Declaración de Practicas de Certificación

OID 2.16.724.4.8.10.60.1

Tabla de contenidos

1 INTRODUCCION

El SESCAM pretende ser una organización de servicios sanitarios públicos moderna y de vanguardia, que se caracterice por la innovación y la calidad del servicio global (medicina, enfermería, servicios auxiliares, etc), por la precisión en el diagnóstico y en el tratamiento, su seguridad, cercanía y agilidad. Sus servicios deben procurar el confort de los usuarios, prestando una atención personalizada que garantice la privacidad y confidencialidad. Debe posibilitar tanto la participación social como la de los profesionales, facilitando la atención y el trato adecuados a los proveedores.

La Atención Sanitaria, el contenido esencial del trabajo del SESCAM, es un servicio complejo (diagnóstico, pronóstico, tratamiento), que requiere profesionales bien formados, medios suficientes, y una adecuada organización, dicha atención además requiere de garantías de seguridad en la ejecución de los procedimientos y acciones realizadas por sus profesionales, dichas acciones deben garantizar el control de acceso a la información, su confidencialidad, integridad y el no-repudio.

En tal sentido, uno de los objetivos del SESCAM es dotar a los servicios y profesionales sanitarios de las herramientas adecuadas para agilizar y facilitar su trabajo y por ende el servicio prestado a los ciudadanos de Castilla la Mancha tal y como se desprende del derecho establecido por la Ley 11/2007 de acceso de los ciudadanos a la administración Electrónica.

El SESCAM siguiendo los principios a favor de un modelo de certificación que se encuentra expresamente inspirada por el artículo 4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, se constituye como un prestador de servicios de certificación, estableciendo entre los servicios a prestar la emisión de certificados requeridos por la Ley 11/2007 para:

- Sede electrónica
- Sello administrativo.
- Empleado Público.

La DPC no reconoce la atribución como "certificados reconocidos" a los certificados de autenticación y cifrado.

El modelo de certificación referido y por tanto la presente DPC ajusta su ámbito de actuación inicialmente al soporte necesario para la implantación de medidas de seguridad y firma electrónica avanzada y firma electrónica reconocida en el entorno operativo del SESCAM, las entidades dependientes de éste, y cualquier otra institución pública o privada.

La presente DPC describe los mecanismos establecidos para la adecuada y completa gestión del ciclo de vida de los certificados gestionados por el SESCAM, así como de los servicios avanzados de soporte a éstos que corresponden a los servicios de Sellado de Tiempo y de validación en línea de certificados.

1.1 Presentación

El presente documento constituye la Declaración de Practicas de Certificación, en adelante DPC, del SESCAM la cual ha sido redactada siguiendo las indicaciones y recomendaciones de la norma IETF RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".*

La presente DPC expone las normas y condiciones generales de los servicios de confianza prestados por el SESCAM, siendo éstos los siguientes:

- ***Servicio de Gestión de Certificados Reconocidos***, el SESCAM emite y gestiona certificados reconocidos de acuerdo con lo establecido en la legislación de firma electrónica vigente, Ley 59/2003, de 19 de diciembre de firma electrónica. Los certificados reconocidos además son conformes con la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.
- ***Servicios de Gestión de Certificados Ordinarios,*** el SESCAM emite certificados ordinarios sin la consideración legal de certificados reconocidos, éste tipo de certificados están orientados a prestar servicios de distinta índole, tales como: autenticación –de cliente o servidor en el establecimiento de comunicaciones-, cifrado, actuación administrativa de declaración de conocimiento, etc.
- ***Servicio de Verificación On-line,*** que permite a terceros comprobar el estado de los certificados en línea mediante la utilización del protocolo IETF RFC 2560 OCSP (Online Certificate Status Protocol), tanto de los certificados emitidos por el SESCAM como por los de aquellos prestadores que hayan llegado a un acuerdo de cooperación mutua con el éste.
- **Servicio de Sellado de Tiempo**, por la cual una entidad consumidora podrá obtener garantía referente a que cierta información existía en un momento concreto del tiempo.

1.2 Identificación

La presente Declaración de Practicas de Certificación del SESCAM se identifica de la siguiente forma:

Nombre del Documento	Declaración de Prácticas de Certificación del SESCAM
Versión	2.1
Estado del Documento	APROBADO
OID de la DPC	2.16.724.4.8.10.60.1
Fecha de creación	29 de Febrero de 2010
Fecha de Caducidad	No aplicable
Localización	http://sescam.jccm.es/pki/dpc/dpcv2.html.

Con el objeto de identificar de forma individual, cada política y tipo de certificado emitido por el SESCAM de acuerdo con la presente Declaración de Prácticas de Certificación, se asigna un identificador de objeto (OID) a cada uno, que aparecerá en la extensión correspondiente de cada certificado emitido.

La división que se ha realizado corresponde al tipo de entidad certificada por el SESCAM, la primera de las clase contemplada refiere a las políticas de certificación de los Servicios de Confianza de valor añadido, esto es: la AST (Autoridad de Sellado de Tiempo) y la AV (Autoridad de Validación).

Clase de Certificado	Política de Certificado	OID Asignado
Certificados de Servicios de Confianza	Política de Autoridad de Sellado de Tiempo	2.16.724.4.8.10.60.10.1.1
	Política de Autoridad de Validación	2.16.724.4.8.10.60.10.1.2

En segundo término se han considerado las políticas de certificación requeridas por la Ley 11/2007 y establecidas en el documento "Esquema de Identificación y firma electrónica de las Administraciones Públicas". En concreto se han considerado los siguientes certificados:

- Empleado Público previsto en el artículo 19 de la Ley 11/2007
- Certificado de sede electrónica administrativa según lo previsto en el artículo 17 de la Ley 11/2007.

- Certificado de Sello Electrónico para la actuación automatizada de la Administración Pública, órgano o entidad de derecho público según lo previsto en el artículo 18 de la Ley 11/2007.

A continuación se detallan los OIDs asignados a cada una de las políticas de susodichas clase de certificados:

Clase de Certificado	Política de Certificado	Nivel	OID Asignado
Certificados de Empleado Público	Autenticación	Alto	2.16.724.4.8.10.60.10.2.1.1.1
		Medio	2.16.724.4.8.10.60.10.2.1.2.1
	No Repudio	Alto	2.16.724.4.8.10.60.10.2.1.1.2
		Medio	2.16.724.4.8.10.60.10.2.1.2.2
	Cifrado	Alto	2.16.724.4.8.10.60.10.2.1.1.3
		Medio	2.16.724.4.8.10.60.10.2.1.2.3
Certificados Administrativos	Sede	Alto	2.16.724.4.8.10.60.10.3.1.1
		Medio	2.16.724.4.8.10.60.10.3.1.2
	Sello	Alto	2.16.724.4.8.10.60.10.3.2.1
		No	2.16.724.4.8.10.60.10.3.2.2

También se prevé la emisión de certificados de persona física, entendiendo éste como un certificado que se emite a una persona natural individual, bien a titulo estrictamente personal o indicando atributos adicionales, como ser miembro de un colectivo o trabajador de una empresa –por ejemplo, prestando una asistencia técnica al SESCAM-. Los tipos de certificados que el SESCAM emite de persona física son:

Clase de Certificado	Política de Certificado	Reconocido	OID Asignado
Certificados Persona física[1]	Autenticación	No	2.16.724.4.8.10.60.10.2.2.1
			1.3.6.1.4.1.21835.1.1.3.1

[1] *Se han reservado dos conjuntos de OIDs para este tipo de certificados, donde el arco 1.3.6.1.4.1.21835.1 corresponde a los certificados emitidos con anterioridad a la publicación de la presente política, y el nuevo arco 2.16.724.4.8.10.60.10.2.2 asignado por la presente DPC para este tipo de certificados de persona física.*

	Firma	Si	2.16.724.4.8.10.60.10.2.2.2
		No	1.3.6.1.4.1.21835.1.1.3.2
	Cifrado	No	2.16.724.4.8.10.60.10.2.2.3
			1.3.6.1.4.1.21835.1.1.3.3

Además el SESCAM emitirá los siguientes tipos de certificados de carácter técnico:

Clase de Certificado	Política de Certificado	OID Asignado
Certificados Dispositivos	Política de Dispositivo Físico de Servidor WEB	2.16.724.4.8.10.60.10.4.1
	Política de Aplicaciones	2.16.724.4.8.10.60.10.4.2
	Política de Controlador de dominio W2K	2.16.724.4.8.10.60.10.4.3
	Política de Firma de Código	2.16.724.4.8.10.60.10.4.4

Aquellos certificados emitidos como reconocidos incorporan además el identificador de política definido por el Instituto Europeo de Normas de Telecomunicación ETSI TS 101 862 sobre perfiles de certificados reconocidos, estos corresponden en principio únicamente a los certificados de No-Repudio para su utilización en procesos de firma electrónica reconocida según la Ley 59/2003.[2]

1.3 Comunidad de usuarios y aplicabilidad

Los servicios prestados por la PKI del SESCAM son apropiados para aquellas situaciones en donde las partes exigen garantías de autenticidad, no repudio y confidencialidad.

Esta Declaración de Prácticas de Certificación regula una comunidad de usuarios, que deben obtener certificados, de acuerdo con la Ley 11/2007, la Ley 59/2003 y la normativa administrativa correspondiente.

Los siguientes párrafos identifican tanto los componentes de la PKI como los perfiles de la comunidad de entidades involucradas en la gestión y mantenimiento de los certificados y claves. Los perfiles se describen en detalle en la sección 5.2.

[2] *Los certificados de Empleado Público de Autenticación son emitidos con el identificador de política de reconocidos por requerimiento de interoperabilidad de perfiles de certificados definidos dentro del ámbito del Esquema Nacional de Interoperabilidad, no obstante este tipo de certificados únicamente debe ser utilizado para procesos de autenticación.*

1.3.1 Autoridad de Aprobación de Políticas.

La Autoridad de Acreditación de Políticas de la Infraestructura de clave pública es la entidad responsable de aprobar la presente DPC, está compuesta por miembros del comité de seguridad del SESCAM y es la máxima y única autoridad responsable de garantizar la correcta aplicación de la presente DPC a los servicios de confianza del SESCAM.

1.3.2 Autoridad de Certificación

El SESCAM 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, garantizando la correspondencia entre los pares de claves de los subscritores con la identidad que éstos representan.

La jerarquía de la infraestructura de clave pública del SESCAM se compone de dos niveles representados por una Autoridad de Certificación Raíz que emitirá y gestionará certificados de la entidades de certificación secundarias o de producción, las cuales serán responsables de la emisión de certificados para entidades finales y para sus propias Autoridades de Registro además de las correspondientes Listas de Revocación.

En la actualidad el SESCAM opera únicamente una Autoridad de Certificación de Producción responsable de la emisión de certificados finales, así mismo opera una segunda Autoridad de Certificación de Producción con objeto de permitir la revocación de certificados y la publicación de CRLs para su anterior CA Subordinada, sustiuoda por la más reciente para ser plenamente conformes a los perfiles definidos por el documento "Esquema de Identificación y Firma – Perfiles de Certificados v1.7.6" del Consejo Superior de Administración Electrónica. Los datos presentes en los certificados de Autoridad de Certificación se presentan a continuación. El conjunto de los certificados se incluyen en los anexos del presente documento:

AC Raíz

Emisor	CN= SESCAM Root CA O = JCCM O = SESCAM (NIF Q-4500146H) C =ES
Titular	CN= SESCAM Root CA O = JCCM O = SESCAM (NIF Q-4500146H) C =ES
Número de Serie	`00 81 2d c3 f2 0f 9e ed 7a ca f3 9e c5 c9 ce ec`
Periodo de Validez	**Desde** 30/11/2010 **hasta** 30/11/2040
Huella (SHA1)	`c4 5b 5a 7a 37 1a 07 2d 0c 84 d8 a6 f4 d0 3c b5 62 a8 e0 7d`

Algoritmo de firma	pkcs1-sha1withRsaSignature

AC Subordinada 2010

Emisor	CN= SESCAM Root CA O = JCCM O = SESCAM (NIF Q-4500146H) C =ES
Titular	CN= SESCAM CA Entidades Finales O = JCCM O = SESCAM (NIF Q-4500146H) C =ES
Número de Serie	`35 58 46 fe 6e e7 5b 55 4c f4 d6 b9 58 35 28 bf`
Periodo de Validez	**Desde** 30/11/2010 **hasta** 30/11/2035
Huella (SHA1)	`52 ef 59 76 ec 6d 2b 2a 34 06 6c f3 4a a7 1e de 9b ab 4f 24`
Algoritmo de firma	pkcs1-sha1withRsaSignature

AC Subordinada 2012

Emisor	CN= SESCAM Root CA O = JCCM O = SESCAM (NIF Q-4500146H) C =ES
Titular	CN= SESCAM CA Entidades Finales O = JCCM OU = SESCAM SERIALNIUMBER = Q4500146H C =ES
Número de Serie	`04 3a a4 e8 cf d1 85 c8 4f 4b 68 d4 00 2c c3 7e`
Periodo de Validez	**Desde** 27/02/2012 **hasta** 27/02/2037
Huella (SHA1)	`3b f3 c8 eb 47 e4 8d 11 bc c5 69 64 23 63 f7 45 8e 9a af 48`
Algoritmo de firma	pkcs1-sha1withRsaSignature

1.3.2.1 Autoridad de Recuperación de claves

La Autoridad de Recuperación de claves (ARC) del SESCAM garantizará la salvaguardia y confidencialidad de las claves de cifrado de los usuarios (personas físicas y/o empleados públicos).

1.3.3 Autoridad de Registro

La Autoridad de Certificación (AC) del SESCAM se vale de varias Autoridades de Registro (AR). Estas autoridades de Registro realizarán las tareas de registro presencial, validación y procesado de las peticiones de certificados y de revocación/suspensión y renovación de certificados.

1.3.4 Autoridad de Validación

La Autoridad de validación del SESCAM es la encargada de suministrar información sobre la vigencia de los certificados electrónicos emitidos por el SESCAM y por aquellas otras Autoridades de Certificación con las que él SESCAM mantenga un acuerdo de cooperación.

La Autoridad de Validación del SESCAM está representada por el siguiente certificado, que será renovado cada 6 meses según se establece en la correspondiente política de certificación para la Autoridad de Validación.

Autoridad de Validación

Emisor	CN= SESCAM CA Entidades Finales O = JCCM OU = SESCAM SERIALNIUMBER = Q4500146H C =ES
Titular	CN= Autoridad Validación SESCAM O = JCCM O = SESCAM (NIF Q-4500146H) C =ES
Número de Serie	`7b 07 f3 46 a8 13 d4 e0 4f 4f 5c 9a 0c 94 2a 4a`
Periodo de Validez	**Desde** 01/03/2012 **hasta** 01/09/2012
Huella (SHA1)	`8e 12 b2 39 23 46 93 bc 23 a2 9d e5 da 1f 30 49 b6 05 93 3e`
Algoritmo de firma	pkcs1-sha1withRsaSignature

El servicio de validación se presta en la siguiente dirección:

http://sescam.jccm.es/va

Así mismo el SESCAM ofrece servicios avanzados de validación (tanto de certificados como de firma electrónica), ofreciendo diversos niveles de servicio:

- Verificación de certificados admitidos.
- Verificación de firma electrónica, así como de los diferentes certificados admitidos en que se basa la firma electrónica.

Estos servicios son ofrecidos a través de la intranet administrativa del la JCCM (Junta de Comunidades de Castilla-La Mancha) en la siguiente URL:

https://trustedx.sescam.jclm.es:8080/trustedx-gw/

El uso de los servicios avanzado de ésta entidad de validación requieren la utilización del protocolo DSS (Digital Signature Services).

1.3.5 Autoridad de Sellado de Tiempo

La Autoridad de Sellado de Tiempo aporta evidencias criptográficas de existencia en un momento determinado, el del sello de tiempo. El SESCAM ofrece a sus usuarios la capacidad de incluir sellos de tiempo dentro de sus procesos de firma a través de su plataforma de servicios de confianza TrustedX, de ésta forma cualquier usuario que genere una firma electrónica podrá incluir un sello de tiempo si la política de firma impuesta para dicha aplicación así lo requiere.

La Entidad de Sellado de Tiempo del SESCAM proporciona servicio según determina la ETSI TS 102 023 y las condiciones adicionales que han sido establecidas por la AGE para adaptar dicha norma a la normativa española.

Los sellos de tiempo emitidos por la Autoridad de sellado de tiempo del SESCAM son conformes con la norma IETF RFC 3161.

La Entidad de Sellado de Tiempo está representada por el siguiente certificado,

Autoridad de Sellado de Tiempo

Emisor	CN= SESCAM CA Entidades Finales O = JCCM OU = SESCAM SERIALNIUMBER = Q4500146H C =ES
Titular	CN= Autoridad de Sellado de Tiempo del SESCAM O = JCCM O = SESCAM (NIF Q-4500146H) C =ES
Número de Serie	3a 9c 35 b0 56 97 b2 34 4f 4f 66 fe db 86 f5 30
Periodo de Validez	**Desde** 01/03/2012 **hasta** 27/02/2037
Huella (SHA1)	96 d2 7f 22 43 a1 f2 72 df 71 46 b0 f7 02 7a f2 25 d1 3a da
Algoritmo de firma	pkcs1-sha1withRsaSignature

El servicio de validación se presta en la siguiente dirección:

http://sescam.jccm.es/tsa

1.3.6 Entidades Relacionadas

Se requieren los servicios del Directorio Corporativo del SESCAM a efectos de publicación, y del servidor de mensajería para localizar a las entidades finales y enviar las notificaciones pertinentes, según se define en los procedimientos de la PKI del ciclo de vida de los certificados y Listas de Certificados Revocados.

1.3.7 Usuarios Finales

Las Entidades finales o Usuarios son las personas físicas o jurídicas que tienen capacidad para solicitar y obtener un certificado electrónico en las condiciones que se establecen en la presente Declaración de Prácticas de Certificación y en las Políticas de Certificación vigentes para cada tipo de certificado.

A los efectos de la presente Declaración de Prácticas de Certificación, son Entidades finales del sistema de certificación del SESCAM, las siguientes:

a) Los solicitantes de certificados.

b) Los suscriptores o responsables de certificados.

c) Terceros de Confianza, los verificadores de firmas y certificados.

1.3.7.1 Solicitantes

Solicitante es la persona física que, en nombre propio o en representación de tercero, y previa identificación, solicita la emisión de un *Certificado*.

En el supuesto de tratarse de un Solicitante de Certificado cuyo Suscriptor sea una persona jurídica dicha persona física sólo podrá ser un administrador o un representante, legal o voluntario con poder bastante a estos efectos, de la persona jurídica que vaya a ser el suscriptor del certificado.

1.3.7.2 Suscriptores

Se entienden por subscritores de la PKI del SESCAM aquella entidad cuyo denominación se refleja en el subject del certificado y que asegura que utiliza su clave y su certificado de acuerdo con la presente DPC.

En el ámbito de la Infraestructura de Clave Pública del SESCAM los suscriptores de los certificados emitidos bajo está DPC serán de los siguientes tipos:

- ***Personal del SESCAM*** (Funcionarios de la JCCM, Estatutarios y Personal Laboral) que sean notificados por el canal de comunicación pertinente a presentarse en un Puesto de Identificación y Expedición de Tarjetas o en un puesto de Registro certificado por el SESCAM.
- ***Personal externo que trabaja en el SESCAM***, que sean notificados por el canal de comunicación pertinente a presentarse en un Puesto de Identificación y Expedición de Tarjetas o en un puesto de Registro certificado por el SESCAM.

- ***Personas físicas,*** que sean notificadas por el canal de comunicación pertinente a presentarse en un Puesto de Identificación y Expedición de Tarjetas o en un puesto de Registro certificado por el SESCAM.
- **Dispositivos de seguridad**, como por ejemplo, controladores de dominio, servidores SSL, routers, concentrardores VPNs, aplicaciones, etc. Estos componentes deberán estar bajo la supervisión del personal responsable de aceptar los certificados y de la correcta protección uso de la clave privada de los mismos.

En certificados de sede y de sello, dentro del campo "Subject" (concretamente en el atributo Common Name) también se identifica el dispositivo o servidor al que están asociados.

1.3.7.3 Terceros que confían en certificados

Aquellas personas físicas o jurídicas que reciben certificados emitidos por el SESCAM son terceros que confían en certificados y, como tales, les es de aplicación lo establecido por la presente Declaración de Prácticas de Certificación cuando deciden confiar efectivamente en tales certificados.

Se considera que los terceros confían en los certificados en función del empleo objetivo que de los mismos realicen en sus relaciones con los suscriptores. En este sentido deberá realizar las comprobaciones oportunas para que éste pueda establecer la relación de confianza en:

- Las firmas digitales realizadas por el suscriptor del certificado,
- En los procesos de control de acceso que requieran la autenticación del suscriptor mediante el certificado correspondiente asignado al mismo por el SESCAM.
- En el envío de elementos cifrados que requieren el uso del certificado del suscriptor por parte del tercero que confía en el mismo.

1.3.8 Otras entidades

El SESCAM admite el uso de certificados emitidos por otras Administraciones públicas españolas y europeas en los siguientes supuestos:

- Como elementos probatorios de identidad de los suscriptores en los procesos de registro remotos frente a la infraestructura de clave pública.
- Reconocimiento de las firmas electrónicas de los suscriptores de las mismas, siempre y cuando éstas hayan sido realizadas con certificados cualificados/reconocidos según la especificación ETSI TS 101 456 y las firmas tengan la calificación de "reconocidas/cualificadas".
- Para el reconocimiento de cualquier otra función o servicio se atenderá a los acuerdos firmados entre el SESCAM o los órganos competentes de la Junta de Comunidades de Castilla la Mancha.

1.4 Usos de los Certificados

Esta sección describe el tipo de aplicaciones para los que los certificados han sido emitidos, también explicita los tipos de aplicación inapropiada de éstos.

1.4.1 Usos apropiados de los certificados

1.4.1.1 Certificado reconocido

Los certificados reconocidos de firma electrónica garantizan la identidad del suscriptor y del poseedor de la clave privada de firma. En el SESCAM los certificados reconocidos son siempre emitidos en un dispositivo de creación de firma segura ofreciendo por tanto la capacidad de generar firmas electrónicas reconocida; esto es, la firma electrónica avanzada que se basa en certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo que, de acuerdo con el artículo 3.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, se equipara a la firma manuscrita por efecto legal, sin necesidad de cumplir requisito adicional alguno.

1.4.1.2 Certificados Ordinarios

Los certificados no reconocidos garantizan la identidad del suscriptor y, en su caso, del poseedor de la clave privada; asimismo, deben emplearse en conjunción con un dispositivo de generación de firma.

