitación de las peticiones de renovación con cambio de claves 28

4.7.4 Notificación de la emisión de nuevos certificados al titular 28

4.7.5 Forma de aceptación del certificado con nuevas claves 28

4.7.6 Publicación del certificado con las nuevas claves por la AC 28

4.7.7 Notificación de la emisión del certificado por la AC a otras Autoridades 28

4.8 Modificación de certificados 29

4.8.1 Causas para la modificación de un certificado 29

4.9 Revocación y suspensión de certificados 29

4.9.1 Causas para la revocación 29

4.9.2 Quien puede solicitar la revocación 29

4.9.3 Procedimiento de solicitud de revocación 29

4.9.4 Periodo de gracia de la solicitud de revocación 30

4.9.5 Plazo en que la AC debe resolver la solicitud de revocación 30

4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes 30

4.9.7 Frecuencia de emisión de CRLs 30

4.9.8 Tiempo máximo entre la generación y la publicación de las CRLs 30

4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados 30

4.9.10 Requisitos de comprobación en línea de la revocación 30

4.9.11 Otras formas de divulgación de información de revocación 31

4.9.12 Requisitos especiales de renovación de claves comprometidas 31

4.9.13 Circunstancias para la suspensión 31

4.9.14 Quien puede solicitar la suspensión 31

4.9.15 Procedimiento para la solicitud de suspensión 31

4.9.16 Límites del periodo de suspensión 31

4.10 Servicios de información del estado de certificados 32

4.10.1 Características operativas 32

4.10.2 Disponibilidad del servicio 32

4.10.3 Características adicionales 32

4.11 Finalización de la suscripción 32

4.12 Custodia y recuperación de claves 32

4.12.1 Prácticas y políticas de custodia y recuperación de claves 32

4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión 33

5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y DE OPERACIONES 34

5.1 Controles de seguridad física 34

5.1.1 Ubicación física y construcción 34

5.1.2 Acceso físico 34

5.1.3 Alimentación eléctrica y aire acondicionado 34

5.1.4 Exposición al agua 34

5.1.5 Protección y prevención de incendios 34

5.1.6 Sistema de almacenamiento 34

5.1.7 Eliminación de los soportes de información 35

5.1.8 Copias de seguridad fuera de las instalaciones 35

5.2 Controles de Procedimiento 35

5.2.1 Roles responsables del control y gestión 35

5.2.2 Número de personas requeridas por tarea 35

5.2.3 Identificación y autenticación para cada usuario 35

5.2.4 Roles que requieren segregación de funciones 35

5.3 Controles de Personal 35

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales 35

5.3.2 Procedimientos de comprobación de antecedentes 36

5.3.3 Requerimientos de formación 36

5.3.4 Requerimientos de frecuencia de actualización de la información 36

5.3.5 Frecuencia y secuencia de rotación de tareas 36

5.3.6 Sanciones por actuaciones no autorizadas 36

5.3.7 Requisitos de contratación de terceros 36

5.3.8 Documentación proporcionada al personal 36

5.4 Procedimientos de auditoria de seguridad 37

5.4.1 Tipos de eventos registrados 37

5.4.2 Frecuencia de procesado de registros de auditoria 37

5.4.3 Periodo de conservación de los registros de auditoria 37

5.4.4 Protección de los registros de auditoria 37

5.4.5 Procedimientos de respaldo de los registros de auditoria 37

5.4.6 Sistema de recogida de información de auditoria 37

5.4.7 Notificación al sujeto causa del evento 37
5.4.8 Análisis de vulnerabilidades 38
5.5 Archivo de registros 38
5.5.1 Tipos de eventos archivados 38
5.5.2 Periodo de conservación de registros 38
5.5.3 Protección del archivo 38
5.5.4 Procedimientos de copia de respaldo del archivo 38
5.5.5 Requerimientos para el sellado de tiempo de los registros 38
5.5.6 Sistema de archivo de información de auditoría 38
5.5.7 Procedimientos para obtener y verificar información archivada 39
5.6 Cambio de claves de una AC 39
5.7 Recuperación en casos de vulneración de una clave y de desastre natural u otro tipo de catástrofe 39
5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades 39
5.7.2 Alteración de los recursos hardware, software y/o datos 39
5.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad 39
5.7.4 Continuidad de negocio después de un desastre natural u otro tipo de catástrofe 39
5.8 Cese de una AC o AR 40
5.8.1 Autoridad de Certificación 40
5.8.2 Autoridad de Registro 40
6. CONTROLES DE SEGURIDAD TÉCNICA 41
6.1 Generación e instalación del par de claves 41
6.1.1 Generación del par de claves 41
6.1.2 Entrega de la clave privada al titular 41
6.1.3 Entrega de la clave pública al emisor del certificado 41
6.1.4 Entrega de la clave pública de la AC a los terceros aceptantes 41
6.1.5 Tamaño de las claves 42
6.1.6 Parámetros de generación de la clave pública y verificación de la calidad 42
6.1.7 Usos admitidos de la clave (campo KeyUsage de X.509 v3) 42
6.2 Protección de la clave privada y controles de ingeniería de los módulos criptográficos 42
6.2.1 Estándares para los módulos criptográficos 43
6.2.2 Control multi-persona (n de m) de la clave privada 43