Los certificados no reconocidos pueden emplearse, si así se define en el tipo de certificado correspondiente, para firmar mensajes de autenticación, establecimiento de sesiones SSL/TSL o IPSEC, correo electrónico seguro S/MIME, cifrado, u otros.

El uso de este tipo de certificados en los procesos de firma digital no se equipara a la firma manuscrita del firmante. Sin embargo, esta firma digital tiene el efecto de garantizar la identidad del suscriptor del certificado de firma, esto es: una firma electrónica avanzada según se establece por la ley 59/2003.

1.4.1.3 Certificados de Sede y Sello Electrónico.

Estos certificados se emiten a las administraciones públicas para la identificación de la sede administrativa y el sellado electrónico de documentos, según lo previsto en la Ley 11/2007.

1.4.2 Usos prohibidos de los certificados

Los certificados deben emplearse para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades de las descritas para cada uno de ellos en *1.4.1 Usos apropiados de los certificados.*

1.5 Administración de la Declaración de Prácticas

Los datos de la organización que administra el documento y sus datos de contacto se ofrecen a continuación:

Nombre Prestador	Servicios de Salud de Castilla La Mancha
Dirección Postal	Avda. Río Guadiana nº 4 45007 Toledo Toledo
Telefono	925 27 41 00
e-mail	cervantes@sescam.jccm.es
Web	http://sescam.jccm.es

1.5.1 Procedimiento de Gestión de la DPC

El procedimiento de aprobación de la DPC se garantiza mediante la adecuada aplicación de los procedimientos correspondientes mantenidos por el SESCAM. Las modificaciones a la DPC son aprobadas por éste, después de verificar el cumplimiento definido en la sección *9.12 Correcciones a la DPC*.

1.6 Definiciones y Acrónimos

1.6.1 Definiciones

AST (Autoridad de Sellado de Tiempo)	Sistema informático dedicado a las funciones de emisión de sellos de tiempo criptográficos en las condiciones necesarias de calidad y seguridad, y en concreto, de la gestión de la fuente fiable de tiempo, que debe estar sincronizada con la hora oficial.
Certificado electrónico	Documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
Certificados reconocidos	Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la ley 59/2003 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.
Dispositivo de	Dispositivo que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el

Creación de Firma Seguro.	artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
Firma electrónica	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	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	Firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro 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.
Firmante	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.
Fuente Fiable de Tiempo	Sistema que nos informa de la hora y la fecha legales, en tiempo universal coordinado, utilizado por la emisión de sellos de tiempo. Bajo está DPS se utiliza el suministrado por el ROA (Real Instituto y Observatorio de la Armada).
Hash	Valor numérico de longitud fija que identifica datos de forma unívoca. Los valores hash se utilizan para comprobar la integridad de los datos.
HSM (Hardware Security Module)	Es un dispositivo hardware con capacidades criptográficas que permiten generar y almacenar de manera segura claves criptográficas.
PIN (Personal Identification Number)	Secuencia de caracteres que permiten el acceso a los dispositivos de creación de firma.
Prestador de servicios de certificación	Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
Sede Electrónica	La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.

1.6.2 Acrónimos

AAP	Autoridad de Aprobación de Políticas
AC	Autoridad de Certificación
AR	Autoridad de Registro
ARC	Autoridad de Recuperación de Claves
AST	Autoridad de Sellado de Tiempos
AV	Autoridad de Validación
CEN	Comité Européen de Normalisation (Comité Européo de Normalización)
CRL	Certficate Revocation List
CWA	CEN Workshop Agreement
DPC	Declaración de Prácticas de Certificación
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module.
IETF	Internet Engineering Task Force
JCCM	Junta de Comunidades de Castilla – La Mancha
LCR	Lista de Certificados Revocados
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object identifier
PKCS	Public Key Cryptography Standards.
PKI	Public Key Infrastructure
RFC	Request For Comments
SESCAM	Servicio de Salud de Castilla – La Mancha

2 Publicación de información y depósito de certificados

2.1 Deposito

Se entiende por depósito el sistema, o los sistemas, donde se publica la información relevante del SESCAM relativa a los servicios de la infraestructura de clave pública. El SESCAM dispone de diferentes depósitos o repositorios dependiendo del acceso que se requiera a los mismos, así pues los repositorios donde se encuentra la información disponible son:

- Toda la información relativa a cada uno de los componentes que conforman la gestión de la emisión, revocación y suspensión de certificados, sellos de tiempo y tokens de validación OCSP está custodiada de forma segura e integra en las Bases de Datos de las Autoridades de Confianza (Autoridades de Certificación, Registro, Validación y Sellado de Tiempo). El acceso a estos repositorios está restringido a personal autorizado del SESCAM.
- Repositorio WEB, donde se podrá encontrar la documentación que rige la operativa de la infraestructura y las listas de revocación de la Autoridad de Certificación del SESCAM.
- Directorios LDAP donde la Autoridad de certificación pública los certificados que deben ser publicados atendiendo a la política de certificación a la que están asociados.
- El acceso a estos sistemas se encuentra disponible los 7 días x 24 horas del año, salvo acciones de mantenimiento preventivo o correctivo que pudieran acontecer.

2.1.1 Publicación de información de la Autoridad de Certificación

El SESCAM como prestador de servicios de confianza mantiene publicadas las siguientes informaciones en sus repositorios públicos:

- La declaración de prácticas de certificación (DPC) en la siguiente dirección http://sescam.jccm.es/pki/dpc.
- Los certificados y Listas de revocación emitidos por las Autoridades de Certificación se publican en diferentes repositorios en aras de satisfacer los requisitos y necesidades establecidos y/o impuestos por diferentes aplicaciones y sistemas.
    - **Repositorio WEB del SESCAM en:**
        - Certificados de Entidades de Confianza:
            - Certificado de la Autoridad de Certificación Raíz

- http://sescam.jccm.es/pki/certs/roots
- Certificado de la Autoridad de Certificación Subordinada
- http://sescam.jccm.es/pki/certs/produccion
- Certificado de la Autoridad de Sellado de Tiempo
- http://sescam.jccm.es/pki/certs/produccion
- Certificado de la Autoridad de Validación
- http://sescam.jccm.es/pki/certs/produccion

- Listas de Revocación, en estas entradas únicamente se publicarán las listas vigentes.
  - Lista de Revocación de la Autoridad de Certificación Raíz
  - http://sescam.jccm.es/pki/arls/
- Listas de Revocación de la Autoridad de Certificación Subordinada
  - http://sescam.jccm.es/pki/crls/

- **Directorio Corporativo del SESCAM**:

  En el directorio corporativo del SESCAM, únicamente accesible desde la red interna de la JCCM, serán publicados únicamente los Certificados de Entidad Final con propósitos de cifrado, esto es:

  - Empleado Público de cifrado, con uno de los siguientes OIDs:
    - 2.16.724.4.8.10.60.10.2.1.1.3
    - 2.16.724.4.8.10.60.10.2.1.1.3
  - Persona Física, con uno de los siguientes OIDs:
    - 2.16.724.4.8.10.60.10.2.2.3
    - 1.3.6.1.4.1.21835.1.1.3.3

  bajo el atributo userCertificate del usuario al que pertenece y cuya entrada existe y es mantenida por el SESCAM.

- En los repositorios "Active Directory" de todos los Dominios de Windows pertenecientes al SESCAM y a sus entidades asociadas bajo las ramas:
  - Autoridad de Certificación Raíz
  - ldap:///CN=SESCAM-ROOT-CA, CN=Certification Authorities, CN=Public Key Services, CN=Services, CN=Configuration, DC=<Controlador de Dominio >, DC=com?cACertificate?base?objectclass=certificationAuthority
  - ldap:///CN=SESCAM-ROOT-CA, CN=AIA, CN=Public Key Services, CN=Services, CN=Configuration, DC=<Controlador de Dominio >, DC=com?cACertificate?base?objectclass=certificationAuthority
  - Autoridad de Certificación Subordinada
  - ldap:///CN=SESCAM-SUB-CA, CN=AIA, CN=Public Key Services, CN=Services, CN=Configuration, DC=<Controlador de Dominio >, DC=com?cACertificate?base?objectclass=certificationAuthority

2.1.2 Frecuencia de Publicación

La Declaración de Prácticas de Certificación (DPC) y las políticas de certificación (PC) se publicarán en cuanto se encuentran disponibles y los correspondientes cambios se gestionarán según lo establecido en este documento en la sección 9.12.

Las listas de revocación (LCR) se publicarán siguiendo los procedimientos definidos en la sección 4.9.7 de este documento.

Los certificados de entidad final susceptibles de ser publicados, lo serán por la Autoridad de Certificación en el momento de su emisión.

2.1.3 Control de acceso

No se establecen controles de acceso de lectura sobre la declaración de prácticas de certificación (DPC), las políticas de certificación (PC), o sobre los certificados de las Autoridades de Certificación y sus LCRs, asi como para los certificados del resto de entidades de confianza. Esto es, no se establecen restricciones de lectura sobre el repositorio WEB ofrecido por el SESCAM, sin embargo se establecen controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros de dicho repositorio.

La autenticidad e integridad de toda la información publicada es éste repositorio está garantizada por el uso de la firma digital, que es utilizada para firmar todos los objetos y documentos publicados en dicho repositorio.

El resto de repositorios son accesibles únicamente en el dominio interno del SESCAM, estableciéndose controles de acceso para la lectura de los mismos a los usuarios y aplicaciones del SESCAM.

El SESCAM emplea sistemas fiables para los repositorios de Base de Datos utilizadas por sus Entidades de Confianza (AC, AV, AR y AST), de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si el suscriptor o responsable del certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 IDENTIFICACION Y AUTENTICACION

3.1 Registro de Nombres

3.1.1 Tipos de nombres

Todos los certificados contienen un nombre distintivo (DN) de la persona y/o organización, identificados en el certificado, definido de acuerdo con lo previsto en la Recomendación ITUT X.501 y contenido en el campo Subject Name, incluyendo un componente Common Name.

Todos los certificados emitidos cumplen, además, con la normativa IETF RFC 5280 - X.509 Public Key Infraestructure, Certificate and Certificate Revocation List Profile.

En el caso de certificados de Entidad Final el operador de registro verificará los nombres distinguidos de la solicitud en el momento de generar la petición de certificación, éste se incluirá en el campo Common Name (CN) y se corresponderá con el nombre que aparece identificado en el DNI, Pasaporte o Documento que identifique unívocamente al subscritor.

3.1.2 Significado de los nombres

Los nombres de los certificados son comprensibles e interpretados de acuerdo con la legislación aplicable a los nombres de las personas físicas y jurídicas titulares de los certificados.

Los nombres incluidos en los certificados son tratados de acuerdo con las siguientes normas:

- En los certificados de empleado público, se incluirá como mínimo la siguiente información:
- Descripción del tipo de certificado
- Datos de identificación personal de titular del certificado
- Nombre de pila
- Primer apellido
- Segundo apellido
- DNI o NIE
- Nombre de la entidad en la que está suscrito el empleado
- Número de Identificación Fiscal de entidad
- En el certificado de SEDE Administrativa, se incluirá como mínimo la siguiente información:

- Descripción del tipo de certificado, esto es, "Sede Administrativa".
- Nombre descriptivo de la sede electrónica
- Denominación de Nombre del dominio / dirección IP
- Nombre de la entidad suscriptora
- Número de Identificación Fiscal de entidad suscriptora
- En el certificado de Sello Administrativo , se incluirá como mínimo la siguiente información:
- Descripción del tipo de certificado, esto es, "Sello Administrativo"
- Nombre de la entidad suscriptora
- Número de Identificación Fiscal de entidad suscriptora
- En los certificados de persona física el nombre del suscriptor estará compuesto al menos por su nombre y apellidos, pudiendo incluir el cargo que ocupa dentro de la organización, así como también el identificador único dentro del directorio LDAP del SESCAM.
- En los certificados de dispositivo de servidor el nombre del suscriptor es el nombre del dominio, la dirección IP del servidor o el nombre que esté indicado en la petición.
- En el certificado de firma de código, en el nombre del suscriptor se indica el nombre del órgano competente o de la entidad a la que pertenece el software.

Por último indicar que la estructura sintáctica y el contenido de los campos de cada certificado, así como su significado semántico se encuentra descrito en cada "perfil de certificado", véase capítulo 7.

3.1.3 Utilización de anónimos y pseudónimos

No se permite la utilización de anónimos ni seudónimos en ningún caso.

3.1.4 Interpretación de formatos de nombres

No se establecen estipulaciones adicionales para la interpretación de nombres.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores son únicos para cada tipo de certificado (Política de certificación) emitido.

3.1.6 Reconocimiento, Autenticación y resolución de conflictos relativos a nombres

Los solicitantes de certificados no pueden incluir nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros. La inclusión en un certificado de un nombre no implica la existencia de ningún derecho sobre el mismo y lo es sin perjuicio del mejor derecho que pudieren ostentar terceros.

El SESCAM no actúa como árbitro o mediador, ni resuelve ninguna disputa relativa a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc.

El SESCAM se reserva el derecho de rehusar una solicitud de certificado por causa de conflicto sobre el nombre.

Los conflictos de nombres de responsables de certificados que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre distintivo del certificado, del DNI del responsable del certificado o de otro identificador asignado por el suscriptor.

3.2 Validación inicial de la Identidad

3.2.1 Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de generación de claves, petición de certificado y entrega del mismo al soporte criptográfico donde las claves están almacenadas.

Los tipos de certificados emitidos bajo esta DPC tienen requisitos diferentes de prueba de posesión dependiendo del procedimiento de registro efectuado para el perfil o la política de certificado requerida, así pues podemos distinguir:

- Registro Presencial y expedición inmediata en Tarjeta. En este caso el subscriptor se persona frente a un Oficial de Registro, quién una vez comprobada la identidad de la persona procede conjuntamente con el subscriptor a generar las claves de éste que serán certificadas por la AC. En este supuesto las claves son generadas en la propia tarjeta –autenticación y firma- o inyectadas de forma segura –cifrado-; con lo que se garantiza la posesión de las claves por el subscriptor.
- Este procedimiento es el utilizado para los certificados de Persona física y empleado público. En estos casos las solicitudes de certificados exigen que el solicitante introduzca el PIN de acceso a la Tarjeta.
- Registro remoto y expedición diferida. En este caso el subscritor que genera el par de claves deberá probar la posesión de la clave privada correspondiente a la clave pública que solicita que se le certifique mediante el envió de la solicitud en formato PKCS#10.

3.2.2 Autenticación de la identidad de una Organización

3.2.2.1 Certificados de Sede y Sello Administrativo

En todos los tipos de certificados emitidos a las AAPP resulta necesario identificar a la Administración Pública, organismo o entidad de derecho público.

No se exige la documentación acreditativa de la existencia de la Administración Pública, organismo o entidad de derecho público.

Se exige la documentación de identidad de la persona que actúa como responsable, en nombre de dicha Administración Pública, organismo o entidad de derecho público.

De esta forma, no será necesario autenticar la identidad de las administraciones y otras organizaciones que actúan como entidades de registro, dado que dicha identidad forma parte del ámbito corporativo de la JCCM o de otras AAPP del Estado.

3.2.2.2 Certificados de Dispositivo

En certificados de dispositivo (Servidor SSL, Aplicaciones, Controlador de Dominio y firma de Código) es necesario comprobar que el dispositivo electrónico que se desea certificar existe y que el solicitante de la misma dispone de la autorización necesaria para exigirlo.

3.2.3 Autenticación de la identidad de una persona física

La identificación y acreditación de las personas físicas exige la personación de las mismas ante los Operadores de Registro y la presentación de uno de los siguientes documentos:

- Documento Nacional de Identidad, o
- Tarjeta de Residencia, NIE
- Pasaporte

No se contemplan procedimientos de acreditación que no requieran la presencia personal al realizarse el proceso de registro y certificación en tiempo real concluyéndose con la entrega de la tarjeta con claves y certificados operativos al usuario.

3.2.4 Información de suscriptor

En conformidad con el articulo 23.1.a) de la Ley de firma electrónica (LFE) el SESCAM como prestador de Servicios de Certificación no será responsable cuando el firmante no haya proporcionado al SESCAM información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de la vigencia, cuando su inexactitud no haya podido ser detectada por el SESCAM.

3.2.5 Validación de Autoridad

El operador de registro del SESCAM velará porque las autorizaciones presentadas por solicitantes en nombre de elementos de la organización sean válidas y fehacientes, estableciendo los mecanismos oportunos para que así sea.

3.2.6 Criterios de Interoperabilidad

No se definen criterios de interoperabilidad entre la AC del SESCAM y otras. Los mecanismos deberán ser establecidos de forma bilateral e independiente con otras Autoridades de Certificación.

3.3 Identificación y autenticación para peticiones de renovación de claves

3.3.1 Registro para renovación rutinaria de claves y certificados

Se excluye la posibilidad de renovación de certificados, siendo necesaria tras su expiración o revocación una nueva emisión.

3.3.2 Registro para renovación de claves y certificados tras revocación

Tras la revocación de un certificado se tendrá que solicitar uno nuevo siguiendo el proceso de solicitud y emisión de certificado establecido para cada clase y tipo de certificado.

3.4 Identificación y autenticación para peticiones de revocación.

Las peticiones de revocación de un certificado vendrán determinadas por los establecido para cada tipo y clase de certificado:

Certificados de Persona (Física y empleado público)	Las peticiones de revocación podrán ser realizadas por: El propio usuario comunicándolo directamente a su operador de registro. El Administrador de Sistemas de la AC, previa petición y autorización de los oficiales de seguridad del SESCAM.
Certificados de Sede y Sello Administrativo	Las peticiones de revocación podrán ser realizadas por: El responsable de la SEDE comunicándolo directamente a su operador de registro. El Administrador de Sistemas de la AC, previa petición y autorización de los oficiales de seguridad del SESCAM.
Certificados de Dispositivo	Las peticiones de revocación y/o suspensión podrán ser realizadas por: El responsable del dispositivo informático comunicándolo directamente a su operador de registro. El Administrador de Sistemas de la AC, previa petición y autorización de los oficiales de seguridad del SESCAM.

4 REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

4.1 Solicitud de certificados

El solicitante debe rellenar y firmar el formulario de solicitud correspondiente al tipo o clase de certificado demandado, aceptar el contrato de suscriptor y entregarlo junto con la documentación requerida en la Entidad de Registro, quien realizará la identificación y las comprobaciones oportunas.

La Entidad de Registro que recibe la solicitud de certificación es responsable de realizar el procedimiento de alta de la misma. Esta información será dada de alta en la base de datos de la autoridad de registro con el fin de realizar consultas posteriores, sobre el estado de la solicitud o de los certificados de un suscriptor particular.

El SESCAM no admite la emisión de más de un certificado de la misma política para un mismo subscritor, por lo que de forma previa a la emisión el Oficial o Entidad de Registro comprueba que el solicitante no es titular de un certificado del mismo tipo, vigente en dicho momento, para el cual ha realizado la solicitud.

Los datos que identifican al poseedor de claves en el certificado y en la solicitud son los que constan en los documentos y sistemas de identificación establecidos por el SESCAM.

4.2 Procesamiento de la solicitud de certificación

En el momento en que el SESCAM o una de sus entidades asociadas recibe una solicitud de certificado se procede al registro de la misma, bien mediante la aplicación de registro correspondiente asociada a la Autoridad de Certificación, bien mediante el uso de la aplicación corporativa de gestión de Usuarios.

Durante el proceso de solicitud existe una comprobación de que el usuario o dispositivo realmente pertenece al subscriptor.

4.2.1 Procesamiento de solicitud de certificados de Entidades de Confianza

Para la solicitud de creación de autoridades de confianza –Autoridades de Validación o Autoridades de Sellado de Tiempo-, será necesario que las

mismas generen un conjunto de claves en dispositivo hardware criptográfico homologado cómo mínimo a FIPS 140-2 nivel 3.

Los Oficiales de Seguridad de estas entidades entregarán la solicitud de certificado en formato PKCS#10 o X509 autofirmado a los Oficiales de Registro de la Autoridad de Certificación, quienes deberán velar por la correcta identificación del suscriptor y sus representantes, y de la autenticidad de la información que se le presenta en la solicitud.

El tiempo de procesamiento de estas solicitudes estará en función de la disponibilidad del conjunto de Oficiales de Registro necesario para procesar dicha solicitud, definido éste como un mínimo de N de los M Oficiales de Registro de la Autoridad de Certificación.

4.2.2 Procesamiento de solicitud de certificados de empleado público o persona física

El solicitante deberá personarse físicamente en la Entidad de Registro para solicitar sus certificados acreditando su identidad mediante la presentación de un documento de identidad legalmente válido: DNI, NIE o Pasaporte.

Los certificados de empleado público son emitidos con carácter general a cualquier empleado público del SESCAM y/o de la JCCM (eg: Funcionario de carrera, funcionarios Interinos, Personal Laboral y Personal Eventual) . La emisión de certificados de esta clase está asociada "***siempre***" a la entrega de un dispositivo criptográfico seguro al usuario, y requiere la emisión de los tres tipos de certificados, es decir, en el proceso de solicitud el suscriptor obtendrá los tres certificados en su tarjeta electrónica para los procesos de autenticación, no-repudio y cifrado.

Los certificados de persona física son emitidos con carácter general a cualquier persona que pueda mantener cualquier tipo de relación con el SESCAM y/o con la JCCM (eg: personal externo, proveedores, ciudadanos, etc) . La emisión de certificados de esta clase está asociada a la entrega de un dispositivo criptográfico seguro al usuario, y requiere la emisión de los tres tipos de certificados, es decir, en el proceso de solicitud el suscriptor obtendrá los tres certificados en su tarjeta electrónica para los procesos de autenticación, no-repudio y cifrado.

4.2.3 Procesamiento para los certificados de sello electrónico.

Para el procesamiento de éste tipo de solicitudes es necesario la identificación de la persona que actúa como responsable del certificado, ya sea en la solicitud o en la entrega del certificado.

Las claves se generan por los mecanismos propios de la aplicación requirente del sello y los solicitantes deberán informar a la Entidad de Registro del tipo de dispositivo en el que fue generado el par de claves.

En el caso de qué el dispositivo sea un HSM (Dispositivo Criptográfico Hardware) deberán requerir la presencia de un oficial de registro del SESCAM o de un fedatario público durante el proceso de generación que atestigüe que las claves han sido generadas por dicho dispositivo.

Posteriormente el solicitante hará entrega a la Entidad de Registro la petición de certificación en formato PKCS#10 para su certificación.

En los casos que el certificado de sello incorpore un órgano, éste debe identificar su identidad, para lo cual el solicitante deberá adjuntar la documentación necesaria para identificar el órgano al que representa conjuntamente con el modelo de solicitud de éste tipo de certificados.

El tiempo de procesamiento de estas solicitudes será cómo máximo de 10 días laborales.

4.2.4 Procesamiento para los certificados de sede electrónica.

Para el procesamiento de éste tipo de solicitudes es necesario la identificación de la persona que actúa como responsable del certificado, ya sea en la solicitud o en la entrega del certificado.

Las claves se generan por los mecanismos propios de la aplicación requirente del sello y los solicitantes deberán informar a la Entidad de Registro del tipo de dispositivo en el que fue generado el par de claves.

En el caso de qué el dispositivo sea un HSM (Dispositivo Criptográfico Hardware) deberán requerir la presencia de un oficial de registro del SESCAM o de un fedatario público durante el proceso de generación que atestigüe que las claves han sido generadas por dicho dispositivo.

Posteriormente el solicitante hará entrega a la Entidad de Registro la petición de certificación en formato PKCS#10 para su certificación.

Además se comprobará fehacientemente por parte de la Entidad de Registro la existencia y titularidad del servidor y nombre de dominio. Para ello se podrá exigir cuanta documentación y certificaciones sean precisas al solicitante del certificado de sede.

El tiempo de procesamiento de estas solicitudes será cómo máximo de 10 días laborales.

4.2.5 Procesamiento de solicitud de certificados de dispositivo

Para la solicitud de certificados de dispositivo, servidor WEB, Aplicaciones, Controlador de dominio Windows, así como también de firma de código, las claves se generan por los mecanismos propios de estos dispositivos y sus administradores entregan en la Entidad de Registro la petición de certificación en formato PKCS#10 junto a la clave pública para su certificación según el procedimiento descrito en 4.3 Emisión de certificados.

El tiempo de procesamiento de estas solicitudes será cómo máximo de 5 días laborales.

4.3 Emisión de certificados

4.3.1 Procedimiento de la Infraestructura para la emisión de certificados

Este apartado describe las acciones llevadas a cabo por los elementos regístrales, es decir, Operador de Registro y/o Aplicación de Registro, Autoridad de Registro y la Autoridad de Certificación. Se indica el procedimiento aplicado por cada uno de los elementos para validarse entre

si, validar la solicitud de certificación y emitir los correspondientes certificados.

4.3.1.1 Emisión de Certificados de Autoridad de Confianza

Una vez recibida una solicitud de estas características, un conjunto determinado de Oficiales de Registro procederá a la generación de certificado mediante la presentación de sus respectivas credenciales a la Autoridad de Certificación.

La emisión de certificados de esta clase sólo se podrá realizar localmente en la Entidad de Certificación del SESCAM, mediante el siguiente procedimiento:

- Un conjunto de operadores de registro con los permisos adecuados iniciará sesión en la aplicación de administración de la Entidad de Certificación del SESCAM.
- Estos operadores de la AC procesarán la petición generada por los oficiales de Seguridad de la Entidad de Confianza Solicitante aplicando el correspondiente perfil de certificación, exportarán en un fichero el certificado emitido y se lo entregará a los oficiales de seguridad de Entidad de Confianza solicitante.
- Los oficiales de Seguridad instalarán el certificado contenido en el fichero entregado en éstos usando las aplicaciones de administración correspondientes de la Entidad de Confianza Solicitante.

4.3.1.2 Emisión de Certificados de Persona Física y Empleado Público

4.3.1.2.1 Procedimiento de emisión de la tarjeta de un usuario en la AR del centro

1. El usuario se presenta en el SESCAM.
2. El operador del SESCAM iniciará sesión en el puesto de Registro.
3. El usuario aporta su dirección de correo electrónico, el identificador de usuario o el DNI. A través de estos datos la AR obtendrá el resto de LDAP.
   Para la obtención del userPrincipalName se conecta con el Active Directory indicado en la entrada LDAP del usuario.
4. El operador decide si se trata de una Tarjeta Corporativa con perfil de Empleado Público o de Persona Física.
5. La XRA comprueba si ya existe un usuario registrado con los mismos datos. Si lo hay se actualizan los datos con los que se han obtenido de LDAP, si no lo hay la AR registra un nuevo usuario con los datos indicados.
6. Se comprueba si el usuario ya tiene certificados válidos del perfil seleccionado. Si es así se muestra un mensaje de error.
7. Si el usuario tiene una petición de certificación pendiente, se informará al puesto de Registro también.
8. A continuación se muestran los datos del usuario registrado en un formulario que se presenta al operador de Registro
9. El puesto de registro generará el par de claves en la tarjeta del usuario personado. Se generan dos pares de claves en la tarjeta, uno

para el certificado de autenticación y otro para el de firma con no repudio.

10. El puesto de registro establece comunicación con la AR y le envía las claves públicas generadas en la tarjeta.
11. La AR recopila los datos del usuario y crea las peticiones de certificación incluyendo esta información y las claves que el puesto de registro le ha enviado.
12. La AR establece comunicación con la CA y le envía las peticiones de certificación para los certificados de autenticación y no repudio.
13. La CA le devuelve a la AR los certificados de autenticación y no repudio generados.
14. La AR le devuelve al puesto de registro los certificados de autenticación y no repudio generados por la CA.
15. La AR inserta los certificados de autenticación y no repudio en la tarjeta.
    La tarjeta dispone en este momento del certificado y claves de autenticación y del certificado y claves de no repudio.
16. El puesto de registro muestra al usuario por pantalla el contrato de la tarjeta, que será firmado por el usuario cuando introduzca el nuevo PIN, aceptando de esta forma las condiciones de uso de la tarjeta y los certificados contenidos en la misma.
17. El puesto de registro solicita al usuario el cambio del PIN por defecto de la tarjeta. Esta introducción del PIN supondrá la firma del contrato mostrado en pantalla.
18. El usuario introduce el nuevo PIN que desea para la tarjeta.
19. El puesto de registro cambia el PIN por defecto de la tarjeta por el elegido por el usuario.
20. Se envía a la AR el contrato firmado para que ésta lo almacene asociado a estos certificados.
21. En el caso de que no se trate de una tarjeta pre-impresa, la impresora de tarjetas imprime en la tarjeta la información personal del usuario y otros datos relativos a la tarjeta.
22. El operador hace entrega al usuario de la tarjeta con los certificados de autenticación y no repudio correspondientes.
23. La AR envía un correo electrónico al usuario con el contenido de las condiciones de uso de la tarjeta que firmo en el paso 17.

4.3.1.3 Emisión de Certificados de Sede, Sello y Dispositivo

La emisión de certificados de Sede, Sello y Dispositivos sólo se podrán realizar localmente en la AC Subordinada del SESCAM, mediante el siguiente procedimiento:

- Un operador con los permisos adecuados iniciará sesión en la aplicación de administración de la AC Subordinada del SESCAM.
- El operador de la AC procesará la petición generada por el solicitante aplicando el correspondiente perfil de certificación, exportará en un fichero el certificado emitido y se lo entregará al solicitante por un mecanismo fuera de línea.
- El solicitante objeto de certificación instalará el certificado contenido en el fichero entregado usando las aplicaciones de administración correspondientes.

4.3.2 Notificación a suscriptores de la emisión de certificados

La Autoridad de Certificación del SESCAM sólo notificará mediante correo electrónico la emisión de certificados o incidencias en el proceso para los certificados de Sede Electrónica, Sello Administrativo y de Dispositivos. El resto de certificados requiere la presencia física del suscriptor en el momento de su emisión por lo que no se requiere un proceso de notificación por parte de la Autoridad de Certificación.

4.4 Aceptación de certificados

4.4.1 Conducta que constituye aceptación de certificado

La firma del contrato de aceptación, la tarjeta criptográfica y la activación de la misma con el PIN elegidos por el suscriptor o poseedor de las claves se considera como aceptación de los certificados de persona física y empleado público, así como de la aceptación por parte de los suscriptores de las obligaciones definidas en esta DPC.

Para los certificados de Sede Electrónica y Sello Administrativo la firma por parte del representante del contrato de aceptación de términos de uso durante el proceso de solicitud, asi como el uso inicial del certificado constituyen elementos de aceptación en el ámbito de ésta DPC.

Para los certificados de dispositivo, se establece el uso inicial del mismo como elemento de aceptación.

4.4.2 Publicación del certificado

Los certificados se pueden publicar sin el consentimiento previo de los poseedores de claves. En el caso particular de certificados de personas físicas y empleados públicos siempre serán publicados los certificados correspondientes a los usos de cifrado.

4.4.3 Notificación de la emisión a terceros

No es de aplicación.

4.5 Uso del par de claves y del certificado

Los certificados emitidos por el SESCAM se utilizan para las relaciones de la JCCM y del SESCAM con otras administraciones, entidades de carácter privado y/o público y con los ciudadanos. En este sentido los certificados expedidos y gestionados por el SESCAM pueden ser utilizados para la implantación de mecanismos de seguridad que permitan una adecuada gestión de la información:

- Privacidad de la información, en este sentido existen diversos aspectos que deben considerarse, entre los que cabe destacar por ejemplo: cumplimiento con requisitos de la LOPD en el uso de comunicaciones cifradas, garantía de privacidad a expedientes médicos, etc.

- Control de acceso, a instalaciones, servicios informáticos y/o recursos informáticos específicos que requieran privilegios y posterior auditoría.
- No repudio, basada actualmente en la firma por parte de diferentes perfiles como mecanismo revisor, autorizador, etc. Este mecanismo ampliamente utilizado y reconocido, por ejemplo cuando el médico firma una receta, un expediente, una solicitud de servicio asistencial, etc, puede ser sustituida por una firma digital con reconocimiento, agilizando los procesos y produciendo un ahorro en recursos materiales.
- Securización de las comunicaciones mediante correo electrónico entre los distintos centros del SESCAM, así como con otros Departamentos, de acuerdo a las relaciones de confianza que se puedan establecer.
- Dotar de mayores medidas de seguridad el acceso a la red de área local de los servicios Centrales de la JCCM y sus organismos dependientes, incluido el SESCAM y sus centros asociados: hospitales, consultorios, etc.

En este sentido los certificados y sus claves asociadas se utilizan para garantizar la calidad y seguridad de estos requerimientos.

4.5.1 Uso por los poseedores de claves

Los certificados se utilizarán de acuerdo con su función propia y finalidad establecida, sin que puedan utilizarse en otras funciones y con otras finalidades.

Los certificados pueden utilizarse, por parte de los titulares de éstos, en cualesquiera otras relaciones telemáticas con otras entidades, organismos, personas jurídicas o físicas que acepten los certificados.

Los certificados podrán utilizarse con un dispositivo seguro de creación de firma electrónica, que cumpla los requisitos establecidos por el artículo 24 de la Ley 59/2003, de 19 de diciembre, con esta DPC y con las correspondientes condiciones adicionales.

4.5.2 Uso por el tercero que confía en certificados

El uso por parte de terceros de los certificados emitidos por el SESCAM deberá estar de acuerdo con el carácter y la funcionalidad para la que fueron emitidos, el uso de los mismos para fines distintos de los recogidos en esta DPC queda estrictamente prohibida.

4.6 Renovación de certificados sin renovación de claves

La renovación de certificados sin renovación de claves únicamente está permitida para los certificados de Entidad de Confianza, cuando haya una motivación que así lo aconseje (eg: renovar el certificado de la AC subordinada con un algoritmo de hash más fuerte que el utilizado, manteniendo la clave y garantizando la capacidad de utilización de los

certificados emitidos hasta que las aplicaciones de mercado implementen de forma generalizada dicho algoritmo, etc).

La renovación de éste tipo de certificados requiere de un proceso formal y auditado que garantice la seguridad del sistema.

4.7 Renovación de certificados con renovación de claves

4.7.1 Renovación de Certificados de Personas físicas y empleados públicos

El proceso de renovación está ligado al de la tarjeta del usuario, se considera igual a una emisión de una nueva tarjeta del suscriptor una vez que su anterior tarjeta ha expirado, tal y como queda reflejado en "4.3.1.2 Emisión de Certificados de Persona Física y Empleado Público" de esta DPC.

Sólo se permitirá emitir una nueva tarjeta de suscriptor antes de que su anterior tarjeta haya expirado si ésta ha sido revocada.

4.7.2 Renovación de Certificados de Sede, Sello y Dispositivo

Sólo se permitirá emitir un nuevo certificado de esta clase antes de que su anterior certificado haya expirado si éste ha sido revocado, en cualquier caso constituirá una nueva emisión de certificado que requerirá también que se hayan generado nuevas claves.

4.8 Modificación de Certificado

Esta DPC requiere la revocación y nueva emisión de certificados si estos requieren cualquier tipo de modificación.

4.9 Revocación y Suspensión de certificados

4.9.1 Supuestos de revocación

Los certificados emitidos por el SESCAM se revocarán en los siguientes casos:

- Circunstancias que afectan la información contenida en el certificado
  - Modificación de alguno de los datos contenidos en el certificado.
  - Descubrimiento que alguno de los datos aportados en la solicitud de certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas para la expedición del certificado.
  - Descubrimiento que alguno de los datos contenidos en el certificado es incorrecto.

- Circunstancias que afectan la seguridad de la clave o del certificado
    - Compromiso de la clave privada o de la infraestructura o sistemas de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de este incidente.
    - Infracción, por la Entidad de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta DPC.
    - Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor o del responsable de certificado.
    - Acceso o utilización no autorizada, por un tercero, de la clave privada del suscriptor o del responsable de certificado.
    - El uso irregular del certificado por el suscriptor o del responsable de certificado, o falta de diligencia en la custodia de la clave privada.
- Circunstancias que afectan la seguridad del dispositivo criptográfico
    - Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
    - Pérdida o inutilización por daños del dispositivo criptográfico.
    - Acceso no autorizado, por un tercero, a los datos de activación del suscriptor o del responsable de certificado
- Circunstancias que afectan el suscriptor o responsable del certificado.
    - Finalización de la relación entre Entidad de Certificación y suscriptor o responsable del certificado.
    - Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor o responsable del certificado.
    - Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
    - Infracción por el suscriptor o responsable del certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en esta Declaración de Prácticas de Certificación.
    - La incapacidad sobrevenida o la muerte del suscriptor o responsable del certificado.
    - La extinción de la persona jurídica suscriptora del certificado, así como la finalidad de la autorización del suscriptor al responsable del certificado o la finalización de la relación entre suscriptor y responsable del certificado.
    - Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4de esta DPC.

- Otras circunstancias
  - La finalización del servicio de la Entidad de Certificación, de acuerdo con lo establecido en la sección 5.8 de esta DPC.

4.9.2 Entidades que pueden solicitar la revocación

Las peticiones de revocación pueden ser realizadas por:

- El operador de Entidad de Registro previa petición del suscriptor o poseedor de claves.
- El Administrador de la Autoridad de Certificación previa petición y autorización de los oficiales de seguridad del SESCAM.

4.9.3 Procedimiento de solicitud de revocación

En el caso de que la petición de revocación sea presentada por el suscriptor o poseedor de claves, el operador de la Entidad de Registro tendrá que identificarlo siguiendo los procedimientos definidos en la sección 3.2.

Si la identificación da resultado positivo el operador de la Entidad de Registro pedirá la razón de la revocación y activará el proceso de revocación:

- Selección del certificado o certificados afectados.
- Generación del lote con la petición de revocación (o las peticiones) y envió a la Autoridad de Certificación.
- Procesado del lote por la Autoridad de Certificación y generación de la nueva Lista de revocación.
- Con este procedimiento la revocación de los certificados se realiza con un proceso en línea y la generación y publicación de la Lista de Revocación es inmediata.

En el caso de que la petición de revocación sea presentada por los responsables seguridad del SESCAM, un Oficial de Registro de la Autoridad de Certificación procederá a la revocación del certificado (o certificados) afectado y a la generación de la nueva lista de revocación.

Siempre que se proceda a la revocación de certificados de una persona física se tendrá que revocar el conjunto de todos sus certificados (eg, para un empleado público del SESCAM: Autenticación, No-Repudio y Cifrado).

4.9.4 Periodo para la solicitud de revocación

El suscriptor del certificado deberá realizar la solicitud de revocación tan pronto le sea posible una vez se haya producido la causa de la misma.

4.9.5 Periodo de procesamiento de la solicitud de revocación por parte de la AC

La solicitud de revocación una vez llega a uno de los operadores de registro del SESCAM se procesa en el tiempo mínimo posible, con carácter de inmediatez, y siempre dentro de los horarios laborales de los departamentos de registro del SESCAM.

4.9.6 Obligación de consulta de información de revocación de certificados

Los terceros que aceptan certificados del SESCAM podrán verificar el estado de los mismos accediendo al punto de distribución de las listas de revocación del SESCAM, dicha información de localización se encuentra en el propio certificado que se pretende verificar. Así mismo, el SESCAM pone a disposición de los terceros un servicio de validación en línea basado en el protocolo OCSP, cuya información de localización también se encuentra en el certificado emitido.

Los servicios de verificación del estado de revocación de los certificados ofrecidos por el SESCAM (admitidos en el ámbito de la Administración General del Estado) no requerirán obligatoriamente la firma de ningún convenio por parte de las Administraciones Públicas que los utilicen.

SESCAM no impone la obligatoriedad de comprobar el estado de los certificados si bien recomienda la verificación de los mismos.

4.9.7 Frecuencia de emisión de listas de certificados revocados

Las listas de revocación se emiten cada vez que un certificado es revocado o suspendido y se publican como está indicado en *"2.1.2 Frecuencia de Publicación"*.

El SESCAM emite una lista de revocación al menos cada día.

La ARL (Lista de Autoridades Revocadas), esto es, la LCR emitida por la AC Raíz se emite y publica manualmente con suficiente antelación a su expiración.

4.9.8 Tiempo de latencia máximo entre LCRs

Una vez se haya producido una revocación, la autoridad de certificación generará una nueva lista de certificados revocados, que sustituirá a la vigente. La nueva lista de certificados revocados será publicada en el lugar de la antigua tal como se establece en *"2.1.1 Publicación de información de la Autoridad de Certificación"* en un plazo no superior a **una hora**.

4.9.9 Disponibilidad Online de los servicios de comprobación de estado de certificados.

Las listas de revocación pueden ser consultadas en al menos dos repositorios diferentes tal y como se indica en "2.1.1 Publicación de información de la Autoridad de Certificación".

La disponibilidad de ambos repositorios está diseñada para dar servicio 24x7x365.

Además el SESCAM provee servicios de validación en línea propiamente dichos basados en el protocolo OCSP (Online Certificate Status Protocol) tal y como define la norma IETF RFC 2560.

4.9.10 Requerimientos de comprobación online del estado de los certificados

Los verificadores deberán comprobar el estado de aquellos certificados en los que deseen confiar.

Si por cualquier circunstancia no fuera factible obtener información del estado de un certificado, el sistema que deba utilizarlo deberá desestimar su uso, o en función del riesgo, del grado de responsabilidad y de las consecuencias que se pudieran producir, utilizarlo sin garantizar su autenticidad en los términos y estándares que se recogen en esta DPC.

4.9.11 Otros mecanismos de información de revocación de Certificados.

Sin estipular.

4.9.12 Requisitos especiales en caso de compromiso de la clave privada

En caso de compromiso de la clave privada del certificado el suscriptor/poseedor de claves deberá notificar la circunstancia a la Entidad de Registro para que se proceda a solicitar la revocación del certificado, o certificados en el caso de que éste pertenezca a persona física o empleado público.

En caso de compromiso de la clave privada de la AC del SESCAM, se procederá de acuerdo a lo establecido en la sección 5.7.3 de esta DPC.

4.9.13 Supuestos de suspensión

Los certificados de persona física y empleado público emitidos por el SESCAM se podrán suspender de forma cautelar cuando existan indicios sobre la existencia de una causa de revocación.

El resto de certificados contemplados en esta DPC no son susceptibles de suspensión temporal.

4.9.14 Entidades que pueden solicitar la suspensión

Las peticiones de suspensión pueden ser realizadas por:

- El operador de Entidad de Registro previa petición del suscriptor o poseedor de claves.
- El Administrador de la Autoridad de Certificación previa petición y autorización de los oficiales de seguridad del SESCAM.

4.9.15 Procedimiento de suspensión

La suspensión de un certificado de empleado público o persona física, asociado a la tarjeta de un usuario, se podrá realizar remotamente a través de la aplicación GESUSER (procedimiento normal de uso) o localmente en la Entidad de Registro correspondiente.

4.9.15.1 Procedimiento de suspensión de la tarjeta de un usuario en la AR del centro

1. Un operador con los permisos adecuados iniciará sesión en la aplicación de administración de la AR del centro.
2. El operador de la AR ordenará a ésta la suspensión de cualquier tarjeta solicitada con el estado *Finalizada con éxito* (seleccionará los datos del correspondiente registro de la tabla de peticiones de tarjeta de la AR).
3. El servicio de la AR procesará la petición mediante el siguiente procedimiento:
    a. Buscará en la tabla de peticiones de tarjetas de la AR del centro un registro conteniendo una dirección de correo electrónico igual a la contenida en la petición y el estado *Finalizada con éxito*
        i. Si no encuentra el registro, devolverá una respuesta conteniendo el correspondiente error (el usuario no tiene tarjeta o ésta ha sido revocada).
        ii. Si encuentra el registro y el estado contenido en el mismo no es *Finalizada con éxito*, devolverá una respuesta conteniendo el correspondiente error:
        iii. Estados *Pending* o *En proceso*: no se puede suspender la tarjeta porque aún no se ha finalizado su generación.
        iv. Estado *Finalizada con errores*: no se puede suspender la tarjeta porque sus certificados no han sido emitidos o han sido revocados.
    b. Estado *Suspendida*: no se puede suspender la tarjeta porque sus certificados ya han sido suspendidos.
    c. Generará un lote conteniendo la suspensión de los 3 certificados emitidos del usuario (localizados en la tabla de peticiones de la AR a partir de los identificadores contenidos en el registro de la tabla de peticiones de tarjetas) y lo enviará al servicio de procesado de lotes de la AC Subordinada (se suspenderán inmediatamente los 3 certificados del usuario).
    d. Modificará el registro cambiando su estado a *Suspendida.*

4.9.16 Periodo máximo de suspensión

Un certificado una vez suspendido, podrá permanecer en dicho estado hasta el momento de su expiración.

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características de operación de los servicios

Los elementos que sustentan los servicios para albergar las listas de certificados revocados son dos:

- Repositorio Corporativo LDAP del SESCAM
- Repositorio WEB del SESCAM

Los verificadores también podrán consultar el estado de los certificados mediante el protocolo OCSP, en la URL de la Autoridad de Validación del SESCAM.

4.10.2 Disponibilidad de los servicios

Los servicios de descarga de Listas de Certificados Revocados del SESCAM y de consulta en línea del estado de los certificados funcionan 24 horas al día, 7 días a la semana, 365 días al año. El SESCAM dispone de un CPD (Centro de Proceso de Datos) donde dichos repositorios se encuentran situados y monitorizados de forma continua.