6.2.3 Custodia de la clave privada 43
6.2.4 Copia de seguridad de la clave privada 43
6.2.5 Archivo de la clave privada 43
6.2.6 Transferencia de la clave privada a o desde el módulo criptográfico 44
6.2.7 Almacenamiento de la clave privada en un módulo criptográfico 44
6.2.8 Método de activación de la clave privada 44
6.2.9 Método de desactivación de la clave privada 44
6.2.10 Método de destrucción de la clave privada 44
6.2.11 Clasificación de los módulos criptográficos 45
6.3 Otros aspectos de la gestión del par de claves 45
6.3.1 Archivo de la clave pública 45
6.3.2 Periodos operativos de los certificados y periodo de uso para el par de claves 45
6.4 Datos de activación 45
6.4.1 Generación e instalación de los datos de activación 45
6.4.2 Protección de los datos de activación 45
6.4.3 Otros aspectos de los datos de activación 45
6.5 Controles de seguridad informática 46
6.6 Controles de seguridad del ciclo de vida 46
6.7 Controles de seguridad de la red 46
6.8 Fuentes de tiempo 46
7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP 47
7.1 Perfil de certificado 47
7.1.1 Número de versión 47
7.1.2 Extensiones del certificado 47
7.1.3 Identificadores de objeto (OID) de los algoritmos 49
7.1.4 Formatos de nombre 49
7.1.5 Restricciones de nombre 49
7.1.6 Identificador de objeto (OID) de la Política de Certificación 50
7.1.7 Uso de la extensión “PolicyConstraints” 50
7.1.8 Sintaxis y semántica de los “PolicyQualifier” 50
7.1.9 Tratamiento semántico para la extensión “Certificate Policy” 50

7.2 Perfil de Certificado de Ciudadano 51

7.3 Perfil de CRL 53

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES 54

8.1 Frecuencia o circunstancias de los controles para cada autoridad 54

8.2 Identificación / cualificación del auditor 54

8.3 Relación entre el auditor y la Autoridad auditada 54

8.4 Aspectos cubiertos por los controles 54

8.5 Acciones a emprender como resultado de la detección de deficiencias 54

8.6 Comunicación de resultados 54

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD 55

9.1 Tarifas 55

9.1.1 Tarifas de emisión de certificado o renovación 55

9.1.2 Tarifas de acceso a los certificados 55

9.1.3 Tarifas de acceso a la información de estado o revocación 55

9.1.4 Tarifas de otros servicios tales como información de políticas 55

9.1.5 Política de reembolso 55

9.2 Responsabilidad Financiera 56

9.2.1 Seguro de responsabilidad civil 56

9.3 Confidencialidad de la información 56

9.3.1 Ámbito de la información confidencial 56

9.3.2 Información no confidencial 56

9.3.3 Deber de secreto profesional 56

9.4 Protección de datos personales 56

9.5 Derechos de propiedad Intelectual 56

9.6 Obligaciones 57

9.6.1 Obligaciones de la AC 57

9.6.2 Obligaciones de la AR 57

9.6.3 Obligaciones de los firmantes 57

9.6.4 Obligaciones de los terceros aceptantes 57

9.6.5 Obligaciones de otros participantes 57

9.7 Renuncias de garantías 57

9.8 Limitaciones de responsabilidad 57

9.9 Responsabilidades 58

9.9.1 Limitaciones de responsabilidades 58

9.9.2 Responsabilidades de la Autoridad de Certificación 58

9.9.3 Responsabilidades de la Autoridad de Registro 58

9.9.4 Responsabilidad del titular 58

9.9.5 Delimitación de responsabilidades 58

9.9.6 Alcance de la cobertura 58

9.9.7 Cobertura de seguro u otras garantías para los terceros aceptantes 59

9.10 Limitaciones de pérdidas 59

9.11 Periodo de validez 59

9.11.1 Plazo 59

9.11.2 Sustitución y derogación de la DPC 59

9.11.3 Efectos de finalización 59

9.12 Notificaciones individuales y comunicaciones con participantes 59

9.13 Reclamaciones y jurisdicción 59

9.14 Legislación aplicable 60

9.15 Conformidad con la Ley aplicable 60

9.16 Clausulas diversas 60

9.16.1 Acuerdo integro 60

9.16.2 Subrogación 60

9.16.3 Divisibilidad 60

9.16.4 Fuerza Mayor 60

9.17 Otras estipulaciones 61

RELACION DE TABLAS

Tabla 1 – Datos identificación DPC 13

Tabla 2 – Organización responsable 16

Tabla 3 – Definición extensión SubjectAltName 49

Tabla 4 – OID políticas de certificación 50

Tabla 5 – Perfil certificado 53

1. INTRODUCCIÓN

1.1 Resumen

El presente documento recoge la Política de Certificación correspondiente a los certificado emitidos por la Autoridad de Certificación (en adelante AC) SIA del tipo ciudadano, que define los mecanismos y procedimientos para la emisión, gestión, revocación, renovación y cualquier otro proceso que afecte al ciclo de vida de los certificados electrónicos emitidos por la AC de SIA. La Política de Certificación (en adelante PC) de SIA se ha estructurado conforme al documento RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". A fin de dotar de un carácter uniforme al documento y facilitar su lectura y análisis, se incluyen todas las secciones establecidas en la RFC-3647. Cuando no se haya previsto nada en alguna sección aparecerá la frase "No Estipulado" o "No Aplica".

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 ciudadano son certificados reconocidos de persona física según la Ley 59/2003 de firma electrónica que se expiden al público y permiten a las personas físicas relacionarse telemáticamente con entidades e instituciones públicas y privadas que admitan su uso.

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

Asimismo, los certificados cumplen las especificaciones técnicas en materia de certificados reconocidos, en concreto:

- ETSI TS 101 862: Qualified Certificate Profile.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.
- ETSI TS 102 280: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.

Los Certificados reconocidos de ciudadano solo pueden ser utilizados por el propio ciudadano. La emisión de estos certificados se realizará en soporte software.

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

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

1.2 Nombre del documento e identificación

Nombre del documento	Política de Certificación de certificado reconocido de ciudadano.
Versión del documento	1.0
Estado del documento	Vigente
Fecha de emisión	30/01/2015
Fecha de caducidad	No aplicable
OID	1.3.6.1.4.1.39131.10.1.3
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

1.3 Entidades y personas intervinientes

Las entidades y personas intervinientes son:

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

1.3.1 Autoridad de Certificación

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

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 para terceros, en este caso, la emisión de Certificado reconocido de ciudadano.

1.3.2 Autoridades de Registro

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

Cada entidad que actúe como AR establecerá:

- Los mecanismos y procedimientos necesarios para realizar la identificación y autenticación del firmante, cumpliendo con lo estipulado en la DPC.
- Los dispositivos de creación de firma a utilizar, que previamente SIA haya homologado.

1.3.3 Firmante

Se entienden por firmante de los certificados las personas físicas titulares que hagan uso de los servicios de emisión y gestión de los certificados así como de los certificados mismos.

1.3.4 Terceras Partes Aceptantes

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.

1.3.5 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.

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

1.4.2 Limitaciones y restricciones en el uso de los certificados

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

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

1.5 Administración de Políticas

1.5.1 Organización responsable

Esta PC es propiedad de SIA.

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

Tabla 2 – Organización responsable

1.5.2 Persona de contacto

Según lo especificado en la DPC de SIA.

1.5.3 Responsables de adecuación de la PC

Según lo especificado en la DPC de SIA.

1.5.4 Procedimientos de aprobación de esta PC

Según lo especificado en la DPC de SIA.

1.6 Definiciones y Acrónimos

1.6.1 Definiciones

En el ámbito de esta PC se utilizan las siguientes definiciones:

En el ámbito de esta PC se utilizan las siguientes definiciones:

• **Autoridad de Certificación (AC):** la Autoridad de Certificación es la entidad que emitirá, a petición de la Autoridad de Registro, los Certificados que se precisen, de forma automatizada y previa confirmación de la Autoridad de Registro.

• **Autoridad de Registro (AR):** la autoridad de registro es la entidad encargada de gestionar el alta (así como las revocaciones y bajas) de los usuarios en una infraestructura de clave pública. El usuario se debe dirigir a la autoridad de registro para solicitar un certificado de clave pública con la garantía de la autoridad certificadora asociada a la autoridad de registro.

En definitiva, realiza las tareas de identificación de los solicitantes, comprobación de la documentación acreditativa de las circunstancias que constan en los certificados así como la validación y aprobación de las solicitudes de emisión, revocación y renovación de los certificados.

• **Certificado Electrónico:** es un documento electrónico firmado electrónicamente por un Prestador de Servicios de Certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

• **Certificado reconocido:** certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone la Ley 59/2003, de 19 de diciembre, de firma electrónica.

• **Confidencialidad:** la confidencialidad es la capacidad de mantener un documento electrónico inaccesible a todos los usuarios, salvo a una determinada lista de personas. De este modo, podemos conseguir que las comunicaciones no sean escuchadas por otros y enviar documentos que solo puedan ser leídos por el destinatario indicado.

• **Criptografía:** la criptografía es una rama de las Matemáticas que estudia la transformación de información legible en información que no se puede leer directamente, es decir, que tiene que ser descifrada para ser leída.

• **Datos de creación de firma (Clave Privada):** datos únicos, como códigos o claves criptográficas privadas que el firmante utiliza para crear la firma electrónica.

• **Datos de Verificación de firma (Clave Pública):** Datos como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

• **Declaración de Prácticas de Certificación (DPC):** declaración que SIA pone a disposición del público de manera fácilmente accesible, por vía electrónica y de forma gratuita.

La DPC tendrá la consideración de documento de seguridad en el que se detallarán, en el marco de la Ley 59/2003 de firma electrónica y de sus disposiciones de desarrollo, las obligaciones que los Prestadores de Servicios de Certificación se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los

certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

• **Dispositivo de creación de firma:** programa o sistema informático que sirve para aplicar los datos de creación de firma.

Dispositivo Seguro de creación de firma: es el dispositivo que sirve para aplicar los datos de creación de firma, que se alinea a los requisitos establecidos en las normas específicas de aplicación en España, así como las recogidas en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se instaura un marco común para la firma electrónica.

• **Firma electrónica:** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

• **Firma electrónica avanzada:** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

• **Firma electrónica reconocida:** se considera firma electrónica reconocida, la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

• **Firmante:** es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

• **Solicitante del certificado:** es aquella persona que, en su propio nombre o en nombre de una organización, solicita la emisión de un certificado.

• **Poseedores de claves:** son las personas físicas que poseen o responden de la custodia de las claves de firma digital.

• **Terceros que confían en terceros:** son las personas físicas o jurídicas que reciben certificados expedidos por SIA. Son terceros que confían en certificados y, como tales, les es de aplicación lo establecido por la Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados.

• **Función hash:** es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

• **Hash o huella digital:** resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que se encuentra asociado unívocamente a los datos iniciales.

• **HSM (Módulo de seguridad criptográfico):** es un dispositivo de seguridad que genera y protege claves criptográficas.

• **Infraestructura de Claves Públicas (PKI, Public Key Infrastructure):** una PKI determina qué entidades entran a formar parte del sistema de certificación, qué papel juegan dichas entidades, qué normas y protocolos se deben seguir para

poder operar dentro del sistema, cómo se codifica y se transmite la información digital, y qué información contendrán los objetos y documentos gestionados por la infraestructura. Todo esto basado en la tecnología de Clave Pública (dos claves).