4.10.3 Otras funciones de los servicios

Sin estipulación adicional.

4.11 Finalización de la suscripción

La finalización de la suscripción vendrá determinada por la finalización de la relación entre el suscriptor y el SESCAM. En caso de que la misma se produzca antes de que los certificados expiren, se procederá a una revocación de los mismos. En el supuesto de que la relación continúe más allá de la vida de los certificados, se procederá a tantas nuevas emisiones como fuere necesario.

4.12 Depósito y recuperación de claves

4.12.1 Política y prácticas de depósito y recuperación de claves

4.12.1.1 Deposito de claves

En el momento de generación de las claves privadas correspondientes a los certificados adscritos a la política de certificado de cifrado:

Clase de Certificado	Política de Certificado	Nivel	OID Asignado
Empleado Público	Cifrado	Alto	2.16.724.4.8.10.60.10.2.1.1.3
		Medio	2.16.724.4.8.10.60.10.2.1.2.3
Persona Física	Cifrado	NA	2.16.724.4.8.10.60.10.2.2.1
			1.3.6.1.4.1.21835.1.1.3.1

éstas son almacenadas por la Autoridad de Salvaguarda de Claves de la Autoridad de Certificación.

Los mecanismos de protección bajo los cuales están custodiadas dichas claves son los propios del producto de Autoridad de Certificación homologado bajo Common Criteria EAL4+.

4.12.1.2 Recuperación de la clave de cifrado de un usuario

Las claves de cifrado de los usuario serán archivadas cifradas (ofuscadas) por la AC Subordinada del SESCAM .

La recuperación del certificado de cifrado de un usuario del SESCAM se podrá realizar remotamente a través de navegadores Web o localmente en la AC Subordinada del SESCAM, por un conjunto n (configurable) de operadores recuperadores de claves, mediante el siguiente procedimiento:

1. El usuario solicitará el inicio de la recuperación de su clave de cifrado a uno de los operadores recuperadores de claves.
2. El operador recuperador de claves iniciará sesión en la aplicación de administración de la AC Subordinada del SESCAM o se conectará con su Navegador Web al servicio de recuperación de claves autenticándose con certificado e iniciará el proceso de recuperación de la clave de cifrado del usuario (identificada por los datos de su certificado).
3. La AC Subordinada generará una contraseña aleatoria y la dividirá en n trozos (contraseña del PKCS#12 recuperado)
4. Durante el proceso de recuperación, los n trozos permanecerán almacenados en la BD cifrados (ofuscados)
5. La AC Subordinada recuperará la clave privada solicitada y el correspondiente certificado de cifrado y los encapsulará en un PKCS#12 protegido por la contraseña aleatoria (PKCS#12 recuperado)

6. La AC Subordinada entregará el PKCS#12 recuperado y el primer trozo de la contraseña aleatoria que lo protege al operador recuperador de claves y éste se los entregará al usuario
7. El usuario solicitará consecutivamente la continuación de la recuperación de su clave de cifrado a otros n-1 operadores recuperadores de claves.
8. Cada uno de los n-1 operadores recuperadores de claves iniciará sesión en la aplicación de administración de la AC Subordinada del SESCAM o se conectará con su Navegador Web al servicio de recuperación de claves autenticándose con certificado y continuará el proceso de recuperación de la clave de cifrado del usuario (identificada por los datos de su certificado).
9. La AC Subordinada entregará a cada uno de los n-1 operadores recuperadores de claves un trozo distinto de la contraseña aleatoria que protege el PKCS#12 recuperado
10. Cada entrega quedará registrada en la base de datos de la AC Subordinada, de forma que un mismo operador recuperador de claves no pueda recuperar dos trozos.
11. El usuario recompondrá la contraseña y con ella instalará en su Navegador Web o en una tarjeta su clave privada de cifrado y su correspondiente certificado contenidos en el PKCS#12 recuperado.

    Si posteriormente el usuario solicita la recuperación de la misma clave de cifrado, el nuevo PKCS#12 recuperado y la contraseña que lo protege serán distintos pero su contenido será el mismo (la misma clave y el mismo certificado de cifrado).

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de seguridad física

El SESCAM cuenta con diversas instalaciones físicas en las que alberga sus instalaciones informáticas y desde las que presta los servicios informáticos que le son propios. En esta sección se consideran aquellos elementos de protección física para la prestación de los servicios de gestión de certificados, la custodia de los dispositivos criptográficos y de todos aquellos elementos fundamentales y secundarios de la infraestructura de certificación.

5.1.1 Localización y construcción de las instalaciones

El edificio donde quedan emplazadas las instalaciones informáticas de la infraestructura de clave pública del SESCAM se encuentra situado en un área central y concurrida de la ciudad de Toledo, que garantiza la presencia de fuerzas de seguridad de forma rápida y eficaz en el caso de incidentes, si bien existe personal de seguridad permanentemente emplazado en el edificio.

Los muros perimetrales del edificio están construidos con materiales sólidos, encontrándose todas las puertas y ventanas externas protegidas frente a entradas no autorizadas.

El CDP (Centro de Proceso de Datos) se encuentra aislado físicamente en el edificio del resto de departamentos, únicamente personal autorizado del SESCAM puede acceder a éste.

5.1.2 Acceso físico

El SESCAM mantiene diferentes niveles para el acceso físico a las instalaciones de la infraestructura de clave pública, en primer lugar para el acceso al edificio es requerida la identificación frente a los servicios de vigilancia.

El acceso al Centro de Proceso de Datos únicamente puede ser realizado por personal autorizado, existiendo un control de acceso físico mediante huella dactilar para garantizar que así sea. El acceso de visitas a las instalaciones es siempre supervisado y en acompañamiento de personal autorizado del centro.

También se mantiene un registro de accesos a las áreas restringidas que es archivado de forma segura.

5.1.3 Electricidad y aire acondicionado

Las calidad del suministro eléctrico es garantizado frente a posibles variaciones mediante sistemas de protección ante picos y sobrecargas, caídas de tensión, etc.

El SESCAM dispone a su vez de los mecanismos adecuados para garantizar la continuidad del servicio frente a posibles caídas del suministro eléctrico, incluyendo sistemas de generación autónomos que garantizan la operación de los diferentes sistemas durante el tiempo necesario.

Los sistemas de aire acondicionado dentro del centro de proceso de datos se encuentran redundados, de tal forma que se garantiza las condiciones de temperatura y humedad para el correcto funcionamiento de los equipos informáticos durante la caída y consecuente reparación de uno de ellos.

5.1.4 Exposición al agua

La localización del CPD se encuentra en un lugar alejado de posibles inundaciones dentro del propio edificio. Además existen los servicios de detección adecuadas para detectar una posible exposición de los equipos que componen el sistema.

5.1.5 Prevención y protección de incendios

En general todas las dependencias del SESCAM requieren de sistemas de detección y protección contra incendios tal y como marca la legislación vigente al respecto.

En concreto, las instalaciones donde se ubican los sistemas correspondientes al sistema de gestión de certificados del SESCAM, cuentan además con sistemas específicos de detección, protección y extinción, propios de un centro de procesos de datos.

5.1.6 Almacenamiento de soportes

El almacenamiento de las copias de seguridad de los sistemas es realizado de forma segura en primera instancia dentro de las dependencias del propio centro de proceso de datos en armario ignifugo, y en segunda estancia en un centro externo separado geográficamente que garantiza la recuperación del sistema frente a desastres.

Tanto la gestión de las generación de copias como los procedimientos de recuperación exigen roles diferentes.

5.1.7 Tratamiento de residuos

EL SESCAM, para la eliminación de soportes de respaldo de información exige la destrucción física de la misma, tanto en formato magnético como en papel, de tal forma que la recuperación contenida en estos soportes no sea posible.

5.1.8 Copia de seguridad externa a las instalaciones

El SESCAM mantiene un centro secundario para el proceso de datos, este centro qué actúa como centro de respaldo alberga también copias de

seguridad. Los procedimientos de almacenamiento y recuperación de las copias de respaldo del centro primario son de aplicación en este.

5.2 Controles de procedimientos

5.2.1 Perfiles de confianza

La operación de un sistema de confianza requiere que éste sea operado de forma segura y fiable, para ello es necesaria que las diferentes operaciones que se han de realizar sobre el sistema sean realizadas por un perfil determinado. El establecimiento del conjunto de perfiles requeridos para la correcta operación conlleva en primera instancia que el componente tecnológico sobre la que la infraestructura se sustenta permita dicha diferenciación.

El SESCAM utiliza de forma general los perfiles definidos en la norma CEN CWA 14167-1, si bien éstos se han extendidos a las necesidades propias del SESCAM.

El conjunto de Perfiles requeridos por el SESCAM son:

Perfil	Descripción
Oficial de Seguridad	Responsable de la administración e implantación de las políticas y prácticas de seguridad.
Administrador del Sistema	Está autorizado a instalar, configurar y mantener el sistema, con acceso controlado a los aspectos de configuración de seguridad.
Operador del Sistema	Responsable de la operación diaria del sistema, con autorización para llevar a cabo las copias de seguridad y las recuperaciones del sistema.
Auditor del Sistema	Autorizado a acceder en modo lectura a archivos y registros de auditoría del sistema.
Oficial de Registro	Responsable de verificar y aprobar la generación/revocación y suspensión de certificados de entidad final (usuarios).
VIPS	Responsables de la generación de claves y certificado de la Autoridad de Certificación Raíz, asi como del establecimiento de los permisos de uso ésta.
Custodio	Responsable de custodiar el material criptográfico y el acceso al mismo.

5.2.2 Número de personas por tarea

La correcta operación de ciertas funciones dentro del sistema exige que existan un número de personas autorizadas de forma concurrente para que puedan ser realizadas.

Entre dichas funciones se encuentran todas aquellas realizadas sobre la Autoridad de Certificación Raíz, exceptuando las propias de operación (levantamiento y caída) y auditoria del sistema.

5.2.3 Identificación y autenticación para cada perfil

La identificación de cada perfil frente al sistema es realizado mediante tarjetas inteligentes con claves criptográficas, el proceso de entrada al sistema exigirá tantas identificaciones de personas como hayan sido definidas para el perfil pretendido.

5.2.4 Perfiles que requieren separación de tareas

La incompatibilidad de funciones de cada perfil es la preestablecida por la normativa europea CEN CWA 14167-1 para sistemas de confianza. Dicha incompatibilidad es de aplicación para todo el sistema de producción del la infraestructura de clave pública del SESCAM, empero la Autoridad de Certificación raíz, donde la funcionalidad del perfil "oficial de seguridad" es dividido en dos subgrupos incompatibles entre si.

5.3 Controles de personal

5.3.1 Requerimientos de historial, calificaciones, experiencia y autorización

El personal responsable de la operación de los servicios de certificación, firma digital y procedimientos de seguridad se encuentra debidamente capacitado y cualificado en dichas áreas.

Los puestos asociados a perfiles de confianza específica se encuentran libres de intereses de carácter personal ajenos al desarrollo normal de la actividad que prestan. Así mismo, para aquellas tareas consideradas sensibles existe un procedimiento que exige la presencia de un número mínimo y preestablecido de personal cualificado y confiable.

SESCAM no establece requerimientos adicionales respecto al historial del personal involucrado en las operaciones de la infraestructura distintos de los requeridos en cualquiera de los puestos del "Área de Tecnologías de la Información", bajo el cuál opera. La calificación para ejercer los puestos específicos podrá ser obtenida por personal del SESCAM mediante la formación correspondiente.

5.3.2 Procedimientos de revisión de historial

El SESCAM no asignará un perfil de confianza para la gestión u operación del sistema a personal ajeno a la institución, se requiere que toda persona de confianza sea empleado público de la Junta de Comunidades de Castilla la Mancha y estar adscrito como personal del SESCAM. De esta forma queda garantizada la adecuada revisión del historial.

5.3.3 Requerimientos de formación

El personal de la Autoridad de Certificación está sujeto a un plan de formación específico para el desarrollo de su función dentro de la organización.

Dicho plan de formación incluye los siguientes aspectos:

- Formación en los aspectos legales básicos relativos a la prestación de servicios de certificación.
- Formación en seguridad de los sistemas de información.
- Servicios proporcionados por la Autoridad de Certificación.
- Conceptos básicos sobre PKI.
- Declaración de Prácticas de Certificación y las Políticas de Certificación pertinentes.
- Gestión de incidencias.

5.3.4 Requerimientos y frecuencia de actualización formativa

Todo el personal que hace uso de los sistemas de certificación y registro de la infraestructura de clave pública requiere de formación previa a su uso. La actualización de la formación se llevará a cabo cada vez que los cambios en los procedimientos o la tecnología utilizada lo requieran.

5.3.5 Secuencia y frecuencia de rotación laboral

No es de aplicación.

5.3.6 Sanciones para acciones no autorizadas

Para el personal funcionario del SESCAM, el determinado por el "Reglamento de Régimen Disciplinario de Funcionarios de la Administración General del Estado", establecido en el Real Decreto 33/1986.

5.3.7 Requerimientos de contratación de personal externo

La contratación de personal sigue los mismos principios establecidos para la contratación de personal de la Junta de Comunidades de Castilla la Mancha, en este sentido es de aplicación lo establecido en:

- Ley 1/2002, de 7 de febrero, por la que se modifica la Ley 3/1988, de 13 de diciembre, de Ordenación de la Función Pública de la Junta de Comunidades de Castilla-La Mancha
- Estatuto de Autonomía de Castilla-La Mancha
- Ley 3/1988, de 1 de diciembre, de Ordenación de la Función Pública de la Junta de Comunidades de Castilla-La Mancha

5.3.8 Documentación suministrada al personal

El personal adscrito al servicio de la infraestructura de clave pública tendrá acceso a toda la información pública de la misma. Se otorgará acceso a la información privada únicamente a aquellos perfiles que por el tipo de tarea que realizan requieran tener detalles de diseño u operación de elementos específicos.

5.4 Procedimientos de auditoría de seguridad

Para auditar los eventos significativos realizados en el ámbito de la infraestructura de clave pública del SESCAM se utilizará la información contenida en la base de datos de logs de la Autoridad de Certificación.

5.4.1 Tipos de evento

Los tipos de eventos registrados en los logs de la Infraestructura de Clave Pública:

- Operaciones realizadas por los diferentes perfiles de la Autoridad de Certificación, incluyendo:
- Cambio en las políticas de certificados.
- Cambio de usuarios
- Cambio en los perfiles de los usuarios
- Cambio en las claves de la Autoridad
- Operaciones realizadas por los operadores de las Entidades de Registro.
- Eventos relativos al ciclo de vida de los certificados.
- Arranque y parada de los sistemas.
- Registro de accesos e intentos de accesos no autorizados.
- Logs de uso de los dispositivos criptográficos hardware

Todos los eventos incluyen los siguientes datos: categoría, fecha, autor, perfil, tipo evento, id evento, módulo, nivel y observaciones.

De forma manual se llevará a cabo una bitácora de la Infraestructura de clave pública donde serán anotadas todas aquellas eventualidades que afecten a la confianza de la misma, como por ejemplo: ceremonia raíz, registro de visitas, informes de intrusión, etc.

5.4.2 Frecuencia del tratamiento de registros de auditoría

Se establecen dos niveles de auditorías de control de los eventos registros con una frecuencia semanal y mensual respectivamente

5.4.3 .Periodo de conservación de los ficheros de auditoría

Los logs de eventos se mantienen en la base de datos durante toda la vida de la Autoridad de Certificación.

5.4.4 Protección de los ficheros de auditoría

Los ficheros de auditoría generados por la autoridad de certificación y la autoridad de registro son protegidos frente a accesos externos mediante mecanismos de control de acceso lógico. La integridad de la información de dichos ficheros queda garantizada mediante la firma electrónica encadenada de los eventos registrados.

Para el control de ficheros físicos se establecen las adecuadas medidas de seguridad física que impiden su acceso no autorizado.

5.4.5 Procedimiento de copia de seguridad de logs de auditoria

La copia de seguridad de la base de datos de eventos del sistema se realiza con la misma planificación y controles que para el resto de elementos del sistema de certificación, para lo cual se generan copias incrementales locales y remotas diariamente, de acuerdo con la Política de Copias de Seguridad del SESCAM.

5.4.6 Localización del sistema de almacenamiento de registros de auditoría

El almacenamiento de las copias de respaldo de los registros de auditoría es el mismo que el del resto del sistema de certificación.

5.4.7 Notificación del evento de auditoría al causante

Sin estipulación adicional.

5.4.8 Análisis de vulnerabilidad

Los eventos de auditoría registrados son utilizados para verificar posibles vulneraciones al sistema. De forma periódica el SESCAM realiza una comprobación de la integridad de los ficheros de auditoría para constatar que no se han producido vulneraciones al sistema, en el caso de encontrar incidencias o discrepancias se realiza un estudio de las mismas para dilucidar la causa y gravedad de la misma.

5.5 Archivado de información

5.5.1 Tipos de evento y datos registrados

Los tipos de eventos registrados en el archivo son:

- Datos relacionados con el proceso de registro y solicitud de certificados.
- Logs de auditoría de la sección 5.4.1 Tipos de evento.
- Certificados y Listas de Revocación.

- Trazas de Sellos de Tiempo
- Tokens de validación OCSP
- Eventos de error en los procesos realizados.
- En general es registrada toda información concerniente a la gestión de la infraestructura de clave pública y al ciclo de vida de los certificados emitidos por ésta.

5.5.2 Periodo de conservación del archivo de eventos

El archivo de eventos se conserva durante al menos 15 años, desde el momento en que dicho evento se produce.

5.5.3 Protección del archivo de eventos

Los mismos que los declarados para "5.4.4 Protección de los ficheros de auditoría"

5.5.4 Procedimiento de copia de seguridad del archivo de eventos

La copia de seguridad del archivo de eventos del sistema se realiza con la misma planificación y controles que para el resto de elementos del sistema de certificación.

5.5.5 Requerimientos de sellado de tiempo de eventos

Los sistemas del SESCAM realizan el registro del instante de tiempo en los que se realizan. El tiempo de los sistemas proviene de una fuente fiable de hora. Todos los sistemas del SESCAM sincronizan su instante de tiempo con esta fuente.

5.5.6 Localización del sistema de archivo

El almacenamiento de las copias de respaldo de los registros de auditoría es el mismo que el del resto del sistema de certificación.

5.5.7 Procedimientos de obtención y verificación de información de archivo

La obtención y verificación de la información únicamente puede ser realizada por personal autorizado por el SESCAM para tal fin y siempre bajo autorización previa documentada y firmada por el responsable de seguridad de sistemas de información del SESCAM.

5.6 Renovación de claves de una Entidad de Certificación

Los certificados de entidad final emitidos por el SESCAM no son renovables.

Para renovar un certificado de entidad final, debido a que haya sido revocado o haya caducado, se deberá solicitar un nuevo certificado.

5.7 Compromiso de claves y recuperación frente a desastres

5.7.1 Procedimiento de gestión de incidencias y compromisos de seguridad

SESCAM establece los procedimientos para la gestión de incidencias y compromisos de seguridad dentro del marco de su "*Plan frente a contingencias*".

5.7.2 Corrupción de recursos, aplicaciones o datos

SESCAM ha dividido el conjunto de recursos, aplicaciones y datos en diferentes niveles para los cuales ha establecido unas medidas diferentes en el caso de que los mismos se vean corrompidos, a saber:

- ***Autoridad de Certificación raíz***, en este caso existe una copia de backup del sistema y de las claves de la misma, así como el procedimiento y el correspondiente manual para su recuperación.
- ***Servicio de Registro***, este sistema no es considerado crítico, el mismo se mantiene distribuido en la organización. La recuperación implica la revocación de la Autoridad de Registro y la generación de una nueva según el procedimiento al uso, existiendo un manual de instalación y puesta en marcha del mismo.
- Los servicios de ***Revocación de Certificado***s y ***Estado de Certificados*** se encuentran redundados en el centro secundario. En caso de corrupción del sistema se procederá a la restauración de los mismos.
- ***Servicio de Emisión de Certificados, Sellado de Tiempo y Validación en Línea (OCSP)***, se encuentran redundados en el centro secundario. En caso de corrupción del sistema primario los sistemas del centro secundario continúan la operación.

5.7.3 Compromiso de la clave privada de la Entidad de Certificación.

En caso de que la autoridad de certificación de producción se vea comprometida la autoridad de certificación raíz procederá a la revocación inmediata de la misma, publicando y notificando de forma inmediata el suceso al resto de componentes del sistema mediante la generación de la correspondiente LAR (Lista de Autoridades Revocadas).

En caso de compromiso de la clave privada de la AC raíz, queda comprometido el sistema por completo, se generará la notificación inmediata a todos los elementos sostenidos bajo el paraguas de confianza del sistema, suspendiéndose toda actividad de forma cautelar, hasta que se pueda generar un nuevo marco de confianza mediante la generación de un nuevo certificado raíz.

5.7.4 Desastre sobre las instalaciones

En el caso en el que exista un desastre sobre las instalaciones del centro primario, se procederá a la activación de los elementos necesarios en el centro secundario a efectos de garantizar la continuidad de los sistemas.

5.8 Fin de servicio

En caso de finalización de servicio de su sistema de certificación, el SESCAM comunicará el fin, por cualquier medio que garantice el envío y la recepción de la notificación, a todos los suscriptores con certificados en vigor con la antelación suficiente.

El SESCAM cumplirá con las obligaciones previstas por el artículo 21 de la Ley 59/2003 de 19 de Diciembre.

6 CONTROLES TECNICOS DE SEGURIDAD

6.1 Generación e instalación del par de claves

6.1.1 Generación par de claves

Para la generación de las claves raíz de la jerarquía del SESCAM se procedió de acuerdo con la ceremonia de claves, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.

La generación de claves de las Entidades de Confianza (Autoridades de Certificación, Validación y Sellado de Tiempo) es realizada en dispositivos hardware criptográfico conformes a la norma FIPS 140-2 Level3 y durante el proceso se exige que existan al menos un número mínimo de personas designadas por el SESCAM con privilegios de acceso a la Entidad de Confianza.

El proceso de generación de claves de Operadores de la Entidad de Registro será realizado por los mecanismos propios que ofrezca la autoridad de registro. Así mismo, las claves de estos deberán ser generadas en una Tarjeta Criptográfica.

Para los certificados de entidad final se sigue el consiguiente proceso:

Certificado	Nivel	Método de Generación
Sede Electrónica Administrativa	Alto	Generación de claves por el usuario en HSM. Emisión sin generación de claves y entrega en formato PKCS#7 o X509v3
Sello Electrónico para actuación Automatizada	Alto	
Empleado Público Autenticación Firma	Alto Medio	Generación de claves por el usuario en SSCD (Tarjeta Inteligente). Emisión e inyección de certificados en SSCD (Tarjeta Inteligente)
Empleado Público Cifrado	Alto Medio	Generación de claves por la Autoridad de Certificación. Backup de PKCS#12 y password ofuscada en Sistema de Recuperación de Claves. Inyección de PKCS#12 (claves y certificados)

		en SSCD (Tarjeta Inteligente).
Persona Física Autenticación Firma	NA	Generación de claves por el usuario en SSCD (Tarjeta Inteligente). Emisión e inyección de certificados en SSCD (Tarjeta Inteligente)
Persona Física Cifrado	NA	Generación de claves por la Autoridad de Certificación. Backup de PKCS#12 y password ofuscada en Sistema de Recuperación de Claves. Inyección de PKCS#12 (claves y certificados) en SSCD (Tarjeta Inteligente).
Sede Electrónica Administrativa	Medio	Generación de claves por el usuario en software o en HSM. Emisión sin generación de claves y entrega en formato PKCS#7 (soporte software o hardware).
Sello Electrónico para actuación Automatizada	Medio	
Dispositivo Servidor SSL Aplicaciones Controlador de Dominio Firma de Código	NA	

6.1.2 Entrega del par de claves al suscriptor

Las claves de los certificados de Personas físicas y Empleado Público son entregadas debidamente protegidas mediante una tarjeta criptográfica que cumpla con los requisitos establecidos por la Ley 59/2003 de dispositivo de creación de firma seguro.

Las claves las claves de cifrado pueden ser recuperadas únicamente a petición justificada del subcriptor por un conjunto n de m, donde n será mayor a 3, de Oficiales de Recuperación de Claves. Estas claves serán entregadas en formato PKCS#12.

Las claves de las Sede, Sello y Dispositivos residen en el mismo dispositivo y por lo tanto no necesitan ser entregadas.

6.1.3 Entrega clave pública al emisor del certificado

Las claves públicas de los operadores de Registro generadas en la tarjeta criptográfica se entregan a la Autoridad de Certificación mediante una petición de certificación en formato PKCS#10.

Las claves públicas de Personas físicas y Empleado Público de Autenticación y de No-Repudio generadas en la tarjeta criptográfica son enviadas a la Autoridad de Certificación por la Autoridad de Registro mediante una petición de certificación en formato PKCS#10. La clave pública de cifrado es generada por la Autoridad de Certificación y por lo tanto no necesita ser entregada a ésta.

Las claves de las Entidades Finales de dispositivos generadas por el mismo dispositivo son enviadas a la Autoridad de Certificación mediante una petición de certificación en formato X.509 o PKCS#10.

6.1.4 Distribución clave publica de la AC

Las claves públicas de la Autoridad de Certificación del SESCAM se distribuyen a través de varios medios, entre ellos la publicación en la WEB del SESCAM. En la presente Declaración de Prácticas de Certificación, apartado 1.3.2 se publican además las huellas SHA1de los correspondientes certificados

6.1.5 Tamaños de claves

El tamaño de las claves RSA utilizadas en el SESCAM es el siguiente:

- 4096 bits para la Autoridad de Certificación raíz.
- 2048 bits para la Autoridad de Certificación Subordinada, la Autoridad de Validación y la Autoridad de Sellado de Tiempo.
- Al menos 1024 bits para los Operadores de registro.
- 2048 bits para la emisión de certificados de Nivel Medio para Entidades Finales, ya sea personas físicas o dispositivos.
- Al menos 1024 bits para la emisión de certificados de personas físicas o dispositivos.
- 1024 bits para la emisión de certificados de Nivel Medio de empleado público ya sea personas físicas o dispositivos.

6.1.6 Generación parámetros de clave pública

Los parámetros de clave pública son generados conforme a PKCS#1, utilizándose como segunda pareja de la clave pública, **FERMAT 4**.

6.1.7 Comprobación calidad parámetros de clave pública

Los parámetros de generación de las claves generados por dispositivo hardware criptográfico están garantizados por la certificación de la norma FIPS 140-1 Nivel 3.

Los parámetros de generación de las claves generadas en tarjeta criptográfica están certificados Common Criteria y/o son conformes con la norma CEN CWA 14169.

6.1.8 Generación claves en Hardware/Software

La generación de las claves se realiza en los siguientes dispositivos Hardware/Software:

- Entidades de Confianza (AC, AV, AST): en dispositivo criptográfico hardware.
- Operadores de registro: en la propia tarjeta criptográfica
- Entidades Finales (personas físicas y empleado público): en la propia tarjeta criptográfica las claves de Autenticación y no-repudio y en la Autoridad de Certificación con procedimientos software las de cifrado.
- Entidades Finales (Sede, Sello y dispositivos): en el propio dispositivo con los procedimientos hardware/software que incorporen.

6.1.9 Propósitos de uso de claves

La utilización de una clave se determina mediante la extensión *KeyUsage* y *ExtKeyUsage*, presentes en todos los certificado.

6.2 Protección clave privada

6.2.1 Estándares de módulos criptográficos

La infraestructura de clave pública del SESCAM hace uso de módulos criptográficos hardware certificados FIPS 140-1 Nivel 3.

Las tarjetas criptográficas utilizadas cumplen con los requisitos establecidos en la norma CEN CWA 14169 o equivalente, estando homologados bajo CC EAL 4+ o superior., aunque también son admisibles certificaciones equivalentes ITSEC E3 o FIPS 140-2 Level 2.

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

La utilización de la clave privada de la Autoridad de Certificación Raíz requiere 4 de las 6 posibles personas para la generación del certificado raíz, y 2 de las 6 posibles para la generación/revocación de certificados de Autoridad de Certificación Subordinada, y de 1 de 6 para la generación de la LAR (Lista de Autoridades Revocadas).

6.2.3 Deposito de la clave privada

Únicamente existe depósito de claves para los certificados de Entidad Final de Persona Física destinadas a proveer cifrado, la autoridad de certificación mediante la funcionalidad de salvaguarda de claves es la responsable de la custodia y acceso a las mismas.

6.2.4 Copia de seguridad de la clave privada

Para las Autoridades de Certificación se dispone de dos conjuntos de seis tarjetas de recuperación inicial para el módulo criptográfico, correspondientes a cada una de las Autoridades de Certificación del

SESCAM. También, se mantienen seis tarjetas de activación de la clave privada, de las cuales son necesarias dos.

El resto de claves del sistema susceptibles de copia de respaldo reside ofuscada en la Base de Datos del SESCAM, de la cual se generan las correspondientes copias tal y como se ha descrito en *"5.1.6 Almacenamiento de soportes".*

6.2.5 Archivo de clave privada

Los certificados generados por la AC, y por lo tanto las claves públicas, son almacenados por la AC durante el periodo de tiempo obligado por la legislación vigente.

Las claves privadas de cifrado, generadas por la Autoridad de certificación se almacenan ofuscadas en la base de datos de ésta, de forma que solo los administradores designados o los propios suscriptores podrán recuperarlas.

Las medidas de protección de la información custodiada por el Sistema de salvaguardia de claves garantizan que no sea posible la entrega de claves y de su custodia en claro.

No se archivan claves privadas de autenticación o firma de usuarios finales.

6.2.6 Introducción de la clave privada en el modulo criptográfico

Se consideran los siguientes casos:

- ***Autoridad de Certificación:*** Las claves privadas quedan almacenadas en ficheros cifrados con claves fragmentadas y en tarjetas inteligentes. Estas tarjetas son utilizadas para introducir la clave privada en el módulo criptográfico.
- ***Operadores de registro:*** la clave privada se genera en la propia tarjeta criptográfica y no hace falta importarla.
- ***Entidades Finales (personas físicas y empleado público):*** la claves privadas de Autenticación y No-repudio se generan en la propia tarjeta criptográfica mientras que la de cifrado es introducida en la tarjeta por la autoridad de registro.
- ***Entidades Finales (dispositivos):*** la clave privada se genera en el propio dispositivo y no hace falta importarla.

6.2.7 Almacenamiento de la clave privada en Modulo criptográfico.

Con la excepción de los certificados de cifrado de Entidad Final que son almacenados con posterioridad a su generación en tarjeta criptográfica, el resto de claves privadas asociadas a dispositivo criptográfico son generadas por éstos y no requieren un almacenamiento posterior.

6.2.8 Método de activación de la clave privada

Para la Autoridad de Certificación y el Sistema de recuperación de claves la clave privada es activada por el grupo de oficiales de seguridad correspondiente.

Para los operadores de registro y las entidades finales de tipo persona física y empleado público, en posesión de una tarjeta criptográfica, las claves privadas se activan con el PIN de la tarjeta misma.

Para los dispositivos las claves privadas son activadas por los correspondientes administradores con contraseñas.

6.2.9 Método de desactivación de la clave privada

Para la Autoridad de Certificación y el Sistema de recuperación de claves la clave privada es desactivada por un administrador finalizando la aplicación.

Para los operadores de registro y las entidades finales en posesión de una tarjeta criptográfica, las claves privadas se desactivan extrayendo la tarjeta del lector.

6.2.10 Método de destrucción de la clave privada

Las claves privadas son destruidas de forma que se impida su robo, modificación, divulgación no autorizada o uso no autorizado. En el caso de claves de usuario en soporte tarjeta mediante la destrucción física de ésta. La destrucción de claves de dispositivo o firma de código no son contempladas por está DPC.

6.2.11 Clasificación de los módulos criptográficos

Los dispositivos criptográficos utilizados por las entidades de confianza (AC, AV y AST) están homologados FIPS 140-1 nivel 3.

Los dispositivos de criptográficos software utilizados por las autoridades de registro están homologados CC EAL4+, bajo el PP CIMC.

Las tarjetas inteligentes utilizadas por suscriptores de certificados están al menos homologadas CC EAL 4+, y cumplen además lo definido por la norma europea CEN CWA 14169.

6.3 Otros aspectos de la gestión del par de claves

6.3.1 Archivo de la clave pública

Los certificados generados por la AC, y por lo tanto las claves públicas, son almacenados por la AC durante el periodo de tiempo obligado por la legislación vigente.

6.3.2 Periodo de utilización de las claves pública y privada

Corresponde con el periodo de validez de cada certificado.

6.4 Datos de activación

6.4.1 Generación e instalación de los datos de activación

Las claves privadas asociadas a los certificados de entidades finales de tipo personas físicas o empleado público asociadas a una tarjeta inteligente requieren para su activación de un PIN. Este PIN es seleccionado por el suscriptor en el momento de realizar la correspondiente solicitud, dicho PIN se graba en la tarjeta sustituyendo el PIN por defecto.

6.4.2 Protección de los datos de activación

Los datos de activación de la Autoridad de Certificación y de las Autoridades de Registro son conocidos sólo por los correspondientes administradores.

Los PINs y contraseñas asociadas a los certificados de entidades finales deben ser memorizados y no almacenados escritos junto con los dispositivos que albergan las claves privadas.

6.4.3 Otros aspectos de los datos de activación

No se definen limitaciones sobre el tiempo de vida de los datos de activación.

6.5 Controles de seguridad informática

6.5.1 Requisitos técnicos específicos de la seguridad informática

Para garantizar la confiabilidad de la infraestructura de clave pública el SESCAM mantiene un conjunto de controles de seguridad sobre los diferentes elementos que lo componen.

El conjunto de controles de seguridad implantados por el SESCAM quedan divididos según:

- Controles Operacionales
    - Mantenimiento de una Política de Seguridad que engloba el Sistema de Clave Pública, esta política contiene detalles particulares de los requerimientos de seguridad y medidas de salvaguarda a implementar y la forma de usarlos correctamente para alcanzar una seguridad adecuada en consonancia con los objetivos de la organización.
    - SESCAM mantiene una estructura organizativa para la seguridad, que sin menos cabo de los roles específicos de seguridad requeridos por la Infraestructura de clave pública, está formada por:
        - *Comité de Seguimiento*, grupo designado por el Comité de Dirección, responsable del seguimiento de los proyectos y de los contratos establecidos dentro del marco de aplicación definido en el Plan Director.

- *Responsable de Seguridad*, es la persona encargada de establecer, comunicar y gestionar las políticas, planes y procedimientos de seguridad necesarios para proteger los activos de la organización en función del riesgo asumible y a un coste razonable.
- *Equipo de Seguridad*, personal especializado que se encarga de poner en marcha y administrar el conjunto de medidas de salvaguarda aprobadas en el Plan de Seguridad, monitorizando la seguridad del sistema para que se mantenga dentro de los límites establecidos.

- El SESCAM dispone de un plan de contingencia para la recuperación de los equipos y sistemas de clave pública.
- Los sistemas del SESCAM disponen de herramientas que garantizan su protección frente a ataques provocados por virus informáticos o códigos software maliciosos.
- El SESCAM dispone de herramientas de monitorización de sistemas y detección de intrusiones al mismo.
- Todas aquellas tareas sensibles quedan documentadas para su posterioridad auditoría.
- El conjunto de funciones para la operación del sistema de certificación y registro están reguladas por una política de seguridad reflejada en las aplicaciones.

- Controles de Acceso
  - Existen controles de acceso físico basados en huella dactilar de los que se mantiene registro a las dependencias donde se hallan los sistemas de información. Únicamente el personal autorizado puede acceder a estos sistemas.
  - Los diferentes usuarios del sistema de clave pública disponen de una tarjeta inteligente que contiene sus credenciales.
  - Para aquella información gestionada por el SESCAM de carácter personal se establece los procedimientos de consulta, modificación y borrado exigidos por la LOPD.
  - Los niveles de acceso son revisados de forma periódica.
- Identificación y Autenticación
  - La identificación de los usuarios frente a los sistemas de clave pública es realizada mediante tarjeta inteligente.
  - El uso de perfiles de seguridad sensibles exige la entrada concurrente en el sistema por un conjunto de n de m usuarios autorizados.
  - Las conexiones telemáticas entre los diferentes componentes y actores del sistema de clave pública se realiza mediante conexiones seguras autenticadas extremo a extremo, utilizando protocolos como TLS o IPSec, siendo las comunicaciones cifradas.

- Nivel de Seguridad de los productos utilizados, en la medida de las posibilidades para los diferentes productos utilizados por el SESCAM se exigen las correspondientes homologaciones Common Criteria que sean de relevancia de los servicios soportados por éstos. En concreto los productos para la gestión de la vida de los certificados y aquellos que han de generar y custodiar las claves privadas, es decir, los dispositivos criptográficos, tendrán una homologación CC EAL4+ o superior.
- Disponibilidad de los sistemas, el SESCAM dispone de un centro de proceso de datos secundario donde se encuentran redundados aquellos sistemas y subsistemas críticos para la operativa diaria de la organización.
- Auditoría de la seguridad, de forma regular el SESCAM realiza auditorías de seguridad que incluyen test de penetración a sus sistemas.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones basadas en los productos KeyOne de AC (Autoridad de Certificación) y AR (Autoridad de Registro) son fiables, de acuerdo con la especificación técnica CEN CWA 14167-1, evaluándose el grado de cumplimiento mediante un perfil de protección adecuado, de acuerdo con la norma CIMC. Igualmente, dichas aplicaciones se encuentran homologadas por el CCN (Centro Criptológico Nacional).

De forma periódica se evalúan las características (vulnerabilidades, riesgos y costes de los mecanismos de seguridad implantados o a implantar) para la arquitectura tecnológica establecida. Dicha evaluación se entrega al Comité de Seguimiento para su valoración.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Los servicios de seguridad soportados por una Infraestructura de Clave Pública (PKI) constituyen la herramienta principal a la hora de garantizar la autoría, la integridad, la confidencialidad y el no repudio en una gran variedad de eventos en aplicaciones del SESCAM basadas en Internet/Intranet, como el control de acceso, correo seguro o el gobierno electrónico.

Las entidades finales que van a hacer uso de las funcionalidades y servicios proporcionados por la infraestructura de clave pública del SESCAM, principalmente empleados, a través de sus aplicaciones de cliente y, servidores de aplicaciones o aplicaciones en general, harán uso de la tecnología de clave pública para múltiples propósitos: identificación y autenticación, control de acceso, firma digital, cifrado, etc.

El SESCAM vigila que dichas aplicaciones que hacen uso de los servicios ofrecidos por su infraestructura cumplan con los requerimientos y las premisas establecidas en esta DPC para el uso de los mismos, introduciendo los controles pertinentes en su metodología de desarrollo software y de implantación de sistemas.

6.6.2 Controles de gestión de seguridad

El SESCAM mantiene establecido el siguiente conjunto de controles para la correcta gestión de la seguridad:

- Comprobación de la integridad de los sistemas de Bases de Datos utilizados por los sistemas de Certificación.
- Comprobación de correcto funcionamiento de los sistemas.
- Comprobación periódica de configuraciones de seguridad de los diferentes elementos, tales como: bases de datos, sistemas operativos, componentes de red, directorios LDAP, etc.

Además, se mantiene actualizado el plan de sistemas de la infraestructura de clave pública mediante una detección temprana de necesidades funcionales y organizativas del SESCAM que requieran del uso de la infraestructura.

6.6.3 Evaluación del nivel de seguridad del ciclo de vida

De forma periódica se evalúan las características (vulnerabilidades y riesgos de los mecanismos de seguridad implantados) para la arquitectura tecnológica establecida. Dicha evaluación se entrega al Comité de Seguimiento para su valoración.

6.7 Controles de seguridad de la red

El SESCAM garantiza el correcto uso y acceso de los sistemas que conforman su infraestructura de clave pública mediante el siguiente conjunto de controles de seguridad de red implantados en sus sistemas:

- Cortafuegos para proteger la red interna frente a accesos externos no autorizados. Los cortafuegos se configuran de forma que se impidan accesos y protocolos que no sean necesarios para la operación del sistema, actuando como primera barrera de seguridad perimetral.
- Medidas anti-spoofing y frente ataques de denegación de servicio.
- Uso de protocolos seguros, confidenciales y autenticados, entre los elementos que conforman la infraestructura de clave pública.
- Mantenimiento en alta disponibilidad mediante clusterización de routers y firewalls.
- Mantenimiento de centro de respaldo que garantiza la continuidad de los servicios de red críticos del SESCAM.
- Controles de acceso físico y lógico a los diferentes dispositivos de red.
- Monitorización de estado de los diferentes elementos de la red.

6.8 Sello de Tiempo

El tiempo se obtiene mediante consulta a los servidores de Tiempo de la Consejería de Presidencia y Administraciones Públicas de la JCCM, la cual está sincronizada con el Real Observatorio de la Armada[3], siguiendo el protocolo NTP a través de Internet. La descripción del protocolo NTP se puede encontrar en el RFC 1305 "*Network Time Protocol*".

[3] http://www.armada.mde.es/ArmadaPortal/page/Portal/ArmadaEspannola/ciencia_observatorio/06_Hora

7 PERFILES DE CERTIFICADOS Y LISTAS DE REVOCACION

7.1 Perfil de certificados

Los certificados emitidos por el SESCAM serán conformes con las siguientes normas:

- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, May 2008
- ISO/IEC 9594-8/ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
- ETSI TS 102 042 v2.1.1 (2009-05). Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 101 456 v1.4.3 (2007-05) : Policy requirements for certification authorities issuing qualified certificates.
- ETSI TS 101 862 V1.3.1 (2004-03): Qualified Certificate Profile, 2004
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (prevaleciendo en caso de conflicto la TS 101 862)
- Esquema de Identificación y Firma - Perfiles de Certificados v.1.7.6, del Consejo Superior de Administración Electrónica (prevaleciendo en caso de conflicto la TS 101 862)

Así mismo se ha tomado en consideración la siguiente recomendación a la hora de establecer los perfiles reconocidos:

- Interoperable Qualified Certificate Profiles, Study on Cross-Border Interoperability of eSignatures (CROBIES), final report.

7.1.1 Número de versión

Los certificados emitidos por el SESCAM son X.509 versión 3, según la norma ISO/IEC 9594-8/ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

7.1.2 Extensiones del certificado

Las extensiones utilizadas de forma generalizada en los certificados emitidos por el SESCAM son:

- KeyUsage. Marcada como crítica
- Basic Constraints. Marcada como crítica.

- Certificate Policies. Marcada como no Crítica.
- Subject Alternative Name. Marcada como no crítica.
- CRL Disitrution Point. Marcada como no crítica
- Authority Information Access. Marcada como no crítica.
- QCStatements. Marcada como no crítica.

Dependiendo del perfil de certificado emitido el SESCAM puede establecer un conjunto de extensiones diferentes para cada certificado. El anexo A describe el conjunto completo de certificados emitidos bajo está DPC.

7.1.3 Identificadores de objeto (OID) de los algoritmos

Identificador de Objeto (OID) del algoritmo Criptográfico utilizado por el SESCAM:

SHA-1 with RSA Encryption (1.2 840.113549.1.1.5)

7.1.4 Formatos de nombres

Los certificados emitidos por el SESCAM contienen el distinguished name X.500 del emisor y el subscriptor del certificado en los campos issuer name y subject name respectivamente.

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a distinguished names X.500, únicos y no ambiguos.

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

Los certificados emitidos bajo esta DPC, sólo utilizarán los OIDs definidos en la sección 1.2.

7.1.7 Uso de la extensión "PolicyConstraints"

Sin estipulación adicional

7.1.8 Sintaxis y semántica de los "PolicyQualifier"

La extensión 'Certificate Policies' podrá contener los siguientes 'Policy Qualifiers', dependiendo del tipo de certificado a que refiera.

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

- User Notice (EN): Nota de texto en inglés con objeto de promover los aspectos de interoperabilidad y reconocimiento de los certificados del SESCAM en el ámbito internacional.

En el anexo A de este documento se puede encontrar la información contenida para cada perfil emitido bajo está DPC.

7.2 Perfil de Listas de Revocación

7.2.1 Número de versión

El formato de las LCRs utilizadas en la presente política es el especificado en la versión 2 (X509 v2).

7.2.2 LCR y extensiones

La presente Declaración de Prácticas de Certificación soporta y utiliza LCRs conformes al estándar X.509.

En el Anexo A se encuentra una definición detallada de los perfiles de LCR emitidos bajo esta DPC.

7.3 Perfil de Autoridad de Sello de Tiempo

Los certificados de Autoridad de Sellado de Tiempo serán emitidos por la Autoridad de Certificación subordinada y serán conformes con las siguientes normas:

- IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, May 2008
- ISO/IEC 9594-8/ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
- IETF RFC 3161 Time-Stamp Protocol (TSP)

El perfil de certificado de la Autoridad de Sellado de Tiempo se puede encontrar en el Anexo A de esta DPC.