• **Lista de Certificados Revocados (CRL):** es aquella lista donde figura la relación de certificados revocados que SIA emite desde el momento en que se produce una revocación con carácter inmediato.

• **Número de serie del Certificado:** es un valor entero y único asociado inequívocamente con un certificado expedido por cualquier Prestador de Servicios de Certificación.

• **OCSP (Online Certificate Status Protocol):** es un protocolo informático que permite la comprobación de la vigencia de un certificado electrónico.

• **OID (Object Identifier):** valor que comprende una secuencia de componentes variables constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que poseen la propiedad de ser únicos entre el resto de OID.

• **PKCS (Public-Key Cryptography Standards):** es el estándar de facto más popular para codificar los diferentes tipos de información, como certificados o archivos firmados. Los programadores o analistas se refieren a estas convenciones o estándares como “formatos” o “lay-out”. PKCS responde a “Public Key Cryptography Standards”.

• **PKCS#10 (Certification Request Syntax Standard):** estándar de facto para solicitud de certificación. Define el formato de los mensajes enviados a una Autoridad de Certificación para solicitar la certificación de una clave pública.

• **PKCS #12 (Personal Information Exchange Syntax Standard):** estándar de facto para sintaxis de intercambio de información personal. Define un formato de fichero usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

• **Política de Certificación:** es un documento anexo a la Declaración de Prácticas de Certificación que recoge el ámbito de aplicación, los caracteres técnicos de los diferentes tipos de certificados, el conjunto de reglas que indican los procedimientos seguidos en la prestación de servicios de certificación, así como sus condiciones de uso.

• **Prestador de Servicios de Certificación (PSC):** es la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

1.6.2 Acrónimos

En el ámbito de esta PC se utilizan los siguientes acrónimos:

AC: Autoridad de Certificación.

AR: Autoridad de Registro.

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CDP: CRL Distribution Point (Punto de Distribución de CRLs).

CEN: Comité Europeo de Normalización.

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CRL: Certificate Revocation List (Lista de Revocación de Certificados).

CWA: CEN Workshop Agreement.

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.

DPC: Declaración de Prácticas de Certificación.

ETSI: European Telecommunications Standard Institute.

FIPS: Federal Information Processing Standard (Estándar USA de procesado de información).

HSM: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.

IETF: Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet).

LDAP: Lightweight Directory Access Protocol (Protocolo de acceso a servicios de directorio).

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.

O: Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

OCSP: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.

OID: Object identifier (Identificador de objeto único).

OU: Organizacional Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

PC: Política de Certificación.

PKCS: Public Key Infrastructure Standards. Estándares de PKI desarrollados por "RSA Laboratories" y aceptados internacionalmente.

PKI: Public Key Infrastructure (Infraestructura de Clave Pública).

PKIX: Grupo de trabajo dentro del IETF (Internet Engineering Task Group) constituido con el objeto de desarrollar las especificaciones relacionadas con PKI e Internet.

PSC: Prestador de Servicios de Certificación.

RFC: Request For Comments (recomendación emitida por la IETF).

2. REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1 Repositorios

Según lo especificado en la DPC de SIA.

2.2 Publicación de información de certificación

Según lo especificado en la DPC de SIA.

2.3 Temporalidad o frecuencia de publicación

Según lo especificado en la DPC de SIA.

2.4 Controles de acceso a los repositorios

Según lo especificado en la DPC de SIA.

3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS TITULARES DE CERTIFICADOS

3.1 Nombres

3.1.1 Tipos de nombres

Según lo especificado en la DPC de SIA.

3.1.2 Necesidad de que los nombres sean significativos

Según lo especificado en la DPC de SIA.

3.1.3 Uso de seudónimos

No se permite la utilización de seudónimos en ningún caso.

3.1.4 Reglas para interpretar varios formatos de nombres

Según lo especificado en la DPC de SIA.

3.1.5 Unicidad de los nombres

Según lo especificado en la DPC de SIA.

3.1.6 Procedimientos de resolución de conflictos sobre nombres

Según lo especificado en la DPC de SIA.

3.1.7 Reconocimiento, autenticación y papel de las marcas registradas

Según lo especificado en la DPC de SIA.

3.2 Validación de la identidad inicial

3.2.1 Métodos para probar la posesión de la clave privada

El par de claves de los Certificados reconocidos de ciudadanos los genera el solicitante, una vez se ha personado, ha sido validado por la Autoridad de Registro y ha firmado el contrato de vinculación.

El par de claves es generado por el ciudadano y la demostración de posesión de la clave privada consiste en la utilización del certificado. En el proceso de registro, el método para probar la posesión de la clave privada por el solicitante será la entrega de un PKCS#10 o una prueba equivalente.

3.2.2 Autenticación de la identidad de una persona jurídica

No estipulado.

3.2.3 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 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.

El régimen de personación en la solicitud de certificados podrá no ser exigible cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya a la AR en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados anteriormente y el período de tiempo transcurrido desde la identificación es menor de cinco (5) años.

3.2.4 Información no verificada sobre el solicitante

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

3.2.5 Comprobación de las facultades de representación

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

3.3 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.

4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 Solicitud de certificados

SIA solo admite solicitudes de emisión de certificado tramitados por una persona física mayor de edad, con capacidad plena de obrar y con capacidad jurídica suficiente.