7.4 Perfil de Autoridad de Validación

Los certificados de Autoridad de Validación serán emitidos por la Autoridad de Certificación subordinada y serán conformes con las siguientes normas:

- IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, May 2008
- ISO/IEC 9594-8/ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
- IETF RFC 2560 Online Certificate Status Protocol - OCSP

El perfil de certificado de la Autoridad de Validación se puede encontrar en el Anexo A de esta DPC.

8 Auditoría de conformidad

El SESCAM verificará la conformidad de que el sistema de clave pública que mantiene y explota cumple con los requisitos procedimentales, técnicos, operacionales y de seguridad necesarios para la prestación de los servicios de certificación que provee.

La ejecución de las auditorías de conformidad podrá ser llevada por personal interno del SESCAM, si bien podrá delegarse a una entidad externa.

8.1 Frecuencia de la auditoría de conformidad

La frecuencia de auditorías de conformidad es realizada de forma periódica, al menos una vez al año, las mismas serán planificadas según los requerimientos y necesidades operaciones del sistema, así como del conjunto de actividades objeto de la auditoría.

El tipo de auditorías podrá ser en todo caso parcial sobre elementos o funciones concretas del sistema.

8.2 Identificación y cualificación del auditor

EL SESCAM exigirá la independencia y experiencia contrastada en Sistemas de Clave Pública en los procesos de contratación o delegación de auditorías a entidades externas. Cualquier empresa o persona contratada para realizar una auditoría de seguridad sobre la AC del SESCAM deberá cumplir con los siguientes requisitos:

- Adecuada y acreditada capacitación y experiencia en PKI, seguridad y procesos de auditoría de sistemas de información.
- Independencia a nivel organizativo de la autoridad del SESCAM, para el caso de auditorías externas.

En el caso de auditorías internas será exigible la adecuada capacitación al personal responsable de realizar la auditoría.

8.3 Relación del auditor con la entidad auditada

El SESCAM podrá emplear auditores internos o externos siempre y cuando los mismos sean funcionalmente independientes del sistema o servicio objeto de auditoría.

8.4 Relación de elementos objeto de auditoría

Los elementos objeto de auditoría en el marco de esta DPC son los siguientes:

- Ceremonia de la Autoridad de Certificación Raíz.
- Procesos relacionados con la gestión propia de los servicios de gestión de certificados llevados a cabo por la Autoridad de Certificación.
- Proceso relacionados con los procedimientos de registro de suscriptores.
- Sistemas de Información.
- Seguridad de los Centros de Procesos de Datos
- Aplicaciones corporativas del SESCAM que hacen uso de los certificados.
- Documentación

8.5 Acciones a emprender como resultado de una falta de conformidad

Una vez se haya detectado una no-conformidad por la auditoría se procederá a establecer un plan de acciones correctivas para subsanar la posible deficiencia, con posterioridad se verificará que las acciones planificadas han resuelto adecuadamente la no-conformidad.

En caso de que existan no-conformidades que no puedan ser resueltas y que afecten a la seguridad, integridad, confiabilidad o continuidad de los servicios se procederá según el Plan de Contingencia.

8.6 Tratamiento de los informes de auditoría

Los informes de auditoría serán entregados al Comité de Seguridad y al Responsable de seguridad del SESCAM para su evaluación.

9 Requisitos legales

9.1 Tarifas

El uso de los servicios prestados por el SESCAM no estipula una tarifa para sus suscriptores.

9.2 Capacidad Financiera

Todos y cada uno de los certificados emitidos en el ámbito del SESCAM bajo las Políticas de Certificación definidas no admiten ninguna responsabilidad económica que se pudiera derivar del uso de los mismos.

El SESCAM establece asimismo las relaciones jurídicas y contractuales que vinculan a los suscriptores y verificadores en caso de infracción de sus obligaciones o de la legislación aplicable.

9.2.1 Seguro de responsabilidad civil

El SESCAM dispone de una garantía de cobertura de su responsabilidad civil suficiente, en los términos previstos en el artículo 20.2 de la Ley 59/2003, de 19 de diciembre.

9.2.2 Otros activos

Sin estipulación adicional.

9.2.3 Cobertura de aseguramiento para suscriptores y terceros que confíen en certificados

Sin estipulación adicional.

9.3 Confidencialidad

9.3.1 Información confidencial

La siguiente información es considerada como sensible por el SESCAM cuando actúa como prestador de servicios de certificación, y por tanto se implantan las medidas de protección necesarias para su acceso y tratamiento:

Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.

- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.

- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por el prestador de servicios de certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como "Sensible".
- Se protege el acceso a las tarjetas de Operación y Administración de los módulos criptográficos que dan soporte a la Entidad de Certificación, así como los números de serie y activación de los soportes criptográficos hardware.
- Se protegen la palabras de paso de acceso a los diferentes roles presentes en la plataforma, no debiendo difundirse en ningún caso entre miembros de perfiles incompatibles y entre los miembros del mismo grupo.

9.3.2 Información no confidencial

La información indicada a continuación no es considerada de carácter confidencial:

- Certificados emitidos y sus estados.
- Nombre, apellidos y dirección de correo del suscriptor del certificado.
- Las listas de revocación (LCR).
- La declaración de prácticas de certificación (DPC) y las políticas de certificación (PC)
- Toda información no clasificada como "Confidencial" y no incluida en la sección 9.3.1 Información confidencial de esta DPC.

9.4 Protección de datos personales

9.4.1 Plan de Protección de Datos Personales

El SESCAM mantiene un plan de protección de datos personales de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, y al Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Para la prestación del servicio, el SESCAM recaba y almacena ciertas informaciones, que incluyen datos personales. Tales informaciones se recaban directamente de los afectados, con su consentimiento explícito o en los casos en los que la ley permita recabar la información sin consentimiento del afectado.

9.4.2 Información considerada privada

De conformidad con lo establecido en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se consideran datos de carácter personal cualquier información relativa a personas físicas identificadas o identificables.

La información personal que no haya de ser incluida en los certificados y en el mecanismo indicado de comprobación del estado de los certificados, es considerada información personal de carácter privado.

La siguiente información es considerada en cualquier caso privada:

- Claves privadas de suscriptores generadas o salvaguardadas por la Autoridad de Certificación.
- Solicitudes de certificado, aprobadas o denegadas.
- Datos personales requeridos y utilizados durante el proceso de registro.
- Registro de transacciones.
- Plan de seguridad de sistemas y de continuidad de negocio y de emergencia.
- Toda información clasificada como "Confidencial".

La información confidencial de acuerdo con la LOPD es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

9.4.3 Información no considerada privada

No se considera información privada de carácter personal aquella que es incluida en el certificado expedido al suscriptor, tampoco aquella información que permita a los verificadores validar el estado del certificado de un suscriptor.

La información de carácter personal incluida en los certificados es recabada durante la solicitud de los mismos, advirtiendo al suscriptor en los mismo términos que la ley de firma electrónica 59/2003 prevé.

9.4.4 Responsabilidad correspondiente a la protección de los datos personales

El SESCAM es responsable último de la correcta protección de los datos de carácter personal, para ello garantiza el cumplimiento de sus obligaciones legales.

9.4.5 Prestación del consentimiento en el uso de los datos personales

El SESCAM obtiene el consentimiento de los titulares de los datos necesarios para prestación los servicios de certificación mediante la aceptación

firmada por parte del suscriptor de la solicitud de certificación y de la retirada de los certificados por parte de este.

9.4.6 Divulgación de la información originada por procedimientos administrativos y/o judiciales.

EL SESCAM está obligada a revelar la identidad de los firmantes a requerimiento de los órganos judiciales en el ejercicio de las funciones que tengan atribuidas y resto de supuestos previstos en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre ,de la Protección de Datos de Carácter Personal donde fuere requerido.

9.4.7 Otros supuestos de divulgación de la información

No han sido contemplados otros supuestos de divulgación adicionales.

9.5 Derechos de propiedad intelectual

El SESCAM es la entidad que mantiene los derechos de propiedad intelectual sobre la Declaración de Practicas de Certificación y de las diferentes Políticas de Certificado que gobiernan el ciclo de vida de éstos. Igualmente SESCAM es el propietario en exclusiva de los certificados y listas de revocación que emite.

La propiedad exclusiva de las claves generadas corresponde a sus suscriptores, al igual que los nombres relativos a éstos y que le son propios. Así mismo el suscriptor mantiene el derecho sobre nombre distinguido que aparece en el certificado y que le identifica.

Los OIDs utilizados por esta DPC y por cada Política de Certificado para su nombramiento único son propiedad del SESCAM, quién tiene registrados los siguientes arcos para su uso exclusivo:

- IANA (Internet Assigned Number Authority) bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1.IANA-Registered Private Enterprises), habiendo asignado ésta al SESCAM el identificador de objetos ***1.3.6.1.4.1. 21835***.
- El Sistema Nacional de Salud, que asigna al SESCAM el arco 2.16.724.4.8.10 para su utilización.

La gestión y uso de este OID es exclusiva del SESCAM no pudiendo ser utilizado en forma alguna por terceras partes excepto para el uso que se describe para cada uno de los especificados en esta DPC y en las correspondientes Políticas de Certificación.

9.6 Obligaciones y Responsabilidad Civil

La presentación de servicios de confianza del SESCAM es responsabilidad de la Administración, la cual se asienta sobre bases objetivas y cubre toda lesión que los particulares sufran siempre que sea consecuencia del funcionamiento normal o anormal de los servicios públicos.

9.6.1 Obligaciones de la Autoridad de Certificación

El SESCAM cuando actúa como Prestador de Servicios de Confianza bajo las directivas definidas en esta DPC asume las siguientes obligaciones:

- Emitir los certificados solicitados en cumplimiento de las normas y procedimientos establecidos en esta DPC, en las políticas de certificación (PC) y en las leyes vigentes.
- Cumplir con los requerimientos de seguridad física, de procedimientos, personales y técnicos definidos en su plan de seguridad.
- Proteger sus claves privadas.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación prestados.
- Emplear personal cualificado y debidamente formado en los procesos a realizar para la prestación del servicio ofrecido.
- Emitir los certificados en cumplimiento del estándar X.509 y de los requerimientos de la petición.
- Publicar las políticas de certificación y esta DPC en la ubicación indicada en los documentos y en los propios certificados
- Revocar / Suspender los certificados siguiendo los procedimientos descritos en la sección 4.3 y publicar la nueva LCR en la ubicación indicada en los Perfiles de Certificación.
- Mantener un registro con la información relativa a los certificados emitidos que pueda ser consultado solamente por personal autorizado.
- Cumplir con todos los requerimientos de la normativa sobre protección de datos de carácter personal.
- Garantizar que puede determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.
- Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.
- Archivar las claves de los certificados de cifrado de forma segura.
- Operar de acuerdo con la legislación aplicable. En concreto se asumen como textos de referencia los siguientes, pertenecientes al marco legislativo Español:
    - 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.
    - La Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
    - Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
    - Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

9.6.2 Obligaciones de la Autoridad de Registro

La autoridad de registro asume las siguientes obligaciones:

- Comprobar la identidad y los datos del solicitante y del suscriptor conforme a los procedimientos establecidos en esta DPC y el las Políticas de Certificación especificas de cada tipo de certificado.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación prestados.
- Emplear personal cualificado y debidamente formado en los procesos a realizar para la prestación del servicio ofrecido.
- Enviar las peticiones de certificación en cumplimiento del estándar X.509.
- Gestionar los procedimientos de suspensión / revocación y renovación de certificados según los procedimientos descritos en la sección 4.3.

9.6.3 Obligaciones de los suscriptores

El solicitante del certificado está obligado a:

- Garantizar que toda la información aportada durante el proceso de registro de la petición del certificado es cierta y correcta.
- Solicitar el certificado siguiendo el procedimiento definido en la sección 4.1 Solicitud de certificados.

El suscriptor del certificado está obligado a:

- Aceptar las directivas establecidos en esta DPC y en las Políticas de Certificación.
- Notificar inmediatamente a la Autoridad de Registro de cualquier información incorrecta que haya sido incluida en el certificado.
- Custodiar de forma diligente los certificados, las claves, el soporte de las mismas y los códigos de activación.
- Notificar inmediatamente a la Autoridad de registro la pérdida, el robo o cualquier compromiso potencial de sus claves privadas.
- Solicitar la Suspensión / Revocación de los certificados cuando se den las condiciones descritas en la sección 4.3 y según los procedimientos allí definidos.
- Aceptar que sus certificados sean publicados en un repositorio común y público.
- Utilizar los certificados adecuadamente y para los usos especificados en esta DPC y en las Políticas de certificación específicas.
- La responsabilidad derivada del uso de los certificados pertenecientes a esta infraestructura de clave pública vendrá en todo caso impuesta por el reglamento disciplinario de aplicación en el ámbito del SESCAM para los certificados de persona física empleado del SESCAM.

9.6.4 Obligaciones de terceras partes verificadoras

Las terceras partes que confiarán en los certificados están obligadas a:

- Cumplir con la legislación vigente aplicable al uso de los certificados.
- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones de los certificados y la Política de Certificación pertinente.
- Obtener y verificar todos los certificados de la cadena de confianza antes de confiar en la firma digital o en alguno de los certificados de la jerarquía.
- Verificar la validez de los certificados a través de las Listas de Revocación obtenidas con una frecuencia no superior a 24 horas o mediante el uso de los servicios puestos a disposición por el SESCAM o por otros organismos de la Administración Pública.
- No comprometer de forma intencionada o por negligencia la seguridad de los servicios de certificación.

9.6.5 Obligaciones del repositorio

La presente DPC asume la integridad y veracidad de la información contenida en el repositorio. Es responsabilidad del repositorio implementar y operar los procedimientos y mecanismos de seguridad que garanticen la disponibilidad del mismo, así como la veracidad e integridad de la información contenida en el mismo.

El SESCAM mantiene publicadas las siguientes informaciones en el repositorio:

- Los certificados de las entidades de confianza.
- Las listas de certificados revocados y otras informaciones de estado de revocación de certificados.
- Las Declaraciones de Prácticas de Certificación.

9.7 Renuncias de garantías

La infraestructura de clave pública del SESCAM podrá renunciar a todas las garantías del servicio que presta y que no se encuentren vinculadas a las obligaciones establecidas por la Ley 59/2003 de firma electrónica.

9.8 Limitaciones de responsabilidad

EL SESCAM limita su responsabilidad a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y dispositivos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado) suministrados por el SESCAM.

El SESCAM sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando no haya consignado en él, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo. No responderá cuando el firmante supere los límites que

figuran en la política del certificado en cuanto a sus posibles usos y no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante. Tampoco responderá el SESCAM si el destinatario de los documentos firmados electrónicamente no comprueba y tiene en cuenta las restricciones que figuran en éste en cuanto a sus posibles usos.

9.9 Indemnizaciones

No se establecen cláusulas de indemnidad de los suscriptores ni de los verificadores.

9.10 Plazo y finalización

9.10.1 Plazo

El SESCAM establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina el período de vigencia de la relación jurídica en virtud de la que suministran certificados a los suscriptores

9.10.2 Finalización

El SESCAM establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, una cláusula que determina las consecuencias de la finalización de la relación jurídica en virtud de la que suministran certificados a los suscriptores.

9.10.3 Efectos de finalización y supervivencia

El SESCAM establece, en sus instrumentos jurídicos con los suscriptores y los verificadores, cláusulas de supervivencia, en virtud de la que ciertas reglas continúan vigentes después de la finalización de la relación jurídica reguladora del servicio entre las partes.

9.11 Notificaciones

Los suscriptores y verificadores de certificados de entidad final deberán notificar a los responsables de las Autoridades Registro cualquier suceso que afecte a la seguridad de sus claves o a la continuidad de su relación con el SESCAM. Dichas comunicaciones deberán realizarse bien mediante el envío de un correo electrónico al servicio de registro de la entidad que gestiono la solicitud o bien de forma presencial.

No se establecen procedimientos particulares para otras notificaciones entre participes de la PKI, cuándo sea necesario la notificación podrá realizarse de la forma más ágil y efectiva posible, siempre y cuando quede constancia de la misma.

9.12 Modificaciones

9.12.1 Procedimiento para modificaciones

El SESCAM podrá modificar esta declaración de prácticas de certificación (DPC) y sus políticas de certificación (PC).

Los cambios aportados deberán garantizar el mantenimiento del nivel de calidad exigido y tendrán que ser justificados desde el punto de vista legal, técnico y procedimental.

Se establece un sistema de numeración para el mantenimiento de las versiones y el numero de versión se añadirá al nombre de la DPC ("DPC del SESCAM Versión 1") como indicado en la sección 1.2 Identificación.

9.12.2 Periodo y mecanismos para notificaciones

La entrada en vigor de una nueva DPC se comunicará a los suscriptores a través del depósito *"2.1 Repositorios"* con una antelación de 30 días. Pasados los 30 días se podrá retirar la referencia al cambio y la nueva DPC entrará en vigor.

9.12.3 Circunstancias en las que un OID tiene que ser cambiado

Sin estipulación adicional.

9.13 Resolución de conflictos

En caso de existir disputas relacionadas con los servicios o disposiciones contempladas por esta Declaración de Prácticas de Certificación, las partes se someterán a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa.

9.14 Legislación aplicable

El SESCAM establece, en sus documentos jurídicos vinculantes con suscriptores y terceros que confían en los certificados, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española.

En la presente DPC se asumen como textos de referencia los siguientes, pertenecientes al marco legislativo Español:

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- La Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- 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.
- Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

9.15 Conformidad con la ley aplicable

El SESCAM declara que la presente DPC cumple con las prescripciones contenidas en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

9.16 Cláusulas diversas

9.16.1 Acuerdo íntegro

Ninguno de los términos de esta Declaración de Prácticas de Certificación que afecte directamente a los derechos y obligaciones del SESCAM y que no afecte al resto de las partes, puede ser corregido, renunciado, suplementado, modificado o eliminado si no es mediante documento escrito autenticado del SESCAM.

9.16.2 Subrogación

Los derechos, deberes y obligaciones asociados a las Autoridades de Certificación del SESCAM no podrán ser objeto de cesión a terceros. En el caso de subrogación del servicio, se procederá a la finalización de las Autoridades de Certificación.

9.16.3 Divisibilidad

En el caso que una o más cláusulas de esta DPC sea o llegase a ser inválida, ilegal, o inexigible legalmente, tal inaplicabilidad no afectará a ninguna otra cláusula, sino que se actuará entonces como si las cláusula o cláusulas inaplicables nunca hubieran sido contenidas por esta DPC, y en tal grado como sea posible se interpretará la DPC para mantener la voluntad original de la misma.

9.16.4 Fuerza Mayor

En caso de fuerza mayor se atenderá a lo establecido en la cláusula 9.8 Limitaciones de Garantía.

9.17 Otras cláusulas

Sin estipulación adicional.

A. Anexo A. Perfiles de Certificados

NOTA: Las extensiones sombreadas son CRITICAS.

A.1 Perfiles de Entidades de Confianza

A.1.1 CA Raíz

A.1.1.1 Perfil de Certificado

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	SESCAM Root CA
Validity	NotBefore	Fecha de emisión del certificado
	NotAfter	NotBefore + 30 Años
Subject	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	SESCAM Root CA
subjectyPublicKeyInfo	Clave pública	Clave RSA – tamaño 4096
Extensiones estándar		
subjectKeyIdentifier	Ident. de clave pública del sujeto	Hash de la clave pública generado automáticamente
keyUsage	Uso de la clave	keyCertSign, cRLSign
CertificatePolicies	Policy Identifier	2.5.29.32.0 *(anyPolicy)*
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
BasicConstraints	CA	TRUE

A.1.1.2 Perfil de ARL

Campo CRL v2	Nombre	Valor
Versión	Versión de CRL	Versión 2
signatureAlgorithm	Algoritmo de firma digital	pkcs1-sha1WithRsaSignature
Issuer	C (País)	Es
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	SESCAM Root CA
thisUpdate	Fecha de la CRL	Calculado de forma automática
nextUpdate	Fecha de generación de la próxima CRL	+ 3 años
CRL Extensions		
authorityKeyIdentifier	Id.de clave pública del emisor	Calculado de forma automática – Mismo valor que la extensión subjectKeyIdentifier del certificado de la CA Raíz
cRLNumber	Número secuencial de CRL	Calculado de forma automática
IssuingDistributionPoint	Punto de distribución de la lista.	http://sescam.jccm.es/pki/crls/sescam_root_ca.crl
Certificados Revocados (1 entrada por certificado)		
serialNumber	Número de serie	Número de serie de los certificados revocados
invalidityDate	Fecha de Rev.	Fijado automáticamente.
reasonCode	Razón	Razón suministrada por el operador. Valores posibles: Unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6)

A.1.2 CA Subordinada 2010
A.1.2.1 Perfil de Certificado

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio, asignado por la CA Raíz
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	SESCAM Root CA
Validity	NotBefore	Fecha de emisión del certificado
	NotAfter	NotBefore + 25 Años
Subject	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	SESCAM CA Entidades Finales
subjectyPublicKeyInfo	Clave pública	Clave RSA – tamaño 2048
Extensiones estándar		
subjectKeyIdentifier	Ident. de clave pública del sujeto	Hash de la clave pública generado automáticamente
authorityKeyIdentifier	Identificador de la clave pública del emisor	Calculado de forma automática – Mismo valor que la extensión subjectKeyIdentifier del certificado de la CA Raíz
keyUsage	Uso de la clave	keyCertSign, cRLSign
CertificatePolicies	Policy Identifier	2.5.29.32.0 *(anyPolicy)*
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
BasicConstraints	CA	TRUE
	PathLenConstraint	0
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_root_ca.crl

A.1.2.2 Perfil de CRL

Campo CRL v2	Nombre	Valor
Versión	Versión de CRL	Versión 2
signatureAlgorithm	Algoritmo de firma digital	pkcs1-sha1WithRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	SESCAM CA Entidades Finales
thisUpdate	Fecha de la CRL	Calculado de forma automática
nextUpdate	Fecha de generación de la próxima CRL	+ 1 día
CRL Extensions		
authorityKeyIdentifier	Id.de clave pública del emisor	Calculado de forma automática – Mismo valor que la extensión subjectKeyIdentifier del certificado de la CA Subordinada
cRLNumber	Número secuencial de CRL	Calculado de forma automática
IssuingDistributionPoint	Punto de distribución de la lista.	http://sescam.jccm.es/pki/crls/sescam_subord_ca.crl
Certificados Revocados (1 entrada por certificado)		
serialNumber	Número de serie	Número de serie de los certificados revocados
invalidityDate	Fecha de Rev.	Fijado automáticamente.
reasonCode	Razón	Razón suministrada por el operador. Valores posibles: Unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6)