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

4.2 Tramitación de las solicitudes de certificados

Compete a la Autoridad de Registro la comprobación de la identidad del solicitante, la verificación de la documentación y la constatación de que el solicitante ha firmado “el documento de comparecencia”. Una vez completa la solicitud, la Autoridad de Registro, la remitirá al Prestador de Servicios de Certificación.

4.3 Emisión de certificados

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

El proceso de emisión se realizará en los siguientes pasos:

1. La AR verificará la identidad del solicitante y los datos que se incluyan en el certificado.
2. La AR entregará al solicitante unos códigos de emisión del certificado que podrán ser usados en la web del prestador para completar el proceso de emisión.
3. El solicitante procede a generar el par de claves en soporte software en su ordenador siguiendo las instrucciones indicadas por la AR.
4. El solicitante introduce los códigos de emisión y se envía la petición de generación de certificado a la AC.
5. Generación del certificado asociado a las claves generadas, y confirmación al solicitante de la generación de las mismas tras el proceso satisfactorio.
6. El solicitante descarga de forma segura el certificado en su ordenador.

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

4.4 Aceptación del certificado

4.4.1 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 el certificado este en posesión del firmante.

Como evidencia de la aceptación deberá quedar una hoja de aceptación firmada por el firmante. El certificado se considera válido a partir de la fecha en que se firmó la hoja de aceptación.

4.4.2 Publicación del certificado por la AC

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

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

No se efectúan notificaciones a terceros.

4.5 Par de claves y uso del certificado

4.5.1 Uso de la clave privada del certificados por el titular

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta PC y de acuerdo con lo establecido en las extensiones “Key Usage” y “Extended Key Usage” del certificado.

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

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

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

4.5.2 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.

4.6 Renovación de certificados sin cambio de claves

4.6.1 Circunstancias para la renovación de certificados sin cambio de claves

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

4.7 Renovación de certificados con cambio de claves

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

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

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

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

4.7.2 Quien puede pedir la renovación de un certificado

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

4.7.3 Tramitación de las peticiones de renovación con cambio de claves

De forma automatizada, la AC informará al firmante de que su certificado está próximo a expirar. Para la renovación del mismo, aparecen dos formas de proceder:

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

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

4.7.4 Notificación de la emisión de nuevos certificados al titular

Al tratarse de una renovación de certificados con cambio de claves, siguiendo el proceso de emisión de certificados como si del proceso inicial se tratara, una vez generado éste satisfactoriamente, se le notificará al firmante.

4.7.5 Forma de aceptación del certificado con nuevas claves

El titular confirmará electrónicamente la aceptación del certificado.

4.7.6 Publicación del certificado con las nuevas claves por la AC

El certificado reconocido de ciudadano no se publicará.

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

No se efectúan notificaciones a terceros.

4.8 Modificación de certificados

4.8.1 Causas para la modificación de un certificado

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

En consecuencia, no se recogen el resto de puntos del apartado 4.8 que establece la RFC 3647, lo que implica, a efectos de esta PC su no estipulación.

4.9 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.

4.9.1 Causas para la revocación

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

4.9.2 Quien puede solicitar la revocación

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

- El titular a nombre del cual fue expedido el certificado.
- La Entidad de Registro que intervino en la emisión.
- La propia AC de SIA cuando tenga conocimiento de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de esta DPC.

4.9.3 Procedimiento de solicitud de revocación

Según lo especificado en la DPC de SIA.

4.9.4 Periodo de gracia de la solicitud de revocación

Según lo especificado en la DPC de SIA.

4.9.5 Plazo en que la AC debe resolver la solicitud de revocación

Según lo especificado en la DPC de SIA.

4.9.6 Requisitos de verificación de las revocaciones por los terceros aceptantes

Según lo especificado en la DPC de SIA.

4.9.7 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 ciudadano.

4.9.8 Tiempo máximo entre la generación y la publicación de las CRLs

Según lo especificado en la DPC de SIA.

4.9.9 Disponibilidad de un sistema en línea de verificación del estado de los certificados

Según lo especificado en la DPC de SIA.

4.9.10 Requisitos de comprobación en línea de la 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.

Este tipo de certificado no tiene previsto un servicio de validación de certificados mediante el protocolo OCSP.

4.9.11 Otras formas de divulgación de información de revocación

Este tipo de certificado no tiene previsto un servicio de validación de certificados mediante el protocolo OCSP.

4.9.12 Requisitos especiales de renovación de claves comprometidas

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

4.9.13 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.

4.9.14 Quien puede solicitar la suspensión

No aplica.

4.9.15 Procedimiento para la solicitud de suspensión

No aplica.

4.9.16 Límites del periodo de suspensión

No aplica.

4.10 Servicios de información del estado de certificados

4.10.1 Características operativas

SIA ofrece un servicio gratuito de publicación en la web de Listas de Certificados Revocados (CRL) sin restricciones de acceso.

4.10.2 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.

4.10.3 Características adicionales

No aplica.

4.11 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.

4.12 Custodia y recuperación de claves

4.12.1 Prácticas y políticas de custodia y recuperación de claves

El PSC en ningún momento custodiará ni copiará la clave privada emitida a los ciudadanos. Por lo tanto el PSC en ningún momento podrá recuperar la clave de los usuarios. En caso de pérdida de la misma, se deberá revocar el certificado y emitir uno nuevo.

4.12.2 Prácticas y políticas de protección y recuperación de la clave de sesión

No estipulado.

5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y DE OPERACIONES

5.1 Controles de seguridad física

5.1.1 Ubicación física y construcción

Según lo estipulado en la DPC de SIA.

5.1.2 Acceso físico

Según lo estipulado en la DPC de SIA.

5.1.3 Alimentación eléctrica y aire acondicionado

Según lo estipulado en la DPC de SIA.

5.1.4 Exposición al agua

Según lo estipulado en la DPC de SIA.

5.1.5 Protección y prevención de incendios

Según lo estipulado en la DPC de SIA.

5.1.6 Sistema de almacenamiento

Según lo estipulado en la DPC de SIA.

5.1.7 Eliminación de los soportes de información

Según lo estipulado en la DPC de SIA.

5.1.8 Copias de seguridad fuera de las instalaciones

Según lo estipulado en la DPC de SIA.

5.2 Controles de Procedimiento

5.2.1 Roles responsables del control y gestión

Según lo estipulado en la DPC de SIA.

5.2.2 Número de personas requeridas por tarea

Según lo estipulado en la DPC de SIA.

5.2.3 Identificación y autenticación para cada usuario

Según lo estipulado en la DPC de SIA.

5.2.4 Roles que requieren segregación de funciones

Según lo estipulado en la DPC de SIA.

5.3 Controles de Personal

5.3.1 Requisitos relativos a la cualificación, conocimiento y experiencia profesionales

Según lo estipulado en la DPC de SIA.

5.3.2 Procedimientos de comprobación de antecedentes

Según lo estipulado en la DPC de SIA.

5.3.3 Requerimientos de formación

Según lo estipulado en la DPC de SIA.

5.3.4 Requerimientos de frecuencia de actualización de la información

Según lo estipulado en la DPC de SIA.

5.3.5 Frecuencia y secuencia de rotación de tareas

Según lo estipulado en la DPC de SIA.

5.3.6 Sanciones por actuaciones no autorizadas

Según lo estipulado en la DPC de SIA.

5.3.7 Requisitos de contratación de terceros

Según lo estipulado en la DPC de SIA.

5.3.8 Documentación proporcionada al personal

Según lo estipulado en la DPC de SIA.

5.4 Procedimientos de auditoria de seguridad

5.4.1 Tipos de eventos registrados

Según lo estipulado en la DPC de SIA.

5.4.2 Frecuencia de procesado de registros de auditoria

Según lo estipulado en la DPC de SIA.

5.4.3 Periodo de conservación de los registros de auditoria

Según lo estipulado en la DPC de SIA.

5.4.4 Protección de los registros de auditoria

Según lo estipulado en la DPC de SIA.

5.4.5 Procedimientos de respaldo de los registros de auditoria

Según lo estipulado en la DPC de SIA.

5.4.6 Sistema de recogida de información de auditoria

Según lo estipulado en la DPC de SIA.

5.4.7 Notificación al sujeto causa del evento

Según lo estipulado en la DPC de SIA.

5.4.8 Análisis de vulnerabilidades

Según lo estipulado en la DPC de SIA.

5.5 Archivo de registros

5.5.1 Tipos de eventos archivados

Según lo estipulado en la DPC de SIA.

5.5.2 Periodo de conservación de registros

Según lo estipulado en la DPC de SIA.

5.5.3 Protección del archivo

Según lo estipulado en la DPC de SIA.

5.5.4 Procedimientos de copia de respaldo del archivo

Según lo estipulado en la DPC de SIA.

5.5.5 Requerimientos para el sellado de tiempo de los registros

Según lo estipulado en la DPC de SIA.

5.5.6 Sistema de archivo de información de auditoría

Según lo estipulado en la DPC de SIA.

5.5.7 Procedimientos para obtener y verificar información archivada

Según lo estipulado en la DPC de SIA.

5.6 Cambio de claves de una AC

Según lo estipulado en la DPC de SIA.

5.7 Recuperación en casos de vulneración de una clave y de desastre natural u otro tipo de catástrofe

5.7.1 Procedimientos de gestión de incidentes y vulnerabilidades

Según lo estipulado en la DPC de SIA.

5.7.2 Alteración de los recursos hardware, software y/o datos

Según lo estipulado en la DPC de SIA.

5.7.3 Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad

Según lo estipulado en la DPC de SIA.

5.7.4 Continuidad de negocio después de un desastre natural u otro tipo de catástrofe

Según lo estipulado en la DPC de SIA.

5.8 Cese de una AC o AR

5.8.1 Autoridad de Certificación

Según lo estipulado en la DPC de SIA.

5.8.2 Autoridad de Registro

Según lo estipulado en la DPC de SIA.

6. 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.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Los pares de claves para los certificados emitidos bajo el ámbito de la presente Política de Certificación se generan en soporte software, normalmente el propio navegador del usuario. Las claves privadas se generan en el dispositivo software del firmante.

6.1.2 Entrega de la clave privada al titular

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

La clave privada se genera en un dispositivo en posesión del firmante y, por lo tanto, no existe ninguna entrega de la clave privada al titular.

6.1.3 Entrega de la clave pública al emisor del certificado

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

6.1.4 Entrega de la clave pública de la AC a los terceros aceptantes

Según lo especificado en la DPC de SIA.

6.1.5 Tamaño de las claves

El tamaño de las claves de los certificados reconocidos de ciudadano es de 2048 bits.

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

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

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

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

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

Key Usage:

- nonRepudiation
- Digital Signature
- Key Encipherment

6.2 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.

6.2.1 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.

6.2.2 Control multi-persona (n de m) de la clave privada

Las claves privadas generadas para los certificados emitidos bajo el ámbito de la presente Política de Certificación se encuentran bajo el control exclusivo de los firmantes. No está estipulado que exista control multi-persona para las claves privadas asociadas a los certificados de esta política.