A.1.3 CA Subordinada 2012

A.1.3.1 Perfil de Certificado

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio, asignado por la CA Raíz
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	SESCAM Root CA
Validity	NotBefore	Fecha de emisión del certificado
	NotAfter	NotBefore + 25 Años
Subject	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
subjectyPublicKeyInfo	Clave pública	Clave RSA – tamaño 2048
Extensiones estándar		
subjectKeyIdentifier	Ident. de clave pública del sujeto	Hash de la clave pública generado automáticamente
authorityKeyIdentifier	Identificador de la clave pública del emisor	Calculado de forma automática – Mismo valor que la extensión subjectKeyIdentifier del certificado de la CA Raíz
keyUsage	Uso de la clave	keyCertSign, cRLSign
CertificatePolicies	Policy Identifier	2.5.29.32.0 *(anyPolicy)*
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
	User Notice (ES)	Los certificados emitidos bajo está política son emitidos por el SESCAM para ACs subordinadas de la AC raiz del SESCAM
	User Notice (EN)	Certificates issued under this policy are issued by the SESCAM Root CA to CAs subordinate to the SESCAM Root CA
BasicConstraints	CA	TRUE
	PathLenConstraint	0
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_root_ca.crl

Campo x509v3	Nombre	Valor
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp
	Access Location (Localización)	• http://sescam.jccm.es/va

A.1.3.2 Perfil de CRL

Campo CRL v2	Nombre	Valor
Versión	Versión de CRL	Versión 2
signatureAlgorithm	Algoritmo de firma digital	pkcs1-sha1WithRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
thisUpdate	Fecha de la CRL	Calculado de forma automática
nextUpdate	Fecha de generación de la próxima CRL	+ 1 día
CRL Extensions		
authorityKeyIdentifier	Id.de clave pública del emisor	Calculado de forma automática – Mismo valor que la extensión subjectKeyIdentifier del certificado de la CA Subordinada
cRLNumber	Número secuencial de CRL	Calculado de forma automática
IssuingDistributionPoint	Punto de distribución de la lista.	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl[4]

[4] *La Autoridad de Certificación hace uso de CRLs Particionadas por tamaño, de forma que cada 1000 certificados se emite una nueva CRL. En este sentido, la extensión IssuingDistributionPoint hará referencia al lugar y nombre de publicación de la CRL a la que corresponde, el nombre completo del fichero de CRL hace uso de la variable crlID (identificador único de CRL) para ser compuesto.*

Campo CRL v2	Nombre	Valor
Certificados Revocados (1 entrada por certificado)		
serialNumber	Número de serie	Número de serie de los certificados revocados
invalidityDate	Fecha de Rev.	Fijado automáticamente.
reasonCode	Razón	Razón suministrada por el operador. Valores posibles: Unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6)

9.18 Autoridad de Validación

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio, asignado por la CA Subordinada
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 6 meses
Subject	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	Autoridad Validación SESCAM
subjectyPublicKeyInfo	Clave pública	Clave RSA – tamaño 2048
Extensiones estándar		
subjectKeyIdentifier	Ident. de clave pública del sujeto	Hash de la clave pública generado automáticamente
authorityKeyIdentifier	Identificador de la clave pública del emisor	Calculado de forma automática – Mismo valor que la extensión subjectKeyIdentifier del certificado de la CA Raíz
keyUsage	Uso de la clave	digitalSignature
Extended KeyUsage	Uso extendido de la clave	OCSP Signing
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.1.2
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
BasicConstraints	CA	False
	PathLenConstraint	Ninguno
CRLDistributionPoints	Punto de distribución de la CRL	URL=http://sescam.jccm.es/pki/crls/sescam_subca_C8D77C1F1D166CCC39141F46DF3A1F409D08C5B4.crl
ocspNoCheck	No comprobar por OCSP	null

A.2 Autoridad de Sellado de Tiempo

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio, asignado por la CA Subordinada
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	Fecha de emisión del certificado
	NotAfter	NotBefore + 25 Años
Subject	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	Autoridad de Sellado de Tiempo del SESCAM
subjectyPublicKeyInfo	Clave pública	Clave RSA – tamaño 2048
Extensiones estándar		
subjectKeyIdentifier	Ident. de clave pública del sujeto	Hash de la clave pública generado automáticamente
authorityKeyIdentifier	Identificador de la clave pública del emisor	Calculado de forma automática – Mismo valor que la extensión subjectKeyIdentifier del certificado de la CA Raíz
keyUsage	Uso de la clave	Digital Signature
Extended KeyUsage	Uso extendido de la clave	TimeStamping
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.1.1
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
BasicConstraints	CA	False
	PathLenConstraint	Ninguno
CRLDistributionPoints	Punto de distribución de la CRL	URL=http://sescam.jccm.es/pki/crls/sescam_subca_C8D77C1F1D166CCC39141F46DF3A1F409D08C5B4.crl

A.3 Perfiles de Persona Física

A.3.1 Perfil de Certificado de Persona Física para Autenticación

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	DN (Nombre distintivo)	Dependiendo de si el certificado ha sido emitido por la SubCA 2010 o la SubCA 2012, el campo Issuer podrá tener uno de los dos siguientes valores a) CN=SESCAM CA Entidades Finales, O=SESCAM (NIF Q-4500146H), O=JCCM, C=ES b) CN=SESCAM CA Entidades Finales, SERIALNUMBER=Q4500146H, O=JCCM, OU=SESCAM, C=ES
Subject	C (Pais)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM
	UID (User Identity>	[Número de identificación único del suscriptor del certificado. Se corresponde con el UID o con el DNI/NIE]
	Title (Cargo)	[Cargo del subscriptor]
	CN (Nombre)	Etiqueta constante **NOMBRE** Espacio en blanco [Apellidos y Nombre del titular del certificado en MAYÚSCULAS] Espacio en blanco Guión Espacio en blanco Etiqueta constante **NIF** Espacio en blanco [Número de identificación fiscal]
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 4 años
subjectyPublicKeyInfo	Clave pública	Clave RSA ≥ 1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Digital signature
extKeyUsage	Uso de clave extendido	ClientAuthentication,

Campo x509v3	Nombre	Valor
		emailProtection, Microsoft Smart Card Logon
NetscapeCertType	Uso de clave extendido	SSL client
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.2.1
		1.3.6.1.4.1.21835.1.1.3.1 [5]
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
	User Notice	Este es un Certificado de Autenticación cuya clave privada está soportada por una Tarjeta Inteligente y cuyo único objeto es el de ser utilizado para autenticar a su subscritor.
	User Notice	This is an Authentication Certificate whose private key is supported by a Smart Card and it is aimed to be used exclusively to authenticate its owner.
BasicConstraints	EC	FALSE
	PathLenContraint	Ninguno
SubjectAltName	UPN	[UPN para realizar SmartCardLogon]
	rfc822Name	[Correo electrónico del subcriptor]
CRLDistributionPoints	Punto de distribución de la CRL	Para certificados emitidos por la SubCA 2010: • http://sescam.jccm.es/pki/crls/sescam_subord_ca.crl Para certificados emitidos por la SubCA 2012: • http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp
	Access Location (Localización)	http://sescam.jccm.es/va

[5] *Para certificados emitidos antes de [fecha puesta en producción del proyecto]*

A.3.2 Perfil Certificado de Persona Física para No-Repudio

A.3.2.1 Reconocido

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos ($1 – 2^{159}$)
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	DN (Nombre distintivo)	Dependiendo de si el certificado ha sido emitido por la SubCA 2010 o la SubCA 2012, el campo Issuer podrá tener uno de los dos siguientes valores a) CN=SESCAM CA Entidades Finales, O=SESCAM (NIF Q-4500146H), O=JCCM, C=ES b) CN=SESCAM CA Entidades Finales, SERIALNUMBER=Q4500146H, O=JCCM, OU=SESCAM, C=ES
Subject	C (Pais)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM
	UID (User Identity>	[Número de identificación único del suscriptor del certificado. Se corresponde con el UID o con el DNI/NIE]
	Title (Cargo)	[Cargo del subscriptor]
	CN (Nombre)	Etiqueta constante **NOMBRE** Espacio en blanco [Apellidos y Nombre del titular del certificado en MAYÚSCULAS] Espacio en blanco Guión Espacio en blanco Etiqueta constante **NIF** Espacio en blanco [Número de identificación fiscal 9 caracteres]
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 4 años
subjectyPublicKeyInfo	Clave pública	Clave RSA ≥ 1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	contentCommitment

Campo x509v3	Nombre	Valor
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.2.2
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
	User Notice	Este es un Certificado Reconocido cuya clave privada está soportada por un dispositivo de creación de firma seguro y cuyo único objeto es el de ser utilizado para generar firmas avanzadas reconocidas
	User Notice	This is a Qualified Certificate whose private key is supported by a Secure Signature Creation Device and it is aimed to be used exclusively to create Qualified Electronic Signatures
Qualified Certificate Statements	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*
	QCEURetentionPeriod	15 años
	QCSSCD	0.4.0.1862.1.4 *Nota: Indica que la clave está en un SSCD*
BasicConstraints	EC	FALSE
	PathLenContraint	Ninguno
SubjectAltName	rfc822Name	[Correo electrónico del subcriptor]
CRLDistributionPoints	Punto de distribución de la CRL	Para certificados emitidos por la SubCA 2010: • http://sescam.jccm.es/pki/crls/sescam_subord_ca.crl Para certificados emitidos por la SubCA 2012: • http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp
	Access Location (Localización)	http://sescam.jccm.es/va

A.3.2.2 Ordinario

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	CN (Nombre)	SESCAM CA Entidades Finales
Subject	C (Pais)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM
	UID (User Identity>	[Número de identificación único del suscriptor del certificado. Se corresponde con el UID o con el DNI/NIE]
	Title (Cargo)	[Cargo del subscriptor]
	CN (Nombre)	[Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte)]
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 4 años
subjectyPublicKeyInfo	Clave pública	Clave RSA ≥ 1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Non-Repudiation
CertificatePolicies	Policy Identifier	1.3.6.1.4.1.21835.1.1.3.2 [6]
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
	User Notice	Limitaciones de garantías de este certificado se pueden encontrar en la DPC.
BasicConstraints	EC	FALSE
	PathLenContraint	Ninguno
SubjectAltName	rfc822Name	[Correo electrónico del subcriptor]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subord_ca.crl

[6] *Para certificados emitidos antes de [fecha puesta en producción del proyecto]*

A.3.3 Perfil Certificado de Persona Física para Cifrado

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	DN (Nombre distintivo)	Dependiendo de si el certificado ha sido emitido por la SubCA 2010 o la SubCA 2012, el campo Issuer podrá tener uno de los dos siguientes valores a) CN=SESCAM CA Entidades Finales, O=SESCAM (NIF Q-4500146H), O=JCCM, C=ES b) CN=SESCAM CA Entidades Finales, SERIALNUMBER=Q4500146H, O=JCCM, OU=SESCAM, C=ES
Subject	C (Pais)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM
	UID (User Identity>	[Número de identificación único del suscriptor del certificado. Se corresponde con el UID o con el DNI/NIE]
	Title (Cargo)	[Cargo del subscriptor]
	CN (Nombre)	Etiqueta constante **NOMBRE** Espacio en blanco [Apellidos y Nombre del titular del certificado en MAYÚSCULAS] Espacio en blanco Guión Espacio en blanco Etiqueta constante **NIF** Espacio en blanco [Número de identificación fiscal]
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 4 años
subjectyPublicKeyInfo	Clave pública	Clave RSA ≥ 1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Key Encipherment, Data Encipherment
extKeyUsage	Uso de clave extendido	ClientAuthentication, emailProtection
NetscapeCertType	Uso de clave extendido	SSL client

Campo x509v3	Nombre	Valor
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.2.3
		1.3.6.1.4.1.21835.1.1.3.3 [7]
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
	User Notice	Este es un Certificado de Cifrado cuya clave privada está soportada por una Tarjeta Inteligente y cuyo único objeto es el de ser utilizado para cifrar información
	User Notice	This is an Encryption Certificate whose private key is supported by a Smart Card and it is aimed to be used exclusively to encrypt information.
BasicConstraints	EC	FALSE
	PathLenContraint	Ninguno
SubjectAltName	rfc822Name	[Correo electrónico del subcriptor]
CRLDistributionPoints	Punto de distribución de la CRL	Para certificados emitidos por la SubCA 2010: • http://sescam.jccm.es/pki/crls/sescam_subord_ca.crl Para certificados emitidos por la SubCA 2012: • http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp
	Access Location (Localización)	http://sescam.jccm.es/va

[7] *Para certificados emitidos antes de [fecha puesta en producción del proyecto]*

A.4 Perfiles de Empleado Público

A.4.1 Perfil Certificado Empleado Público de Autenticación

A.4.1.1 Nivel Alto

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos (1 – 2^{159})
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	SESCAM
	OU (Organizational Unit)	certificado electrónico de empleado público
	OU (Organizational Unit)	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	OU (Organizational Unit)	[Número de identificación del suscriptor del certificado. Se corresponde con el UID]
	Title (Cargo)	[Puesto o cargo del empleado público]
	SerialNumber	[Corresponderá al DNI/NIE del empleado]
	Surname (Apellidos)	[Primer apellido, espacio en blanco, segundo apellido del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	Given Name (Nombre)	[Nombre de pila del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	CN (Nombre Común)	[Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI.]
subjectyPublicKeyInfo	Clave pública	Clave RSA de 2048
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la	Mismo valor que la extensión

Campo x509v3	Nombre	Valor		
	llave pública del emisor	subjectKeyIdentifier de la CA		
keyUsage	Uso de la clave	digitalSignature		
extKeyUsage	Uso de clave extendido	EmailProtection clientAuthentication Microsoft Smart Card Logon		
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.1.1.1		
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html		
	User Notice (ES)	Este es un Certificado Reconocido cuya clave privada está soportada por una Tarjeta Inteligente y cuyo único objeto es el de ser utilizado para autenticar al empleado público.		
	User Notice (EN)	This is a Qualified Certificate whose private key is supported by a Smart Card and it is only aimed to be used exclusively to authenticate a public employee.		
Qualified Certificate Statements	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*		
	QCEURetentionPeriod	15 años		
	QCSSCD	0.4.0.1862.1.4 *Nota: Indica que la clave esta en un SSCD*		
SubjectAltName	Rfc822Name	[Correo electrónico de contacto del suscriptor]		
	UserPrincipalName	[UPN para realizar SmartCardLogon]		
	Directory Name			
	Nombre	OID	Valor	
	Tipo certificado	2.16.724.1.3.5.3.1.*1*	certificado electrónico de empleado público	
	Nombre Entidad	2.16.724.1.3.5.3.1.2	[entidad subscriptora]	
	NIF Entidad	2.16.724.1.3.5.3.1.3	[NIF entidad subscriptora]	
	DNI/NIE Responsable	2.16.724.1.3.5.3.1.4	[DNI/NIE Responsable]	
	Número de Identificación del personal	2.16.724.1.3.5.3.1.5	[Número de identificación del suscriptor del certificado. Eg: UID]	
	Nombre	2.16.724.1.3.5.3.1.6	[Nombre de pila del responsable del certificado de acuerdo con el DNI/NIE]	
	Primer Apellido	2.16.724.1.3.5.3.1.7	[Primer apellido del responsable del certificado de acuerdo con el DNI/NIE]	
	Segundo Apellido	2.16.724.1.3.5.3.1.8	[Segundo Apellido del responsable del certificado de acuerdo con el DNI/NIE]	
	Correo electrónico responsable	2.16.724.1.3.5.3.1.9	[Correo del responsable del certificado de acuerdo con el DNI/NIE]	
	Unidad Organizativa	2.16.724.1.3.5.3.1.10	[Unidad de la Adm. en la que está incluida el suscriptor del certificado]	
	Puesto o cargo	2.16.724.1.3.5.3.1.11	[Puesto desempeñado]	
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl		

Campo x509v3	Nombre	Valor
		Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp
	Access Location (Localización)	http://sescam.jccm.es/va

A.4.1.2 Nivel Medio

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos (1 – 2^{159})
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	SESCAM
	OU (Organizational Unit)	certificado electrónico de empleado público
	OU (Organizational Unit)	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	OU (Organizational Unit)	[Número de identificación del suscriptor del certificado. Se corresponde con el UID]
	Title (Cargo)	[Puesto o cargo del empleado público]
	SerialNumber	[Corresponderá al DNI/NIE del empleado]
	Surname (Apellidos)	[Primer apellido, espacio en blanco, segundo apellido del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	Given Name (Nombre)	[Nombre de pila del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	CN (Nombre Común)	[Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI.]

Campo x509v3	Nombre	Valor	
subjectyPublicKeyInfo	Clave pública	Clave RSA de 1024	
Extensiones estándar			
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente	
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA	
keyUsage	Uso de la clave	digitalSignature	
extKeyUsage	Uso de clave extendido	EmailProtection clientAuthentication Microsoft Smart Card Logon	
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.1.2.1	
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html	
	User Notice (ES)	Este es un Certificado Reconocido cuya clave privada está soportada por un dispositivo de creación de firma seguro y cuyo único objeto es el de ser utilizado para autenticar al empleado público.	
	User Notice (EN)	This is a Qualified Certificate whose private key is supported by a Secure Signature Creation Device and it is aimed to be used exclusively to authenticate a public employee.	
Qualified Certificate Statements	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*	
	QCEURetentionPeriod	15 años	
SubjectAltName	Rfc822Name	[Correo electrónico de contacto del suscriptor]	
	UserPrincipalName	[UPN para realizar SmartCardLogon]	
	Directory Name		
	Nombre	OID	Valor
	Tipo certificado	2.16.724.1.3.5.3.2.*1*	certificado electrónico de empleado público
	Nombre Entidad	2.16.724.1.3.5.3.2.2	[entidad subscriptora]
	NIF Entidad	2.16.724.1.3.5.3.2.3	[NIF entidad subscriptora]
	DNI/NIE Responsable	2.16.724.1.3.5.3.2.4	[DNI/NIE Responsable]
	Numero de Identificación del personal	2.16.724.1.3.5.3.2.5	[Número de identificación del suscriptor del certificado. Eg: UID]
	Nombre	2.16.724.1.3.5.3.2.6	[Nombre de pila del responsable del certificado de acuerdo con el DNI/NIE]
	Primer Apellido	2.16.724.1.3.5.3.2.7	[Primer apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Segundo Apellido	2.16.724.1.3.5.3.2.8	[Segundo Apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Correo electrónico responsable	2.16.724.1.3.5.3.2.9	[Correo del responsable del certificado de acuerdo con el DNI/NIE]

Campo x509v3	Nombre	Valor	
	Unidad Organizativa	2.16.724.1.3.5.3.2.10	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	Puesto o cargo	2.16.724.1.3.5.3.2.11	[Puesto desempeñado]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.	
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp	
	Access Location (Localización)	http://sescam.jccm.es/va	

A.4.2 Perfil de Certificado Empleado Público de No-Repudio

A.4.2.1 Nivel Alto

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos ($1 - 2^{159}$)
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	SESCAM
	OU (Organizational Unit)	certificado electrónico de empleado público
	OU (Organizational Unit)	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	OU (Organizational Unit)	[Número de identificación del suscriptor del certificado. Se corresponde con el UID]
	Title (Cargo)	[Puesto o cargo del empleado público]

Campo x509v3	Nombre	Valor
	SerialNumber	[Corresponderá al DNI/NIE del empleado]
	Surname (Apellidos)	[Primer apellido, espacio en blanco, segundo apellido del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	Given Name (Nombre)	[Nombre de pila del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	CN (Nombre Común)	[Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI.]
subjectyPublicKeyInfo	Clave pública	Clave RSA de 2048
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Content Commitment
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.1.1.2
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
	User Notice (ES)	Este es un Certificado Reconocido cuya clave privada está soportada por un dispositivo de creación de firma seguro y cuyo único objeto es el de ser utilizado para generar firmas avanzadas reconocidas
	User Notice (EN)	This is a Qualified Certificate whose private key is supported by a Secure Signature Creation Device and it is aimed to be used exclusively to create Qualified Electronic Signatures
Qualified Certificate Statements	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*
	QCEURetentionPeriod	15 años
	QCSSCD	0.4.0.1862.1.4 *Nota: Indica que la clave esta en un SSCD*
SubjectAltName	Rfc822Name	[Correo electrónico de contacto del suscriptor]
	Directory Name	

Nombre	OID	Valor
Tipo certificado	2.16.724.1.3.5.3.1.1	certificado electrónico de empleado público
Nombre Entidad	2.16.724.1.3.5.3.1.2	[entidad subscriptora]
NIF Entidad	2.16.724.1.3.5.3.1.3	[NIF entidad subscriptora]
DNI/NIE Responsable	2.16.724.1.3.5.3.1.4	[DNI/NIE Responsable]
Numero de Identificación del personal	2.16.724.1.3.5.3.1.5	[Número de identificación del suscriptor del certificado. Eg: UID]
Nombre	2.16.724.1.3.5.3.1.6	[Nombre de pila del

Campo x509v3	Nombre	Valor	
			responsable del certificado de acuerdo con el DNI/NIE]
	Primer Apellido	2.16.724.1.3.5.3.1.7	[Primer apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Segundo Apellido	2.16.724.1.3.5.3.1.8	[Segundo Apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Correo electrónico responsable	2.16.724.1.3.5.3.1.9	[Correo del responsable del certificado de acuerdo con el DNI/NIE]
	Unidad Organizativa	2.16.724.1.3.5.3.1.10	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	Puesto o cargo	2.16.724.1.3.5.3.1.11	[Puesto desempeñado]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.	
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp	
	Access Location (Localización)	http://sescam.jccm.es/va	

A.4.2.2 Nivel Medio

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos ($1 – 2^{159}$)
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	SESCAM
	OU (Organizational Unit)	certificado electrónico de empleado público
	OU (Organizational Unit)	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]

Campo x509v3	Nombre	Valor
	OU (Organizational Unit)	[Número de identificación del suscriptor del certificado. Se corresponde con el UID]
	Title (Cargo)	[Puesto o cargo del empleado público]
	SerialNumber	[Corresponderá al DNI/NIE del empleado]
	Surname (Apellidos)	[Primer apellido, espacio en blanco, segundo apellido del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	Given Name (Nombre)	[Nombre de pila del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	CN (Nombre Común)	[Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI.]
subjectyPublicKeyInfo	Clave pública	Clave RSA de 1024

Extensiones estándar			
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente	
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA	
keyUsage	Uso de la clave	Content Commitment	
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.1.2.2	
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html	
	User Notice (ES)	Este es un Certificado Reconocido cuya clave privada está soportada por un dispositivo de creación de firma seguro y cuyo único objeto es el de ser utilizado para generar firmas avanzadas reconocidas	
	User Notice (EN)	This is a Qualified Certificate whose private key is supported by a Secure Signature Creation Device and it is aimed to be used exclusively to create Qualified Electronic Signatures	
Qualified Certificate Statements	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*	
	QCEURetentionPeriod	15 años	
SubjectAltName	Rfc822Name	[Correo electrónico de contacto del suscriptor]	
	Directory Name		
	Nombre	OID	Valor
	Tipo certificado	2.16.724.1.3.5.3.2.1	certificado electrónico de empleado público
	Nombre Entidad	2.16.724.1.3.5.3.2.2	[entidad subscriptora]
	NIF Entidad	2.16.724.1.3.5.3.2.3	[NIF entidad subscriptora]
	DNI/NIE Responsable	2.16.724.1.3.5.3.2.4	[DNI/NIE Responsable]
	Numero de Identificación del	2.16.724.1.3.5.3.2.5	[Número de identificación del suscriptor del

Campo x509v3	Nombre	Valor	
	personal		certificado. Eg: UID]
	Nombre	2.16.724.1.3.5.3.2.6	[Nombre de pila del responsable del certificado de acuerdo con el DNI/NIE]
	Primer Apellido	2.16.724.1.3.5.3.2.7	[Primer apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Segundo Apellido	2.16.724.1.3.5.3.2.8	[Segundo Apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Correo electrónico responsable	2.16.724.1.3.5.3.2.9	[Correo del responsable del certificado de acuerdo con el DNI/NIE]
	Unidad Organizativa	2.16.724.1.3.5.3.2.10	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	Puesto o cargo	2.16.724.1.3.5.3.2.11	[Puesto desempeñado]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.	
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp	
	Access Location (Localización)	http://sescam.jccm.es/va	

A.4.3 Perfil Certificado Empleado Público de Cifrado

A.4.3.1 Nivel Alto

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos ($1 - 2^{159}$)
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	SESCAM

Campo x509v3	Nombre	Valor
	OU (Organizational Unit)	certificado electrónico de empleado público
	OU (Organizational Unit)	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	OU (Organizational Unit)	[Número de identificación del suscriptor del certificado. Se corresponde con el UID]
	Title (Cargo)	[Puesto o cargo del empleado público]
	SerialNumber	[Corresponderá al DNI/NIE del empleado]
	Surname (Apellidos)	[Primer apellido, espacio en blanco, segundo apellido del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	Given Name (Nombre)	[Nombre de pila del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	CN (Nombre Común)	[Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI.]
subjectyPublicKeyInfo	Clave pública	Clave RSA de 2048
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	keyEncipherment, dataEncipherment
extKeyUsage	Uso de clave extendido	EmailProtection clientAuthentication
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.1.1.3
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
	User Notice (ES)	Este es un Certificado Reconocido cuya clave privada está soportada por una tarjeta inteligente y cuyo único objeto es el de ser utilizado para cifrar información.
	User Notice (EN)	This is a Qualified Certificate whose private key is supported by a Smart Card and it is aimed to be used exclusively to encrypt information.
Qualified Certificate Statements	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*
	QCEURetentionPeriod	15 años
	QCSSCD	0.4.0.1862.1.4 *Nota: Indica que la clave esta en un SSCD*
SubjectAltName	Rfc822Name	[Correo electrónico de contacto del suscriptor]
	Directory Name	

Campo x509v3	Nombre	Valor	
	Nombre	OID	Valor
	Tipo certificado	2.16.724.1.3.5.3.1.*1*	certificado electrónico de empleado público
	Nombre Entidad	2.16.724.1.3.5.3.1.2	[entidad subscriptora]
	NIF Entidad	2.16.724.1.3.5.3.1.3	[NIF entidad subscriptora]
	DNI/NIE Responsable	2.16.724.1.3.5.3.1.4	[DNI/NIE Responsable]
	Numero de Identificación del personal	2.16.724.1.3.5.3.1.5	[Número de identificación del suscriptor del certificado. Eg: UID]
	Nombre	2.16.724.1.3.5.3.1.6	[Nombre de pila del responsable del certificado de acuerdo con el DNI/NIE]
	Primer Apellido	2.16.724.1.3.5.3.1.7	[Primer apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Segundo Apellido	2.16.724.1.3.5.3.1.8	[Segundo Apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Correo electrónico responsable	2.16.724.1.3.5.3.1.9	[Correo del responsable del certificado de acuerdo con el DNI/NIE]
	Unidad Organizativa	2.16.724.1.3.5.3.1.10	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	Puesto o cargo	2.16.724.1.3.5.3.1.11	[Puesto desempeñado]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.	
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp	
	Access Location (Localización)	http://sescam.jccm.es/va	

A.4.3.2 Nivel Medio

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos ($1 - 2^{159}$)
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H

Campo x509v3	Nombre	Valor
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	SESCAM
	OU (Organizational Unit)	certificado electrónico de empleado público
	OU (Organizational Unit)	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	OU (Organizational Unit)	[Número de identificación del suscriptor delcertificado. Se corresponde con el UID]
	Title (Cargo)	[Puesto o cargo del empleado público]
	SerialNumber	[Corresponderá al DNI/NIE del empleado]
	Surname (Apellidos)	[Primer apellido, espacio en blanco, segundo apellido del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	Given Name (Nombre)	[Nombre de pila del suscriptor del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	CN (Nombre Común)	[Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte), así como DNI.]
subjectyPublicKeyInfo	Clave pública	Clave RSA de 1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	keyEncipherment, dataEncipherment
extKeyUsage	Uso de clave extendido	EmailProtection clientAuthentication
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.2.1.2.3
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
	User Notice (ES)	Este es un Certificado Reconocido cuya clave privada está soportada por una tarjeta inteligente y cuyo único objeto es el de ser utilizado para cifrar información.
	User Notice (EN)	This is a Qualified Certificate whose private key is supported by a Smart Card and it is aimed to be used exclusively to encrypt information.
Qualified Certificate	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*

Campo x509v3	Nombre	Valor	
Statements	QCEURetentionPeriod	15 años	
SubjectAltName	Rfc822Name	[Correo electrónico de contacto del suscriptor]	
	Directory Name		
	Nombre	OID	Valor
	Tipo certificado	2.16.724.1.3.5.3.2.1	certificado electrónico de empleado público
	Nombre Entidad	2.16.724.1.3.5.3.2.2	[entidad subscriptora]
	NIF Entidad	2.16.724.1.3.5.3.2.3	[NIF entidad subscriptora]
	DNI/NIE Responsable	2.16.724.1.3.5.3.2.4	[DNI/NIE Responsable]
	Numero de Identificación del personal	2.16.724.1.3.5.3.2.5	[Número de identificación del suscriptor del certificado. Eg: UID]
	Nombre	2.16.724.1.3.5.3.2.6	[Nombre de pila del responsable del certificado de acuerdo con el DNI/NIE]
	Primer Apellido	2.16.724.1.3.5.3.2.7	[Primer apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Segundo Apellido	2.16.724.1.3.5.3.2.8	[Segundo Apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Correo electrónico responsable	2.16.724.1.3.5.3.2.9	[Correo del responsable del certificado de acuerdo con el DNI/NIE]
	Unidad Organizativa	2.16.724.1.3.5.3.2.10	[Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado]
	Puesto o cargo	2.16.724.1.3.5.3.2.11	[Puesto desempeñado]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.	
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp	
	Access Location (Localización)	http://sescam.jccm.es/va	

A.5Sede Administrativa

A.5.1 Nivel Alto

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos (1 – 2^{159})
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	[Nombre "Oficial" de la organización del subscriptor.]
	OU (Organizational Unit)	sede electrónica
	OU (Organizational Unit)	[Nombre descriptivo de la sede]
	SerialNumber	[Corresponderá al NIF de la entidad]
	CN (Nombre Común)	[Denominación de nombre de dominio (DNS o IP) donde residirá el certificado].
subjectyPublicKeyInfo	Clave pública	Clave RSA de 2048
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Digital signature, Key Encipherment
extKeyUsage	Uso de clave extendido	serverAuthentication
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.3.1.1
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html

<table>
<tr><th>Campo x509v3</th><th>Nombre</th><th colspan="2">Valor</th></tr>
<tr><td rowspan="2"></td><td>User Notice (ES)</td><td colspan="2">Certificado reconocido de Sede electrónica cuya clave privada está soportada por un dispositivo de creación de firma seguro y cuyo objeto es la identificación electrónica de la sede Administrativa.</td></tr>
<tr><td>User Notice (EN)</td><td colspan="2">This is a Qualified Certificate belonging to the Public Administration whose private key is supported by a Secure Signature Creation Device and it is aimed to identify the subsriptor's eGoverment portal.</td></tr>
<tr><td rowspan="2">Qualified Certificate Statements</td><td>QCCompliance</td><td colspan="2">0.4.0.1862.1.1
Nota: Indica que el certificado es reconocido.</td></tr>
<tr><td>QCEURetentionPeriod</td><td colspan="2">15 años</td></tr>
<tr><td rowspan="10">SubjectAltName</td><td>rfc822Name</td><td colspan="2">[Correo electrónico de contacto de la entidad subscriptora de la sede]</td></tr>
<tr><td>dnsName</td><td colspan="2">[Nombre del Dominio DNS de la Sede]</td></tr>
<tr><td colspan="3">Directory Name</td></tr>
<tr><td>Nombre</td><td>OID</td><td>Valor</td></tr>
<tr><td>Tipo certificado</td><td>2.16.724.1.3.5.1.1.1</td><td>sede electrónica</td></tr>
<tr><td>Nombre Entidad</td><td>2.16.724.1.3.5.1.1.2</td><td>[entidad subscriptora]</td></tr>
<tr><td>NIF Entidad</td><td>2.16.724.1.3.5.1.1.3</td><td>[NIF entidad subscriptora]</td></tr>
<tr><td>Nombre Descriptivo</td><td>2.16.724.1.3.5.1.1.4</td><td>[Nombre descriptivo de la sede electrónica]</td></tr>
<tr><td>Denominación de nombre de dominio IP</td><td>2.16.724.1.3.5.1.1.5</td><td>[Nombre dominio IP]</td></tr>
<tr><td>CRLDistributionPoints</td><td>Punto de distribución de la CRL</td><td colspan="2">http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl
Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.</td></tr>
<tr><td rowspan="2">Authority Info Acesss</td><td>Access Method (Metodo de acceso)</td><td colspan="2">Id-ad-ocsp</td></tr>
<tr><td>Access Location (Localización)</td><td colspan="2">http://sescam.jccm.es/va</td></tr>
</table>

A.5.2 Nivel Medio

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos (1 – 2^{159})
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	[Nombre "Oficial" de la organización del subscriptor.]
	OU (Organizational Unit)	sede electrónica
	OU (Organizational Unit)	[Nombre descriptivo de la sede]
	SerialNumber	[Corresponderá al NIF de la entidad]
	CN (Nombre Común)	[Denominación de nombre de dominio (DNS o IP) donde residirá el certificado].
subjectyPublicKeyInfo	Clave pública	Clave RSA ≥ 1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Digital signature, Key Encipherment
extKeyUsage	Uso de clave extendido	serverAuthentication
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.3.1.2
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html

<table>
<tr><th>Campo x509v3</th><th>Nombre</th><th colspan="2">Valor</th></tr>
<tr><td rowspan="2"></td><td>User Notice (ES)</td><td colspan="2">Certificado reconocido de Sede electrónica cuya clave privada está soportada por un dispositivo de creación de firma y cuyo objeto es la identificación electrónica de la sede Administrativa.</td></tr>
<tr><td>User Notice (EN)</td><td colspan="2">This is a Qualified Certificate belonging to the Public Administration whose private key is supported by a Signature Creation Device and it is aimed to identify the subsriptor's eGoverment portal.</td></tr>
<tr><td rowspan="2">Qualified Certificate Statements</td><td>QCCompliance</td><td colspan="2">0.4.0.1862.1.1
Nota: Indica que el certificado es reconocido.</td></tr>
<tr><td>QCEURetentionPeriod</td><td colspan="2">15 años</td></tr>
<tr><td rowspan="9">SubjectAltName</td><td>rfc822Name</td><td colspan="2">[Correo electrónico de contacto de la entidad subscriptora de la sede]</td></tr>
<tr><td>dnsName</td><td colspan="2">[Nombre del Dominio DNS de la Sede]</td></tr>
<tr><td colspan="3">Directory Name</td></tr>
<tr><td>Nombre</td><td>OID</td><td>Valor</td></tr>
<tr><td>Tipo certificado</td><td>2.16.724.1.3.5.1.2.1</td><td>sede electrónica</td></tr>
<tr><td>Nombre Entidad</td><td>2.16.724.1.3.5.1.2.2</td><td>[entidad subscriptora]</td></tr>
<tr><td>NIF Entidad</td><td>2.16.724.1.3.5.1.2.3</td><td>[NIF entidad subscriptora]</td></tr>
<tr><td>Nombre Descriptivo</td><td>2.16.724.1.3.5.1.2.4</td><td>[Nombre descriptivo de la sede electrónica]</td></tr>
<tr><td>Denominación de nombre de dominio IP</td><td>2.16.724.1.3.5.1.2.5</td><td>[Nombre dominio IP]</td></tr>
<tr><td>CRLDistributionPoints</td><td>Punto de distribución de la CRL</td><td colspan="2">http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl
Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.</td></tr>
<tr><td rowspan="2">Authority Info Acesss</td><td>Access Method (Metodo de acceso)</td><td colspan="2">Id-ad-ocsp</td></tr>
<tr><td>Access Location (Localización)</td><td colspan="2">http://sescam.jccm.es/va</td></tr>
</table>

A.6Sello Administrativo para la actuación Automatizada

A.6.1 Nivel Alto

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos (1 – 2^{159})
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	[Nombre "Oficial" de la organización del subscriptor]
	OU (Organizational Unit)	sello electrónico
	SerialNumber	[Corresponderá al NIF de la entidad]
	Surname (Apellidos)	[Primer apellido, espacio en blanco, segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	Given Name (Nombre)	Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	CN (Nombre Común)	Nombre descriptivo del sistema automático.
subjectyPublicKeyInfo	Clave pública	Clave RSA de 2048
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Digital signature, Content Commitment, Key Encipherment, Data Encipherment.
extKeyUsage	Uso de clave extendido	EmailProtection clientAuthentication

Campo x509v3	Nombre	Valor		
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.3.2.1		
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html		
	User Notice (ES)	Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho Público cuya clave privada está soportada por un dispositivo de creación de firma seguro y cuyo objeto es la actuación automatizada.		
	User Notice (EN)	This is a Qualified Certificate belonging to the Public Administration whose private key is supported by a Secure Signature Creation Device and it is aimed to provide automated actions.		
Qualified Certificate Statements	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*		
	QCEURetentionPeriod	15 años		
BasicConstraints	EC	FALSE		
	PathLenContraint	Ninguno		
SubjectAltName	Rfc822Name	[Correo electrónico de contacto de la entidad subscriptora del sello]		
	Directory Name			
	Nombre	OID	Valor	
	Tipo certificado	2.16.724.1.3.5.2.1.*1*	sello electrónico	
	Nombre Entidad	2.16.724.1.3.5.2.1.*2*	[entidad subscriptora]	
	NIF Entidad	2.16.724.1.3.5.2.1.*3*	[NIF entidad subscriptora]	
	DNI/NIE Responsable	2.16.724.1.3.5.2.1.*4*	[DNI/NIE Responsable]	
	Denominación Sistema o componente	2.16.724.1.3.5.2.1.*5*	[Nombre descriptivo del sistema de sellado automático]	
	Nombre Responsable	2.16.724.1.3.5.2.1.*6*	[Nombre de pila del responsable del certificado de acuerdo con el DNI/NIE]	
	Primer Apellido Responsable	2.16.724.1.3.5.2.1.*7*	[Primer apellido del responsable del certificado de acuerdo con el DNI/NIE]	
	Segundo Apellido Responsable	2.16.724.1.3.5.2.1.*8*	[Segundo Apellido del responsable del certificado de acuerdo con el DNI/NIE]	
	Correo electrónico responsable	2.16.724.1.3.5.2.1.*9*	[Correo del responsable del certificado de acuerdo con el DNI/NIE]	
CRLDistributionPoints	Punto de distribución de CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.		
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp		

Campo x509v3	Nombre	Valor
	Access Location (Localización)	http://sescam.jccm.es/va

A.6.2 Nivel Medio

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA, es un entero positivo no mayor de 20 octetos (1 – 2^{159})
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	[Nombre "Oficial" de la organización del subscriptor]
	OU (Organizational Unit)	sello electrónico
	SerialNumber	[Corresponderá al NIF de la entidad]
	Surname (Apellidos)	[Primer apellido, espacio en blanco, segundo apellido del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	Given Name (Nombre)	[Nombre de pila del responsable del certificado de acuerdo con el DNI o en caso de extranjero en el pasaporte]
	CN (Nombre Común)	[Nombre descriptivo del sistema automático.]
subjectyPublicKeyInfo	Clave pública	Nivel Medio: Clave RSA ≥ 1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Digital signature, Content Commitment, Key Encipherment, Data Encipherment.
extKeyUsage	Uso de clave extendido	EmailProtection clientAuthentication

Campo x509v3	Nombre	Valor	
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.3.2.2	
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html	
	User Notice (ES)	Certificado reconocido de sello electrónico de Administración, órgano o entidad de derecho Público cuya clave privada está soportada por un dispositivo de creación de firma y cuyo objeto es la actuación automatizada.	
	User Notice (EN)	This is a Qualified Certificate belonging to the Public Administration whose private key is supported by a Signature Creation Device and it is aimed to provide automated actions.	
Qualified Certificate Statements	QCCompliance	0.4.0.1862.1.1 *Nota: Indica que el certificado es reconocido.*	
	QCEURetentionPeriod	15 años	
BasicConstraints	EC	FALSE	
	PathLenContraint	Ninguno	
SubjectAltName	Rfc822Name	[Correo electrónico de contacto de la entidad subscriptora del sello]	
	Directory Name		
	Nombre	OID	Valor
	Tipo certificado	2.16.724.1.3.5.2.2.*1*	sello electrónico
	Nombre Entidad	2.16.724.1.3.5.2.2.*2*	[entidad subscriptora]
	NIF Entidad	2.16.724.1.3.5.2.2.*3*	[NIF entidad subscriptora]
	DNI/NIE Responsable	2.16.724.1.3.5.2.2.*4*	[DNI/NIE Responsable]
	Denominación Sistema o componente	2.16.724.1.3.5.2.2.*5*	[Nombre descriptivo del sistema de sellado automático]
	Nombre Responsable	2.16.724.1.3.5.2.2.*6*	[Nombre de pila del responsable del certificado de acuerdo con el DNI/NIE]
	Primer Apellido Responsable	2.16.724.1.3.5.2.2.*7*	[Primer apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Segundo Apellido Responsable	2.16.724.1.3.5.2.2.*8*	[Segundo Apellido del responsable del certificado de acuerdo con el DNI/NIE]
	Correo electrónico responsable	2.16.724.1.3.5.2.2.*9*	[Correo del responsable del certificado de acuerdo con el DNI/NIE]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.	
Authority Info Acesss	Access Method (Metodo de acceso)	Id-ad-ocsp	
	Access Location (Localización)	http://sescam.jccm.es/va	

A.7Dispositivos

A.7.1 Perfil de Certificado Servidor WEB

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Subject	[El contenido en la petición]	
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 1 años
subjectyPublicKeyInfo	Clave pública	Clave RSA ≥1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la CA
keyUsage	Uso de la clave	Digital signature, Key Encipherment
extKeyUsage	Uso de clave extendido	ServerAuthentication
NetscapeCertType	Uso de clave extendido	SSL server
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.4.1
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
BasicConstraints	EC	FALSE
	PathLenContraint	Ninguno
SubjectAltName	rfc822Name	[Correo electrónico de contacto de la entidad subscriptora del Servidor SSL]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.

A.7.2 Perfil de Certificado de Aplicaciones

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	OU (Unidad Organizativa)	[Nombre Unidad]
	CN (Nombre)	[Nombre aplicación]
subjectyPublicKeyInfo	Clave publica de la EC	Clave RSA ≥1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la ECS
keyUsage	Uso de la clave	Digital signature, Content Commitment, Key Encipherment, Data Encipherment.
extKeyUsage	Uso de clave extendido	ClientAuth, ServerAuth, EmailProtection
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.4.2
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
BasicConstraints	EC	FALSE
	PathLenContraint	Ninguno
SubjectAltName	rfc822Name	[Correo electrónico de contacto de la entidad subscriptora del Servidor SSL]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.

A.7.3 Perfil de Certificado Controlador de Dominio

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	OU (Unidad Organizativa)	[Nombre Unidad]
	CN (Nombre)	[Nombre controlador]
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 3 años
subjectyPublicKeyInfo	Clave publica de la EC	Clave RSA ≥1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la ECS
keyUsage	Uso de la clave	Digital signature, Key Encipherment
extKeyUsage	Uso de clave extendido	ClientAuth, ServerAuth
Certificate Template Name	Plantilla de certificado	"DomainController"
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.4.3
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
BasicConstraints	EC	FALSE
	PathLenContraint	Ninguno
SubjectAltName	OtherName	[GUID del Controlador de Dominio]
	DNSName	[Nombre del Controlador de Dominio (DNS)]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.

A.7.4 Perfil de Certificado para Firma de Código

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio asignado por la CA
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	ES
	O (Organización)	JCCM
	OU (Unidad Org.)	SESCAM
	SERIALNUMBER	Q4500146H
	CN (Nombre)	SESCAM CA Entidades Finales
Validity	NotBefore	
	NotAfter	NotBefore + 3 años
Subject	C (País)	ES
	O (Organización)	JCCM
	O (Organización)	SESCAM (NIF Q-4500146H)
	OU (Unidad Organizativa)	< Nombre Dpto >
	CN (Nombre)	<Suscriptor>
subjectyPublicKeyInfo	Clave publica de la EC	Clave RSA ≥1024
Extensiones estándar		
subjectKeyIdentifier	Identificador de clave pública del sujeto	Hash de la clave pública que se genera automáticamente
authorityKeyIdentifier	Identificador de la llave pública del emisor	Mismo valor que la extensión subjectKeyIdentifier de la ECS
keyUsage	Uso de la clave	Digital signature
extKeyUsage	Uso de clave extendido	Code Signing
CertificatePolicies	Policy Identifier	2.16.724.4.8.10.60.10.4.4
	CPS Pointer	http://sescam.jccm.es/pki/dpc/dpcv2.html
BasicConstraints	EC	FALSE
	PathLenContraint	Ninguno
SubjectAltName	rfc822Name	[correo dpto suscriptor]
CRLDistributionPoints	Punto de distribución de la CRL	http://sescam.jccm.es/pki/crls/sescam_subca_{crlId}.crl Donde {crlId} indica el identificador de la CRL particionada a la que está asociado el certificado y en el que puede encontrarse información acerca de su estado.