6.2.3 Custodia de la clave privada

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

6.2.4 Copia de seguridad de la clave privada

Bajo ningún concepto, SIA copiará las claves privadas de firma de los firmantes de los certificados definidos por la presente política.

El firmante puede exportar sus claves privadas mediante formato PKCS#12 a un fichero protegido con una contraseña seleccionada por él. En cualquier caso, es responsabilidad del firmante la conservación de sus datos de creación de firma y asegurar su confidencialidad y la protección de todo acceso o revelación.

6.2.5 Archivo de la clave privada

Las claves privadas de los certificados reconocidos de los firmantes nunca serán archivadas por la AC.

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

La generación de las claves vinculadas al certificado reconocido de ciudadano se realiza en el propio dispositivo software del equipo del usuario. Se puede utilizar un fichero en formato PKCS#12 para transferir la clave privada a otro módulo criptográfico, pero la responsabilidad de proteger este fichero y esta operación es del propio usuario.

6.2.7 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.

6.2.8 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.

6.2.9 Método de desactivación de la clave privada

La desactivación se realizará cuando el firmante cierre la aplicación software de creación de firma o el módulo criptográfico asociado.

6.2.10 Método de destrucción de la clave privada

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

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

6.2.11 Clasificación de los módulos criptográficos

Según lo estipulado en la DPC.

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

Según lo estipulado en la DPC de SIA.

6.3.2 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.

6.4 Datos de activación

6.4.1 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.

6.4.2 Protección de los datos de activación

El propio firmante generará el par de claves en el dispositivo software. Por lo tanto, el firmante es el responsable de la protección de los datos de activación de su clave privada. SIA recomienda una contraseña o PIN para el acceso a la clave privada y requerida para el proceso de firma, pero se deja a discreción de los usuarios.

6.4.3 Otros aspectos de los datos de activación

No aplica.

6.5 Controles de seguridad informática

Según lo estipulado en la DPC de SIA.

6.6 Controles de seguridad del ciclo de vida

Según lo estipulado en la DPC de SIA.

6.7 Controles de seguridad de la red

Según lo estipulado en la DPC de SIA.

6.8 Fuentes de tiempo

Según lo estipulado en la DPC de SIA.

7. PERFILES DE LOS CERTIFICADOS, CRL Y OCSP

7.1 Perfil de certificado

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

- ETSI TS 101 862 "Qualified Certificate profile".
- RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and CRL Profile".
- RFC 3739 "Internet x509 Public Key Infrastructure. Qualified Certificates Profile".
- Perfiles de Certificados Electrónicos para la Administración General del Estado según Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos Los perfiles están definidos en el Anexo II de la Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente.
- ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

7.1.1 Número de versión

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

7.1.2 Extensiones del certificado

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

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

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

Las extensiones utilizadas en los certificados son:

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

Los certificados emitidos con la consideración de reconocidos incorporan adicionalmente el identificador de objeto (OID) definido por el TS 101 862, sobre perfiles de certificados reconocidos: 0.4.0.1862.1.1.

Los certificados que son expedidos con la calificación de reconocidos están identificados en la extensión QcStatements con OID 1.3.6.1.5.5.7.1.3, que indica la existencia de una lista de declaraciones "QcStatementes", conforme a la especificación técnica TS 101 862, concretamente los certificados reconocidos de ciudadano 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.

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

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

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

OID	Concepto	Descripción
1.3.6.1.4.1.39131.10.2.1	Tipo de certificado	Tipo de certificado

1.3.6.1.4.1.39131.10.2.2	Nombre	Nombre del usuario
1.3.6.1.4.1.39131.10.2.3	Apellido1	Primer apellido del usuario
1.3.6.1.4.1.39131.10.2.4	Apellido2	Segundo apellido del usuario
1.3.6.1.4.1.39131.10.2.5	DNI	DNI del usuario

Tabla 3 – Definición extensión SubjectAltName

7.1.3 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).

7.1.4 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.

7.1.5 Restricciones de nombre

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

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

- CN, GN, SN, SerialNumber, C

Los atributos CN (Common Name), GN (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
- GN = Nombre
- SN = Apellido1
- SerialNumber = DNI con el formato NNNNNNNNA

- C = País del ciudadano. En este caso, España. El atributo "C" (country) se codificará de acuerdo a "ISO 3166-1-alpha-2 code elements", en PrintableString.

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

El OID de la presente PC es 1.3.6.1.4.1.39131.10.1.3. Los identificadores de los certificados expedidos bajo la presenta Política de Certificación son los siguientes:

Política de Certificados de Ciudadano	1.3.6.1.4.1.39131.10.1.3

Tabla 4 – OID políticas de certificación

7.1.7 Uso de la extensión "PolicyConstraints"

No estipulado.

7.1.8 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.

7.1.9 Tratamiento semántico para la extensión "Certificate Policy"

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

7.2 Perfil de Certificado de Ciudadano

Certificado reconocido de ciudadano		
Nombre atributo	**Valor**	**Observaciones**
Campos x509 v1		
Versión	V3	
Serial Number	Número secuencial único, asignado automáticamente por la AC subordinada emisora	
Signature Algorithm	SHA-256 con RSA-2048	
Issuer Distinguished Name (Emisor)		
Country (C)	ES	
Organization (O)	SISTEMAS INFORMATICOS ABIERTOS SOCIEDAD ANONIMA	
Organizational Unit (OU)	QUALIFIED CA	
Serial Number (serialNumber)	A82733262	
Common Name (CN)	SIA SUB01	
Validity		
Not Before	Fecha de emisión del certificado	
Not After	Fecha de emisión + 3 años	
Subject (Asunto)		
Country (C)	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>	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	**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		
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-calssuers	
Access Method	https://psc.sia.es/ac_sub01.crt	
Qualified Certificate Statements		
QcCompliance	OID 0.4.0.1862.1.1	Certificado reconocido
QcEuRetentionPeriod	15 años	Duración custodia
Certificate Policies		
Policy Identifier	1.3.6.1.4.1.39131.10.1.3	
Policy Qualifier ID	Especificación de la DPC	
CPS Pointer	https://psc.sia.es/	
User Notice	“Certificado reconocido de Ciudadano. 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		
Tipo del certificado	OID: 1.3.6.1.4.1.39131.10.2.1: CIUDADANO	
Nombre	OID: 1.3.6.1.4.1.39131.10.2.2: <Nombre>	Nombre del usuario
Primer apellido	OID: 1.3.6.1.4.1.39131.10.2.3: <Apellido1>	Primer apellido del

		usuario
Segundo apellido	OID: 1.3.6.1.4.1.39131.10.2.4: <Apellido2>	Segundo apellido del usuario
DNI	OID: 1.3.6.1.4.1.39131.10.2.5: <DNI>	DNI del usuario

Tabla 5 – Perfil certificado

7.3 Perfil de CRL

Según lo estipulado en la DPC de SIA.

8. AUDITORÍAS DE CUMPLIMIENTO Y OTROS CONTROLES

8.1 Frecuencia o circunstancias de los controles para cada autoridad

Según lo estipulado en la DPC de SIA.

8.2 Identificación / cualificación del auditor

Según lo estipulado en la DPC de SIA.

8.3 Relación entre el auditor y la Autoridad auditada

Según lo estipulado en la DPC de SIA.

8.4 Aspectos cubiertos por los controles

Según lo estipulado en la DPC de SIA.

8.5 Acciones a emprender como resultado de la detección de deficiencias

Según lo estipulado en la DPC de SIA.

8.6 Comunicación de resultados

Según lo estipulado en la DPC de SIA.

9. OTRAS CUESTIONES LEGALES Y DE ACTIVIDAD

9.1 Tarifas

9.1.1 Tarifas de emisión de certificado o renovación

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

9.1.2 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.

9.1.3 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.

9.1.4 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.

9.1.5 Política de reembolso

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

9.2 Responsabilidad Financiera

9.2.1 Seguro de responsabilidad civil

Según lo estipulado en la DPC de SIA.

9.3 Confidencialidad de la información

Según lo estipulado en la DPC de SIA.

9.3.1 Ámbito de la información confidencial

Según lo estipulado en la DPC de SIA.

9.3.2 Información no confidencial

Según lo estipulado en la DPC de SIA.

9.3.3 Deber de secreto profesional

Según lo estipulado en la DPC de SIA.

9.4 Protección de datos personales

Según lo estipulado en la DPC de SIA.

9.5 Derechos de propiedad Intelectual

Según lo estipulado en la DPC de SIA.

9.6 Obligaciones

9.6.1 Obligaciones de la AC

Según lo estipulado en la DPC de SIA.

9.6.2 Obligaciones de la AR

Según lo estipulado en la DPC de SIA.

9.6.3 Obligaciones de los firmantes

Según lo estipulado en la DPC de SIA.

9.6.4 Obligaciones de los terceros aceptantes

Según lo estipulado en la DPC de SIA.

9.6.5 Obligaciones de otros participantes

Según lo estipulado en la DPC de SIA.

9.7 Renuncias de garantías

Según lo estipulado en la DPC de SIA.

9.8 Limitaciones de responsabilidad

Según lo estipulado en la DPC de SIA.

9.9 Responsabilidades

9.9.1 Limitaciones de responsabilidades

Según lo estipulado en la DPC de SIA.

9.9.2 Responsabilidades de la Autoridad de Certificación

Según lo estipulado en la DPC de SIA.

9.9.3 Responsabilidades de la Autoridad de Registro

Según lo estipulado en la DPC de SIA.

9.9.4 Responsabilidad del titular

Según lo estipulado en la DPC de SIA.

9.9.5 Delimitación de responsabilidades

Según lo estipulado en la DPC de SIA.

9.9.6 Alcance de la cobertura

Según lo estipulado en la DPC de SIA.

9.9.7 Cobertura de seguro u otras garantías para los terceros aceptantes

Según lo estipulado en la DPC de SIA.

9.10 Limitaciones de pérdidas

Según lo estipulado en la DPC de SIA.

9.11 Periodo de validez

9.11.1 Plazo

Según lo estipulado en la DPC de SIA.

9.11.2 Sustitución y derogación de la DPC

Según lo estipulado en la DPC de SIA.

9.11.3 Efectos de finalización

Según lo estipulado en la DPC de SIA.

9.12 Notificaciones individuales y comunicaciones con participantes

Según lo estipulado en la DPC de SIA.

9.13 Reclamaciones y jurisdicción

Según lo estipulado en la DPC de SIA.

9.14 Legislación aplicable

Según lo estipulado en la DPC de SIA.

9.15 Conformidad con la Ley aplicable

Según lo estipulado en la DPC de SIA.

9.16 Clausulas diversas

9.16.1 Acuerdo integro

Según lo estipulado en la DPC de SIA.

9.16.2 Subrogación

Según lo estipulado en la DPC de SIA.

9.16.3 Divisibilidad

Según lo estipulado en la DPC de SIA.

9.16.4 Fuerza Mayor

Según lo estipulado en la DPC de SIA.

9.17 Otras estipulaciones

No se contemplan.